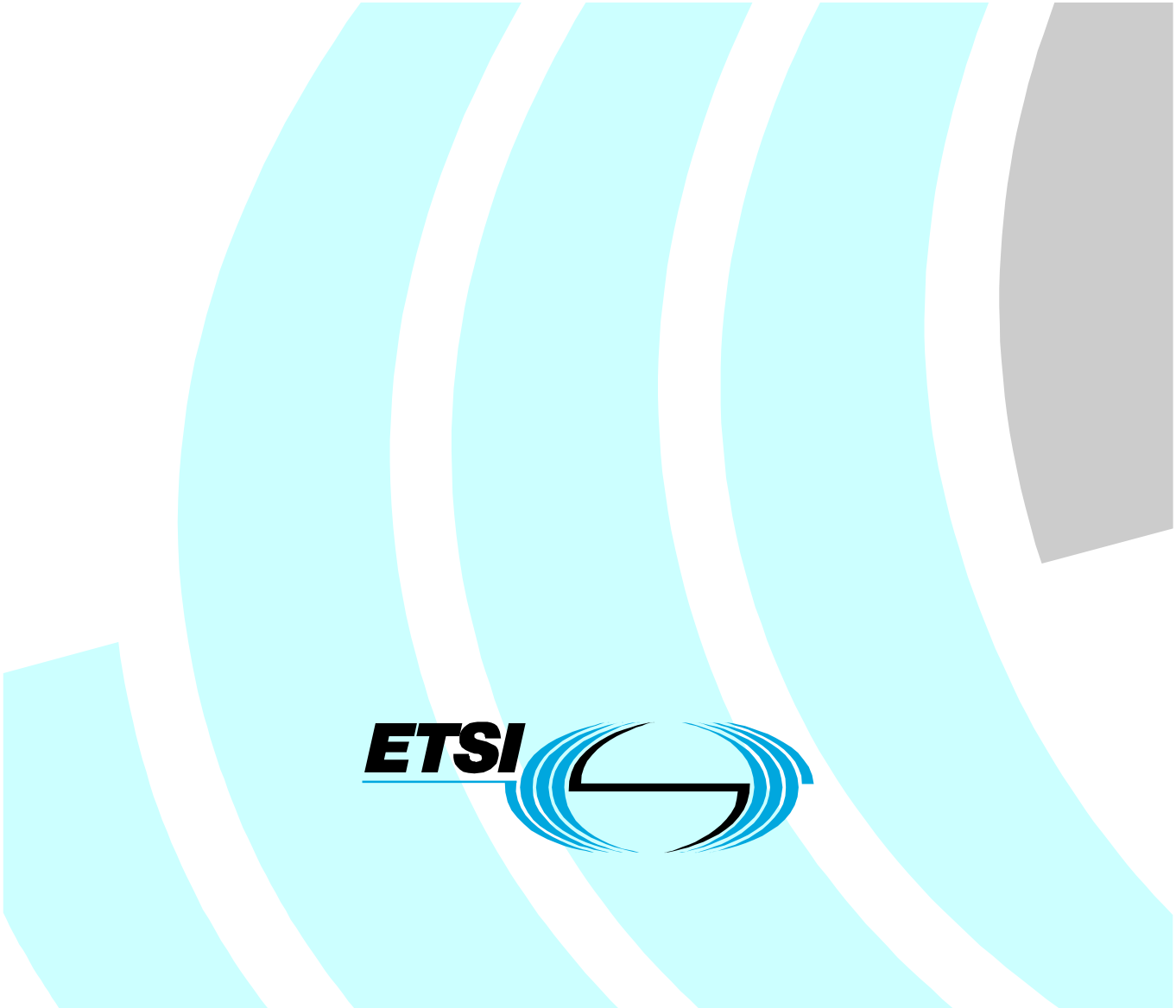
ETSI TS 102 559 V1.1.1 (2006-12)

Technical Specification

Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Mobility; Requirements Catalogue



Reference
DTS/MTS-IPT-013-IPv6-MobReq

Keywords
IP, IPv6, mobility, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

1 Scope

The present document is a catalogue of all of the mobility-related IPv6 requirements extracted from the following IETF specifications:

RFC3775 [2]: Mobility Support in IPv6 (MIPv6).

RFC3776 [3]: Using IPsec to Protect Mobile IPv6 Signalling between Mobile Nodes and Home Agents.

RFC4068 [4]: Fast Handovers for Mobile IPv6.

RFC2473 [1]: Generic Packet Tunnelling in IPv6.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

[1] IETF RFC2473: "Generic Packet Tunneling in IPv6 Specification".

[2] IETF RFC3775: "Mobility Support in IPv6".

[3] IETF RFC3776: "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents".

[4] IETF RFC4068: "Fast Handovers for Mobile IPv6".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AH	Authentication Header
DES	Data Encryption Standard
ESP	Encapsulated Security Payload
IANA	Internet Assigned Number Association
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Message Authentication Code
MIPv6	Mobile IPv6
NAR	New Address Router
PAR	Previous Access Router
RFC	Request For Comments (IETF terminology for a draft standard)

SA	Security Association
TCP	Transport Control Protocol
UDP	User Datagram Protocol

4 Requirements Catalogue

The mobility requirements related to Internet Protocol version 6 (IPv6) are specified in a number of IETF documents. These documents include requirements for the overall IPv6 mobility architecture [2], the use of the IP Security (IPsec) [3], tunnelling MIPv6 packets [1] and fast handover [4]. The present document is a catalogue of all of the normative requirements from these mobility specifications. Each requirement is given a unique identifier (for example, RQ_001_1234) and the following information is included with each:

- the clause number in the RFC from which the requirement has been extracted;
- the type of requirement (Mandatory, Optional or Recommended);
- the type of device to which the requirement applies (for example, Mobile Node or Home Agent);
- the actual text from which the requirement was extracted.

4.1 Requirements extracted from RFC3775

Identifier: RQ_001_1001
RFC Clause: 1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Mobile IPv6 SHALL enable a mobile node to move from one link to another without changing the mobile node's "home address".

RFC Text:
The protocol defined in this document, known as Mobile IPv6,allows a mobile node to move from one link to another without changing the mobile node's "home address". Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet. The mobile node may also continue to communicate with other nodes (stationary or mobile) after moving to a new link.

Identifier: RQ_001_1002
RFC Clause: 1
Type: Optional
Applies to: Mobile_Node

Requirement:
Packets may be routed to the mobile node using its home address regardless of the mobile node's current point of attachment to the Internet.

RFC Text:
The protocol defined in this document, known as Mobile IPv6, allows a mobile node to move from one link to another without changing the mobile node's "home address". **Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet.** The mobile node may also continue to communicate with other nodes (stationary or mobile) after moving to a new link.

Identifier: RQ_001_1003
RFC Clause: 1
Type: Optional
Applies to: Mobile_Node

Requirement:
The mobile node CAN also continue to communicate with other nodes (stationary or mobile) after moving to a new link

RFC Text:
The protocol defined in this document, known as Mobile IPv6, allows a mobile node to move from one link to another without changing the mobile node's "home address". Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet. **The mobile node may also continue to communicate with other nodes (stationary or mobile) after moving to a new link.**

Identifier: RQ_001_1004
RFC Clause: 4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
A mobile node is addressable at its home address, whether it is currently attached to its home link or is away from home

RFC Text:
A mobile node is always expected to be addressable at its home address, whether it is currently attached to its home link or is away from home. The "home address" is an IP address assigned to the mobile node within its home subnet prefix on its home link. While a mobile node is at home, packets addressed to its home address are routed to the mobile node's home link, using conventional Internet routing mechanisms.

Identifier: RQ_001_1005
RFC Clause: 4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
While a mobile node is attached to some foreign link away from home, it is also addressable at one or more care-of addresses

RFC Text:
While a mobile node is attached to some foreign link away from home, it is also addressable at one or more care-of addresses. A care-of address is an IP address associated with a mobile node that has the subnet prefix of a particular foreign link. The mobile node can acquire its care-of address through conventional IPv6 mechanisms, such as stateless or stateful auto-configuration. As long as the mobile node stays in this location, packets addressed to this care-of address will be routed to the mobile node. The mobile node may also accept packets from several care-of addresses, such as when it is moving but still reachable at the previous link.

Identifier: RQ_001_1006
RFC Clause: 4.1
Type: Optional
Applies to: Home_Agent

Requirement:
Support bidirectional tunneling using IPv6 encapsulation between the Home Agent and the mobile node

RFC Text:
There are two possible modes for communications between the mobile node and a correspondent node. **The first mode, bidirectional tunneling, does not require Mobile IPv6 support from the correspondent node and is available even if the mobile node has not registered its current binding with the correspondent node**. Packets from the correspondent node are routed to the home agent and then tunneled to the mobile node. Packets to the correspondent node are tunneled from the mobile node to the home agent ("reverse tunneled") and then routed normally from the home network to the correspondent node. In this mode, the home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address (or home addresses) on the home link. Each intercepted packet is tunneled to the mobile node's primary care-of address. This tunneling is performed using IPv6 encapsulation [15].

Identifier: RQ_001_1006
RFC Clause: 4.1
Type: Optional
Applies to: Mobile_Node

Requirement:
Support bidirectional tunneling using IPv6 encapsulation between the Home Agent and the mobile node

RFC Text:
There are two possible modes for communications between the mobile node and a correspondent node. **The first mode, bidirectional tunneling, does not require Mobile IPv6 support from the correspondent node and is available even if the mobile node has not registered its current binding with the correspondent node**. Packets from the correspondent node are routed to the home agent and then tunneled to the mobile node. Packets to the correspondent node are tunneled from the mobile node to the home agent ("reverse tunneled") and then routed normally from the home network to the correspondent node. In this mode, the home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address (or home addresses) on the home link. Each intercepted packet is tunneled to the mobile node's primary care-of address. This tunneling is performed using IPv6 encapsulation [15].

Identifier: RQ_001_1007
RFC Clause: 4.1
Type: Optional
Applies to: Mobile_Node

Requirement:
the mobile node MAY register its current binding at the correspondent node

RFC Text:
The second mode, "route optimization", requires the mobile node to register its current binding at the correspondent node. Packets from the correspondent node can be routed directly to the care-of address of the mobile node. When sending a packet to any IPv6 destination, the correspondent node checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses a new type of IPv6 routing header [11] (see Section 6.4) to route the packet to the mobile node by way of the care-of address indicated in this binding.

Identifier: RQ_001_1008
RFC Clause: 4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Mobile Nodes shall support “dynamic home agent address discovery"

RFC Text:
Mobile IPv6 also provides support for multiple home agents, and a limited support for the reconfiguration of the home network. In these cases, the mobile node may not know the IP address of its own home agent, and even the home subnet prefixes may change over time. A mechanism, known as "dynamic home agent address discovery" allows a mobile node to dynamically discover the IP address of a home agent on its home link, even when the mobile node is away from home. Mobile nodes can also learn new information about home subnet prefixes through the "mobile prefix discovery" mechanism. These mechanisms are described starting from Section 6.5.

Identifier: RQ_001_1009
RFC Clause: 4.1
Type: Optional
Applies to: Mobile_Node

Requirement:
Mobile nodes MAY learn new information about home subnet prefixes through the "mobile prefix discovery" mechanism

RFC Text:
Mobile IPv6 also provides support for multiple home agents, and a limited support for the reconfiguration of the home network. In these cases, the mobile node may not know the IP address of its own home agent, and even the home subnet prefixes may change over time. A mechanism, known as "dynamic home agent address discovery" allows a mobile node to dynamically discover the IP address of a home agent on its home link, even when the mobile node is away from home. Mobile nodes can also learn new information about home subnet prefixes through the "mobile prefix discovery" mechanism. These mechanisms are described starting from Section 6.5.

Identifier: RQ_001_1010
RFC Clause: 4.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
home addresses MUST be unicast routable addresses

RFC Text:
This specification requires that home and care-of addresses MUST be unicast routable addresses. Site-local addresses may be usable on networks that are not connected to the Internet, but this specification does not define when such usage is safe and when it is not. Mobile nodes may not be aware of which site they are currently in, it is hard to prevent accidental attachment to other sites, and ambiguity of site-local addresses can cause problems if the home and visited networks use the same addresses. Therefore, site-local addresses SHOULD NOT be used as home or care-of addresses.

Identifier: RQ_001_1011
RFC Clause: 4.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
care-of addresses MUST be unicast routable addresses.

RFC Text:
This specification requires that home and care-of addresses MUST be unicast routable addresses. Site-local addresses may be usable on networks that are not connected to the Internet, but this specification does not define when such usage is safe and when it is not. Mobile nodes may not be aware of which site they are currently in, it is hard to prevent accidental attachment to other sites, and ambiguity of site-local addresses can cause problems if the home and visited networks use the same addresses. Therefore, site-local addresses SHOULD NOT be used as home or care-of addresses.

Identifier: RQ_001_1012
RFC Clause: 4.6
Type: Recommendation
Applies to: Mobile_Node

Requirement:
site-local addresses SHOULD NOT be used as home or care-of addresses.

RFC Text:
This specification requires that home and care-of addresses MUST be unicast routable addresses. Site-local addresses may be usable on networks that are not connected to the Internet, but this specification does not define when such usage is safe and when it is not. Mobile nodes may not be aware of which site they are currently in, it is hard to prevent accidental attachment to other sites, and ambiguity of site-local addresses can cause problems if the home and visited networks use the same addresses. Therefore, **site-local addresses SHOULD NOT be used as home or care-of addresses**.

Identifier: RQ_001_1013
RFC Clause: 5
Type: Mandatory
Applies to: Home_Agent

Requirement:
Binding Updates between Mobile Node and Home Agent MUST be protected by the use of IPsec extension headers.

RFC Text:
Binding Updates are protected by the use of IPsec extension headers, or by the use of the Binding Authorization Data option. This option employs a binding management key, Kbm, which can be established through the return routability procedure. Mobile prefix discovery is protected through the use of IPsec extension headers. Mechanisms related to transporting payload packets - such as the Home Address destination option and type 2 routing header - have been specified in a manner which restricts their use in attacks.

Identifier: RQ_001_1013
RFC Clause: 5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Binding Updates between Mobile Node and Home Agent MUST be protected by the use of IPsec extension headers.

RFC Text:
Binding Updates are protected by the use of IPsec extension headers, or by the use of the Binding Authorization Data option. This option employs a binding management key, Kbm, which can be established through the return routability procedure. Mobile prefix discovery is protected through the use of IPsec extension headers. Mechanisms related to transporting payload packets - such as the Home Address destination option and type 2 routing header - have been specified in a manner which restricts their use in attacks.

Identifier: RQ_001_1014
RFC Clause: 5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Mobile prefix discovery is protected through the use of IPsec extension headers

RFC Text:
Binding Updates are protected by the use of IPsec extension headers, or by the use of the Binding Authorization Data option. This option employs a binding management key, Kbm, which can be established through the return routability procedure. **Mobile prefix discovery is protected through the use of IPsec extension headers**. Mechanisms related to transporting payload packets - such as the Home Address destination option and type 2 routing header - have been specified in a manner which restricts their use in attacks.

Identifier: RQ_001_1015
RFC Clause: 5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If binding Updates are protected by the use of Ipsec, the mobile node and the home agent MUST use an IPsec security association to protect the integrity and authenticity of the Binding Updates and Acknowledgements

RFC Text:
The mobile node and the home agent MUST use an IPsec security association to protect the integrity and authenticity of the Binding Updates and Acknowledgements. Both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [6] header in transport mode and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection. Note that Authentication Header (AH) [5] is also possible but for brevity not discussed in this specification.

Identifier: RQ_001_1016
RFC Clause: 5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If binding Updates are protected by the use of Ipsec, both the mobile nodes and the home agents MUST support the Encapsulating Security Payload (ESP) header in transport mode

RFC Text:
The mobile node and the home agent MUST use an IPsec security association to protect the integrity and authenticity of the Binding Updates and Acknowledgements. **Both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [6] header in transport mode** and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection. Note that Authentication Header (AH) [5] is also possible but for brevity not discussed in this specification.

Identifier: RQ_001_1016
RFC Clause: 5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If binding Updates are protected by the use of Ipsec, both the mobile nodes and the home agents MUST support the Encapsulating Security Payload (ESP) header in transport mode

RFC Text:
The mobile node and the home agent MUST use an IPsec security association to protect the integrity and authenticity of the Binding Updates and Acknowledgements. **Both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [6] header in transport mode** and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection. Note that Authentication Header (AH) [5] is also possible but for brevity not discussed in this specification.

Identifier: RQ_001_1017
RFC Clause: 5.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
If binding Updates are protected by the use of Ipsec, both the mobile nodes and the home agents SHOULD use the Encapsulating Security Payload (ESP) header in transport mode

RFC Text:
The mobile node and the home agent MUST use an IPsec security association to protect the integrity and authenticity of the Binding Updates and Acknowledgements. Both the mobile nodes and the home agents MUST support and **SHOULD use the Encapsulating Security Payload (ESP) [6] header in transport** mode and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection. Note that Authentication Header (AH) [5] is also possible but for brevity not discussed in this specification.

Identifier: RQ_001_1017
RFC Clause: 5.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If binding Updates are protected by the use of Ipsec, both the mobile nodes and the home agents SHOULD use the Encapsulating Security Payload (ESP) header in transport mode

RFC Text:
The mobile node and the home agent MUST use an IPsec security association to protect the integrity and authenticity of the Binding Updates and Acknowledgements. Both the mobile nodes and the home agents MUST support and **SHOULD use the Encapsulating Security Payload (ESP) [6] header in transport** mode and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection. Note that Authentication Header (AH) [5] is also possible but for brevity not discussed in this specification.

Identifier: RQ_001_1018
RFC Clause: 5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If binding Updates are protected by the use of Ipsec, both the mobile nodes and the home agents MUST use a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

RFC Text:
The mobile node and the home agent MUST use an IPsec security association to protect the integrity and authenticity of the Binding Updates and Acknowledgements. Both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [6] header in transport mode **and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.** Note that Authentication Header (AH) [5] is also possible but for brevity not discussed in this specification.

Identifier: RQ_001_1018
RFC Clause: 5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If binding Updates are protected by the use of Ipsec, both the mobile nodes and the home agents MUST use a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

RFC Text:
The mobile node and the home agent MUST use an IPsec security association to protect the integrity and authenticity of the Binding Updates and Acknowledgements. Both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [6] header in transport mode **and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.** Note that Authentication Header (AH) [5] is also possible but for brevity not discussed in this specification.

Identifier: RQ_001_1019
RFC Clause: 5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries MUST be created.

RFC Text:
In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries must be created. A mobile node must be prevented from using its security association to send a Binding Update on behalf of another mobile node using the same home agent. This MUST be achieved by having the home agent check that the given home address has been used with the right security association. Such a check is provided in the IPsec processing, by having the security policy database entries unequivocally identify a single security association for protecting Binding Updates between any given home address and home agent. In order to make this possible, it is necessary that the home address of the mobile node is visible in the Binding Updates and Acknowledgements. The home address is used in these packets as a source or destination, or in the Home Address Destination option or the type 2 routing header.

Identifier: RQ_001_1019
RFC Clause: 5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries MUST be created.

RFC Text:
In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries must be created. A mobile node must be prevented from using its security association to send a Binding Update on behalf of another mobile node using the same home agent. This MUST be achieved by having the home agent check that the given home address has been used with the right security association. Such a check is provided in the IPsec processing, by having the security policy database entries unequivocally identify a single security association for protecting Binding Updates between any given home address and home agent. In order to make this possible, it is necessary that the home address of the mobile node is visible in the Binding Updates and Acknowledgements. The home address is used in these packets as a source or destination, or in the Home Address Destination option or the type 2 routing header.

Identifier: RQ_001_1020
RFC Clause: 5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Home Agent must prevent the Mobile Node from using its security association to send a Binding Update on behalf of another mobile node using the same home agent.

RFC Text:
In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries must be created. **A mobile node must be prevented from using its security association to send a Binding Update on behalf of another mobile node using the same home agent**. This MUST be achieved by having the home agent check that the given home address has been used with the right security association. Such a check is provided in the IPsec processing, by having the security policy database entries unequivocally identify a single security association for protecting Binding Updates between any given home address and home agent. In order to make this possible, it is necessary that the home address of the mobile node is visible in the Binding Updates and Acknowledgements. The home address is used in these packets as a source or destination, or in the Home Address Destination option or the type 2 routing header.

Identifier: RQ_001_1021
RFC Clause: 5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The prevention of a mobile node from using its security association to send a Binding Update on behalf of another mobile node using the same home agent MUST be achieved by having the home agent check that the given home address has been used with the right security association.

RFC Text:
In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries must be created. A mobile node must be prevented from using its security association to send a Binding Update on behalf of another mobile node using the same home agent. **This MUST be achieved by having the home agent check that the given home address has been used with the right security association**. Such a check is provided in the IPsec processing, by having the security policy database entries unequivocally identify a single security association for protecting Binding Updates between any given home address and home agent. In order to make this possible, it is necessary that the home address of the mobile node is visible in the Binding Updates and Acknowledgements. The home address is used in these packets as a source or destination, or in the Home Address Destination option or the type 2 routing header.

Identifier: RQ_001_1022
RFC Clause: 5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The home address of the mobile node MUST be visible in the Binding Updates and Acknowledgements.

RFC Text:
In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries must be created. A mobile node must be prevented from using its security association to send a Binding Update on behalf of another mobile node using the same home agent. This MUST be achieved by having the home agent check that the given home address has been used with the right security association. Such a check is provided in the IPsec processing, by having the security policy database entries unequivocally identify a single security association for protecting Binding Updates between any given home address and home agent. **In order to make this possible, it is necessary that the home address of the mobile node is visible in the Binding Updates and Acknowledgements.** The home address is used in these packets as a source or destination, or in the Home Address Destination option or the type 2 routing header.

Identifier: RQ_001_1023
RFC Clause: 5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The home address of the mobile node MUST be used in the Binding Update packets as a source or destination, or in the Home Address Destination option or the type 2 routing header.

RFC Text:
In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries must be created. A mobile node must be prevented from using its security association to send a Binding Update on behalf of another mobile node using the same home agent. This MUST be achieved by having the home agent check that the given home address has been used with the right security association. Such a check is provided in the IPsec processing, by having the security policy database entries unequivocally identify a single security association for protecting Binding Updates between any given home address and home agent. In order to make this possible, it is necessary that the home address of the mobile node is visible in the Binding Updates and Acknowledgements. **The home address is used in these packets as a source or destination, or in the Home Address Destination option or the type 2 routing header.**

Identifier: RQ_001_1024
RFC Clause: 5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Manual configuration of security associations MUST be supported

RFC Text:
As with all IPsec security associations in this specification, **manual configuration of security associations MUST be supported.** The used shared secrets MUST be random and unique for different mobile nodes, and MUST be distributed off-line to the mobile nodes.

Identifier: RQ_001_1025
RFC Clause: 5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The used shared secrets MUST be random and unique for different mobile nodes

RFC Text:
As with all IPsec security associations in this specification, manual configuration of security associations MUST be supported. **The used shared secrets MUST be random and unique for different mobile nodes,** and MUST be distributed off-line to the mobile nodes.

Identifier: RQ_001_1026
RFC Clause: 5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The used shared secrets MUST be distributed off-line to the mobile nodes.

RFC Text:
As with all IPsec security associations in this specification, manual configuration of security associations MUST be supported. **The used shared secrets** MUST be random and unique for different mobile nodes, and **MUST be distributed off-line to the mobile nodes.**

Identifier: RQ_001_1027
RFC Clause: 5.1
Type: Optional
Applies to: Home_Agent

Requirement:
Automatic key management with IKE [9] MAY be supported

RFC Text:
Automatic key management with IKE [9] MAY be supported. When IKE is used, either the security policy database entries or the Mobile IPv6 processing MUST unequivocally identify the IKE phase 1 credentials which can be used to authorize the creation of security associations for protecting Binding Updates for a particular home address. How these mappings are maintained is outside the scope of this specification, but they may be maintained, for instance, as a locally administered table in the home agent. If the phase 1 identity is a Fully Qualified Domain Name (FQDN), secure forms of DNS may also be used.

Identifier: RQ_001_1027
RFC Clause: 5.1
Type: Optional
Applies to: Mobile_Node

Requirement:
Automatic key management with IKE [9] MAY be supported

RFC Text:
Automatic key management with IKE [9] MAY be supported. When IKE is used, either the security policy database entries or the Mobile IPv6 processing MUST unequivocally identify the IKE phase 1 credentials which can be used to authorize the creation of security associations for protecting Binding Updates for a particular home address. How these mappings are maintained is outside the scope of this specification, but they may be maintained, for instance, as a locally administered table in the home agent. If the phase 1 identity is a Fully Qualified Domain Name (FQDN), secure forms of DNS may also be used.

Identifier: RQ_001_1028
RFC Clause: 5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When IKE is supported, either the security policy database entries or the Mobile IPv6 processing MUST unequivocally identify the IKE phase 1 credentials which can be used to authorize the creation of security associations for protecting Binding Updates for a particular home address.

RFC Text:
Automatic key management with IKE [9] MAY be supported. **When IKE is used, either the security policy database entries or the Mobile IPv6 processing MUST unequivocally identify the IKE phase 1 credentials which can be used to authorize the creation of security associations for protecting Binding Updates for a particular home address.** How these mappings are maintained is outside the scope of this specification, but they may be maintained, for instance, as a locally administered table in the home agent. If the phase 1 identity is a Fully Qualified Domain Name (FQDN), secure forms of DNS may also be used.

Identifier: RQ_001_1029
RFC Clause: 5.1
Type: Optional
Applies to: Home_Agent

Requirement:
security associations for protecting Binding Updates for a particular home address MAY be maintained as a locally administered table in the home agent.

RFC Text:
Automatic key management with IKE [9] MAY be supported. When IKE is used, either the security policy database entries or the Mobile IPv6 processing MUST unequivocally identify the IKE phase 1 credentials which can be used to authorize the creation of **security associations for protecting Binding Updates for a particular home address. How these mappings are maintained is outside the scope of this specification, but they may be maintained, for instance, as a locally administered table in the home agent. If the phase 1 identity is a Fully Qualified Domain Name (FQDN), secure forms of DNS may also be used.**

Identifier: RQ_001_1030
RFC Clause: 5.1
Type: Optional
Applies to: Home_Agent

Requirement:
security associations for protecting Binding Updates for a particular home address MAY be maintained using secure forms of DNS, if the phase 1 identity is a Fully Qualified Domain Name (FQDN).

RFC Text:
Automatic key management with IKE [9] MAY be supported. When IKE is used, either the security policy database entries or the Mobile IPv6 processing MUST unequivocally identify the IKE phase 1 credentials which can be used to authorize the creation of security associations for protecting Binding Updates for a particular home address. How these mappings are maintained is outside the scope of this specification, but **they may be maintained, for instance, as a locally administered table in the home agent. If the phase 1 identity is a Fully Qualified Domain Name (FQDN),** secure forms of DNS may also be used.

Identifier: RQ_001_1031
RFC Clause: 5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When IKE version 1 is used with preshared secret authentication between the mobile node and the home agent, aggressive mode MUST be used.

RFC Text:
When IKE version 1 is used with preshared secret authentication between the mobile node and the home agent, aggressive mode MUST be used.

Identifier: RQ_001_1032
RFC Clause: 5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ID_IPV6_ADDR Identity Payload MUST NOT be used in IKEv1 phase 1.

RFC Text:
The ID_IPV6_ADDR Identity Payload MUST NOT be used in IKEv1 phase 1.

Identifier: RQ_001_1033
RFC Clause: 5.2.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Each correspondent node has a secret key, Kcn, called the "node key", which it uses to produce the keygen tokens sent to the mobile nodes.

RFC Text:
Each correspondent node has a secret key, Kcn, called the "node key", which it uses to produce the keygen tokens sent to the mobile nodes. The node key MUST be a random number, 20 octets in length. The node key allows the correspondent node to verify that the keygen tokens used by the mobile node in authorizing a Binding Update are indeed its own. This key MUST NOT be shared with any other entity.

Identifier: RQ_001_1034
RFC Clause: 5.2.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The node key(Kcn) MUST be a random number, 20 octets in length.

RFC Text:
Each correspondent node has a secret key, Kcn, called the "node key", which it uses to produce the keygen tokens sent to the mobile nodes. **The node key MUST be a random number, 20 octets in length**. The node key allows the correspondent node to verify that the keygen tokens used by the mobile node in authorizing a Binding Update are indeed its own. This key MUST NOT be shared with any other entity.

Identifier: RQ_001_1035
RFC Clause: 5.2.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The node key(Kcn) MUST NOT be shared with any other entity.

RFC Text:
Each correspondent node has a secret key, Kcn, called the "node key", which it uses to produce the keygen tokens sent to the mobile nodes. **The node key MUST be a random number, 20 octets in length**. The node key allows the correspondent node to verify that the keygen tokens used by the mobile node in authorizing a Binding Update are indeed its own. **This key MUST NOT be shared with any other entity**.

Identifier: RQ_001_1036
RFC Clause: 5.2.1
Type: Optional
Applies to: Correspondent_Node

Requirement:
A correspondent node MAY generate a fresh node key at any time

RFC Text:
A correspondent node MAY generate a fresh node key at any time; this avoids the need for secure persistent key storage. Procedures for optionally updating the node key are discussed later in Section 5.2.7.

Identifier: RQ_001_1037
RFC Clause: 5.2.2
Type: Recommendation
Applies to: Node

Requirement:
Nonces should be generated by using a random number generator that is known to have good randomness properties

RFC Text:
Each correspondent node also generates nonces at regular intervals. **The nonces should be generated by using a random number generator that is known to have good randomness properties [1].** A correspondent node may use the same Kcn and nonce with all the mobiles it is in communication with.

Identifier: RQ_001_1038
RFC Clause: 5.2.2
Type: Optional
Applies to: Correspondent_Node

Requirement:
A correspondent node may use the same Kcn and nonce with all the mobiles it is in communication with.

RFC Text:
Each correspondent node also generates nonces at regular intervals. The nonces should be generated by using a random number generator that is known to have good randomness properties [1]. **A correspondent node may use the same Kcn and nonce with all the mobiles it is in communication with.**

Identifier: RQ_001_1039
RFC Clause: 5.2.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
When a new nonce is generated, it must be associated with a new nonce index

RFC Text:
Each nonce is identified by a nonce index. **When a new nonce is generated, it must be associated with a new nonce index**; this may be done, for example, by incrementing the value of the previous nonce index, if the nonce index is used as an array pointer into a linear array of nonces. However, there is no requirement that nonces be stored that way, or that the values of subsequent nonce indices have any particular relationship to each other. The index value is communicated in the protocol, so that if a nonce is replaced by new nonce during the run of a protocol, the correspondent node can distinguish messages that should be checked against the old nonce from messages that should be checked against the new nonce. Strictly speaking, indices are not necessary in the authentication, but allow the correspondent node to efficiently find the nonce value that it used in creating a keygen token.

Identifier: RQ_001_1041
RFC Clause: 5.2.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Expired nonce values MUST be discarded.

RFC Text:
Correspondent nodes keep both the current nonce and a small set of valid previous nonces whose lifetime has not yet expired. **Expired values MUST be discarded,** and messages using stale or unknown indices will be rejected.

Identifier: RQ_001_1042
RFC Clause: 5.2.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Messages using stale or unknown nonce indices will be rejected.

RFC Text:
Correspondent nodes keep both the current nonce and a small set of valid previous nonces whose lifetime has not yet expired. Expired values MUST be discarded, **and messages using stale or unknown indices will be rejected.**

Identifier: RQ_001_1043
RFC Clause: 5.2.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
The recommended length of a nonce is 64 bits.

RFC Text:
A nonce is an octet string of any length. **The recommended length is 64 bits.**

Identifier: RQ_001_1044
RFC Clause: 5.2.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The mobile node should set the home init or care-of init cookie to a newly generated random number in every Home or Care-of Test Init message it sends.

RFC Text:
The mobile node should set the home init or care-of init cookie to a newly generated random number in every Home or Care-of Test Init message it sends. The cookies are used to verify that the Home Test or Care-of Test message matches the Home Test Init or Care-of Test Init message, respectively. These cookies also serve to ensure that parties who have not seen the request cannot spoof responses.

Identifier: RQ_001_1045
RFC Clause: 5.2.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
A keygen token is valid as long as both the secret key (Kcn) and the nonce used to create it are valid.

RFC Text:
Home and care-of keygen tokens are produced by the correspondent node based on its currently active secret key (Kcn) and nonces, as well as the home or care-of address (respectively). **A keygen token is valid as long as both the secret key (Kcn) and the nonce used to create it are valid.**

Identifier: RQ_001_1046
RFC Clause: 5.2.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Message Authentication Codes (MACs) are computed using HMAC_SHA1 [25, 20].

RFC Text:
In this specification, the function used to compute hash values is SHA1 [20]. **Message Authentication Codes (MACs) are computed using HMAC_SHA1 [25, 20].** HMAC_SHA1(K,m) denotes such a MAC computed on message m with key K.

Identifier: RQ_001_1047
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If direct binding between the mobile node and the correspondant node is established, the Return Routability Procedure MUST be used to enable the correspondent node to obtain some reasonable assurance that the mobile node is in fact addressable at its claimed care-of address as well as at its home address.

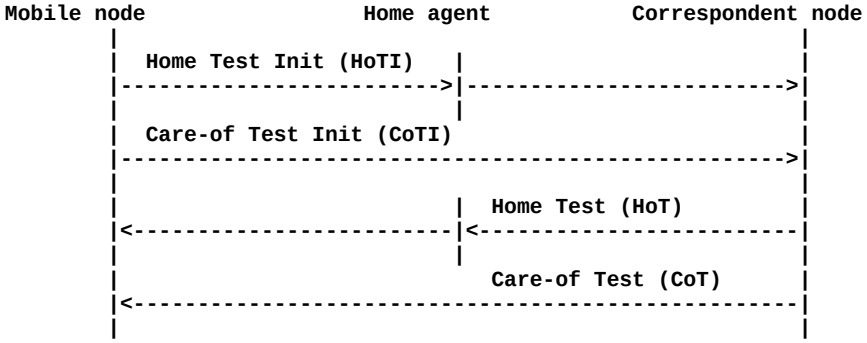
RFC Text:
The Return Routability Procedure enables the correspondent node to obtain some reasonable assurance that the mobile node is in fact addressable at its claimed care-of address as well as at its home address. Only with this assurance is the correspondent node able to accept Binding Updates from the mobile node which would then instruct the correspondent node to direct that mobile node's data traffic to its claimed care-of address.

This is done by testing whether packets addressed to the two claimed addresses are routed to the mobile node. The mobile node can pass the test only if it is able to supply proof that it received certain data (the "keygen tokens") which the correspondent node sends to those addresses. These data are combined by the mobile node into a binding management key, denoted Kbm.

Identifier: RQ_001_1048
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
To initiate the return routability procedure, the mobile node shall send the Home Test Init (HoTi) via the Home Agent and the Care-of Test Init (CoTi) message directly to the correspondernt node

RFC Text:
The figure below shows the message flow for the return routability procedure.

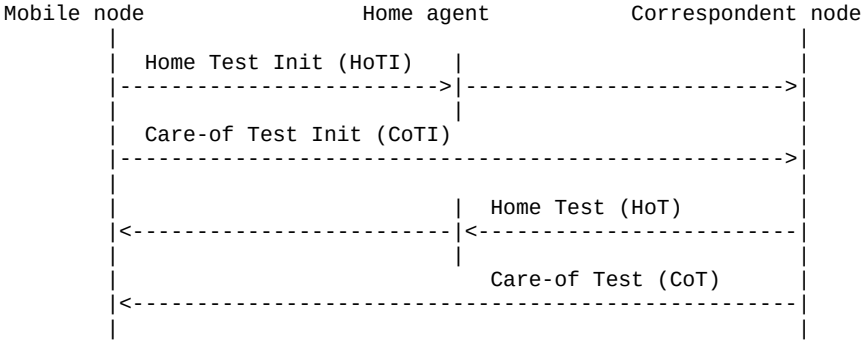


The Home and Care-of Test Init messages are sent at the same time. The procedure requires very little processing at the correspondent node, and the Home and Care-of Test messages can be returned quickly, perhaps nearly simultaneously. These four messages form the return routability procedure.

Identifier: RQ_001_1049
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the return routability procedure, the Home Test Init and Care-of Test Init messages shall be sent at the same time.

RFC Text:
The figure below shows the message flow for the return routability procedure.

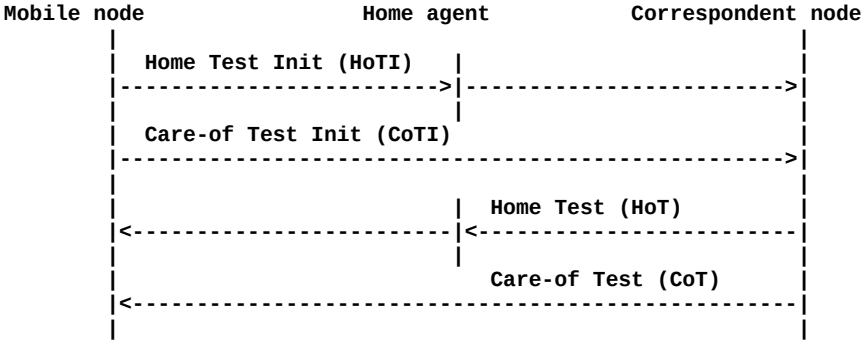


The Home and Care-of Test Init messages are sent at the same time. The procedure requires very little processing at the correspondent node, and the Home and Care-of Test messages can be returned quickly, perhaps nearly simultaneously. These four messages form the return routability procedure.

Identifier: RQ_001_1050
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the return routability procedure, on receipt of the Home test Init (HoTi) message, the Correspondant node shall respond with a Home Test (HoT) message.

RFC Text:
The figure below shows the message flow for the return routability procedure.

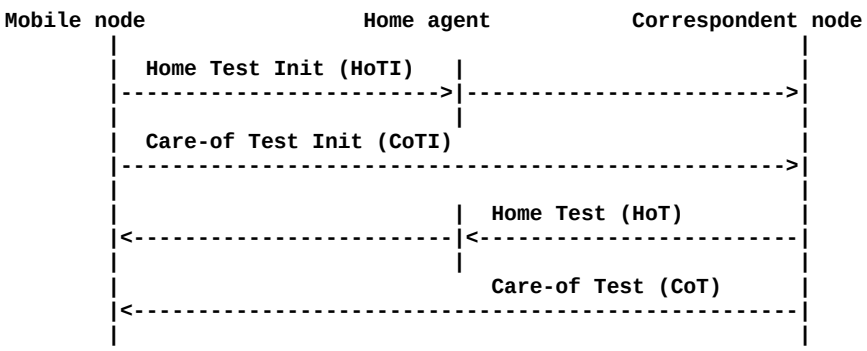


The Home and Care-of Test Init messages are sent at the same time. The procedure requires very little processing at the correspondent node, and the Home and Care-of Test messages can be returned quickly, perhaps nearly simultaneously. These four messages form the return routability procedure.

Identifier: RQ_001_1051
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the return routability procedure, on recept of the Care-of test Init (CoTi) message, the Correspondant node shall respond with a Care-of Test (CoT) message.

RFC Text:
The figure below shows the message flow for the return routability procedure.



The Home and Care-of Test Init messages are sent at the same time. The procedure requires very little processing at the correspondent node, and the Home and Care-of Test messages can be returned quickly, perhaps nearly simultaneously. These four messages form the return routability procedure.

Identifier: RQ_001_1052
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If, as a result of the return routability procedure, the mobile Node recieves both the HoT and CoT messages from the correspondent node, it shall take the "keygen tokens" which the correspondent node sends, and combines them into a binding management key, denoted Kbm.

RFC Text:
This is done by testing whether packets addressed to the two claimed addresses are routed to the mobile node. The mobile node can pass the test only if it is able to supply proof that it received certain data (the "keygen tokens") which the correspondent node sends to those addresses. These data are combined by the mobile node into a binding management key, denoted Kbm.

Identifier: RQ_001_1053
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:

The contents of the Home Test Init(HoTi) message shall be:
* Source Address = home address
* Destination Address = correspondent
* Parameters:
  + home init cookie

RFC Text:

A mobile node sends a Home Test Init message to the correspondent node (via the home agent) to acquire the home keygen token. **The contents of the message can be summarized as follows:**

*** Source Address = home address**

*** Destination Address = correspondent**

*** Parameters:**

+ home init cookie

The Home Test Init message conveys the mobile node's home address to the correspondent node. The mobile node also sends along a home init cookie that the correspondent node must return later. The Home Test Init message is reverse tunneled through the home agent. (The headers and addresses related to reverse tunneling have been omitted from the above discussion of the message contents.) The mobile node remembers these cookie values to obtain some assurance that its protocol messages are being processed by the desired correspondent node.

Identifier: RQ_001_1054
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:

The contents of the Care-of Test Init (CoTi) message shall be:
* Source Address = care-of address
* Destination Address = correspondent
* Parameters:
  + care-of init cookie

RFC Text:

The mobile node sends a Care-of Test Init message to the correspondent node (directly, not via the home agent) to acquire the care-of keygen token. **The contents of this message can be summarized as follows:**

*** Source Address = care-of address**

*** Destination Address = correspondent**

*** Parameters:**

+ care-of init cookie

The Care-of Test Init message conveys the mobile node's care-of address to the correspondent node. The mobile node also sends along a care-of init cookie that the correspondent node must return later. The Care-of Test Init message is sent directly to the correspondent node.

Identifier: RQ_001_1055
RFC Clause: 5.2.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The "home init cookie" and "care-of init cookie" are random 64 bit values

RFC Text:
The "home init cookie" and "care-of init cookie" are 64 bit values sent to the correspondent node from the mobile node, and later returned to the mobile node. The home init cookie is sent in the Home Test Init message, and returned in the Home Test message. The care-of init cookie is sent in the Care-of Test Init message, and returned in the Care-of Test message.

Identifier: RQ_001_1056
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The contents of the Home Test message message shall be:
* Source Address = correspondent
* Destination Address = home address
* Parameters:
  + home init cookie
  + home keygen token
  + home nonce index

RFC Text:
The Home Test message is sent in response to a Home Test Init message. It is sent via the home agent. The contents of the message are:

*** Source Address = correspondent**
*** Destination Address = home address**
*** Parameters:**
+ home init cookie
+ home keygen token
+ home nonce index

When the correspondent node receives the Home Test Init message, it generates a home keygen token as follows:

home keygen token := First (64, HMAC_SHA1 (Kcn, (home address | nonce | 0)))

where | denotes concatenation. The final "0" inside the HMAC_SHA1 function is a single zero octet, used to distinguish home and care-of cookies from each other.

The home keygen token is formed from the first 64 bits of the MAC. The home keygen token tests that the mobile node can receive were messages sent to its home address. Kcn is used in the production of home keygen token in order to allow the correspondent node to verify that it generated the home and care-of nonces, without forcing the correspondent node to remember a list of all tokens it has handed out.

The Home Test message is sent to the mobile node via the home network, where it is presumed that the home agent will tunnel the message to the mobile node. This means that the mobile node needs to already have sent a Binding Update to the home agent, so that the home agent will have received and authorized the new care-of address for the mobile node before the return routability procedure. For improved security, the data passed between the home agent and the mobile node is made immune to inspection and passive attacks. Such protection is gained by encrypting the home keygen token as it is tunneled from the home agent to the mobile node as specified in Section 10.4.6. The security properties of this additional security are discussed in Section 15.4.1.

The home init cookie from the mobile node is returned in the Home Test message, to ensure that the message comes from a node on the route between the home agent and the correspondent node.

The home nonce index is delivered to the mobile node to later allow the correspondent node to efficiently find the nonce value that it used in creating the home keygen token.

Identifier: RQ_001_1057
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The contents of the home keygen token shall be : First (64, HMAC_SHA1 (Kcn, (home address | nonce | 0)))

RFC Text:
The Home Test message is sent in response to a Home Test Init message. It is sent via the home agent. The contents of the message are:

* Source Address = correspondent
* Destination Address = home address
* Parameters:
  + home init cookie
  + home keygen token
  + home nonce index

When the correspondent node receives the Home Test Init message, it generates a home keygen token as follows:

home keygen token := First (64, HMAC_SHA1 (Kcn, (home address | nonce | 0)))

where | denotes concatenation. The final "0" inside the HMAC_SHA1 function is a single zero octet, used to distinguish home and care-of cookies from each other.

The home keygen token is formed from the first 64 bits of the MAC. The home keygen token tests that the mobile node can receive were messages sent to its home address. Kcn is used in the production of home keygen token in order to allow the correspondent node to verify that it generated the home and care-of nonces, without forcing the correspondent node to remember a list of all tokens it has handed out.

The Home Test message is sent to the mobile node via the home network, where it is presumed that the home agent will tunnel the message to the mobile node. This means that the mobile node needs to already have sent a Binding Update to the home agent, so that the home agent will have received and authorized the new care-of address for the mobile node before the return routability procedure. For improved security, the data passed between the home agent and the mobile node is made immune to inspection and passive attacks. Such protection is gained by encrypting the home keygen token as it is tunneled from the home agent to the mobile node as specified in Section 10.4.6. The security properties of this additional security are discussed in Section 15.4.1.

The home init cookie from the mobile node is returned in the Home Test message, to ensure that the message comes from a node on the route between the home agent and the correspondent node.

The home nonce index is delivered to the mobile node to later allow the correspondent node to efficiently find the nonce value that it used in creating the home keygen tonken.

Identifier: RQ_001_1058
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

The contents of theCare-of Test message message shall be:
* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + care-of init cookie
  + care-of keygen token
  + care-of nonce index

RFC Text:

Care-of Test

This message is sent in response to a Care-of Test Init message. This message is not sent via the home agent, it is sent directly to the mobile node. **The contents of the message are:**
* **Source Address = correspondent**
* **Destination Address = care-of address**
* **Parameters:**
  + **care-of init cookie**
  + **care-of keygen token**
  + **care-of nonce index**

When the correspondent node receives the Care-of Test Init message, it generates a care-of keygen token as follows:

care-of keygen token :=
First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1)))

Here, the final "1" inside the HMAC_SHA1 function is a single octet containing the hex value 0x01, and is used to distinguish home and care-of cookies from each other. The keygen token is formed from the first 64 bits of the MAC, and sent directly to the mobile node at its care-of address. The care-of init cookie from the Care-of Test Init message is returned to ensure that the message comes from a node on the route to the correspondent node.

The care-of nonce index is provided to identify the nonce used for the care-of keygen token. The home and care-of nonce indices MAY be the same, or different, in the Home and Care-of Test messages.

When the mobile node has received both the Home and Care-of Test messages, the return routability procedure is complete. As a result of the procedure, the mobile node has the data it needs to send a Binding Update to the correspondent node. The mobile node hashes the tokens together to form a 20 octet binding key Kbm:

Kbm = SHA1 (home keygen token | care-of keygen token)

A Binding Update may also be used to delete a previously established binding (Section 6.1.7). In this case, the care-of keygen token is not used. Instead, the binding management key is generated as follows:

Kbm = SHA1(home keygen token)

Note that the correspondent node does not create any state specific to the mobile node, until it receives the Binding Update from that mobile node. The correspondent node does not maintain the value for the binding management key Kbm; it creates Kbm when given the nonce indices and the mobile node's addresses.

Identifier: RQ_001_1059
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The contents of the Care-of keygen token shall be : First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1)))

RFC Text:
Care-of Test

This message is sent in response to a Care-of Test Init message. This message is not sent via the home agent, it is sent directly to the mobile node. The contents of the message are:

* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + care-of init cookie
  + care-of keygen token
  + care-of nonce index

When the correspondent node receives the Care-of Test Init message, it generates a care-of keygen token as follows:

care-of keygen token :=
First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1)))

Here, the final "1" inside the HMAC_SHA1 function is a single octet containing the hex value 0x01, and is used to distinguish home and care-of cookies from each other. The keygen token is formed from the first 64 bits of the MAC, and sent directly to the mobile node at its care-of address. The care-of init cookie from the Care-of Test Init message is returned to ensure that the message comes from a node on the route to the correspondent node.

The care-of nonce index is provided to identify the nonce used for the care-of keygen token. The home and care-of nonce indices MAY be the same, or different, in the Home and Care-of Test messages.

When the mobile node has received both the Home and Care-of Test messages, the return routability procedure is complete. As a result of the procedure, the mobile node has the data it needs to send a Binding Update to the correspondent node. The mobile node hashes the tokens together to form a 20 octet binding key Kbm:

Kbm = SHA1 (home keygen token | care-of keygen token)

A Binding Update may also be used to delete a previously established binding (Section 6.1.7). In this case, the care-of keygen token is not used. Instead, the binding management key is generated as follows:

Kbm = SHA1(home keygen token)

Note that the correspondent node does not create any state specific to the mobile node, until it receives the Binding Update from that mobile node. The correspondent node does not maintain the value for the binding management key Kbm; it creates Kbm when given the nonce indices and the mobile node's addresses.

Identifier: RQ_001_1060
RFC Clause: 5.2.5
Type: Optional
Applies to: Correspondent_Node

Requirement:
The home and care-of nonce indices MAY be the same in the Home and Care-of Test messages.

RFC Text:
Care-of Test

This message is sent in response to a Care-of Test Init message. This message is not sent via the home agent, it is sent directly to the mobile node. The contents of the message are:

* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + care-of init cookie
  + care-of keygen token
  + care-of nonce index

When the correspondent node receives the Care-of Test Init message, it generates a care-of keygen token as follows:

care-of keygen token :=
First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1)))

Here, the final "1" inside the HMAC_SHA1 function is a single octet containing the hex value 0x01, and is used to distinguish home and care-of cookies from each other. The keygen token is formed from the first 64 bits of the MAC, and sent directly to the mobile node at its care-of address. The care-of init cookie from the Care-of Test Init message is returned to ensure that the message comes from a node on the route to the correspondent node.

The care-of nonce index is provided to identify the nonce used for the care-of keygen token. **The home and care-of nonce indices MAY be the same, or different, in the Home and Care-of Test messages.**

When the mobile node has received both the Home and Care-of Test messages, the return routability procedure is complete. As a result of the procedure, the mobile node has the data it needs to send a Binding Update to the correspondent node. The mobile node hashes the tokens together to form a 20 octet binding key Kbm:

Kbm = SHA1 (home keygen token | care-of keygen token)

A Binding Update may also be used to delete a previously established binding (Section 6.1.7). In this case, the care-of keygen token is not used. Instead, the binding management key is generated as follows:

Kbm = SHA1(home keygen token)

Note that the correspondent node does not create any state specific to the mobile node, until it receives the Binding Update from that mobile node. The correspondent node does not maintain the value for the binding management key Kbm; it creates Kbm when given the nonce indices and the mobile node's addresses.

Identifier: RQ_001_1061
RFC Clause: 5.2.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:

When the mobile node has received both the Home and Care-of Test messages, the return routability procedure is complete. As a result of the procedure, the mobile node has the data it needs to send a Binding Update to the correspondent node. The mobile node hashes the tokens together to form a 20 octet binding key Kbm:

```
Kbm = SHA1 (home keygen token | care-of keygen token)
```

RFC Text:

Care-of Test

This message is sent in response to a Care-of Test Init message. This message is not sent via the home agent, it is sent directly to the mobile node. The contents of the message are:

* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + care-of init cookie
  + care-of keygen token
  + care-of nonce index

When the correspondent node receives the Care-of Test Init message, it generates a care-of keygen token as follows:

```
care-of keygen token :=
   First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1)))
```

Here, the final "1" inside the HMAC_SHA1 function is a single octet containing the hex value 0x01, and is used to distinguish home and care-of cookies from each other. The keygen token is formed from the first 64 bits of the MAC, and sent directly to the mobile node at its care-of address. The care-of init cookie from the Care-of Test Init message is returned to ensure that the message comes from a node on the route to the correspondent node.

The care-of nonce index is provided to identify the nonce used for the care-of keygen token. The home and care-of nonce indices MAY be the same, or different, in the Home and Care-of Test messages.

When the mobile node has received both the Home and Care-of Test messages, the return routability procedure is complete. As a result of the procedure, the mobile node has the data it needs to send a Binding Update to the correspondent node. The mobile node hashes the tokens together to form a 20 octet binding key Kbm:

Kbm = SHA1 (home keygen token | care-of keygen token)

A Binding Update may also be used to delete a previously established binding (Section 6.1.7). In this case, the care-of keygen token is not used. Instead, the binding management key is generated as follows:

```
Kbm = SHA1(home keygen token)
```

Note that the correspondent node does not create any state specific to the mobile node, until it receives the Binding Update from that mobile node. The correspondent node does not maintain the value for the binding management key Kbm; it creates Kbm when given the nonce indices and the mobile node's addresses.

Identifier: RQ_001_1062
RFC Clause: 5.2.5
Type: Optional
Applies to: Mobile_Node

Requirement:

A Binding Update MAY also be used to delete a previously established binding . In this case, the care-of keygen token is not used. Instead, the binding management key is generated as follows:

Kbm = SHA1(home keygen token)

RFC Text:

Care-of Test

This message is sent in response to a Care-of Test Init message. This message is not sent via the home agent, it is sent directly to the mobile node. The contents of the message are:

* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + care-of init cookie
  + care-of keygen token
  + care-of nonce index

When the correspondent node receives the Care-of Test Init message, it generates a care-of keygen token as follows:

care-of keygen token :=
First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1)))

Here, the final "1" inside the HMAC_SHA1 function is a single octet containing the hex value 0x01, and is used to distinguish home and care-of cookies from each other. The keygen token is formed from the first 64 bits of the MAC, and sent directly to the mobile node at its care-of address. The care-of init cookie from the Care-of Test Init message is returned to ensure that the message comes from a node on the route to the correspondent node.

The care-of nonce index is provided to identify the nonce used for the care-of keygen token. The home and care-of nonce indices MAY be the same, or different, in the Home and Care-of Test messages.

When the mobile node has received both the Home and Care-of Test messages, the return routability procedure is complete. As a result of the procedure, the mobile node has the data it needs to send a Binding Update to the correspondent node. The mobile node hashes the tokens together to form a 20 octet binding key Kbm:

Kbm = SHA1 (home keygen token | care-of keygen token)

A Binding Update may also be used to delete a previously established binding (Section 6.1.7). In this case, the care-of keygen token is not used. Instead, the binding management key is generated as follows:

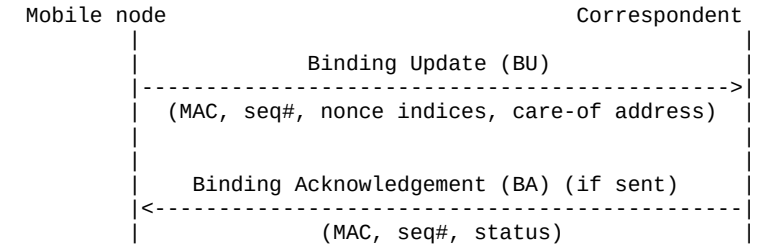
Kbm = SHA1(home keygen token)

Note that the correspondent node does not create any state specific to the mobile node, until it receives the Binding Update from that mobile node. The correspondent node does not maintain the value for the binding management key Kbm; it creates Kbm when given the nonce indices and the mobile node's addresses.

Identifier: RQ_001_1063
RFC Clause: 5.2.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
After the mobile node has created the binding management key (Kbm), it can supply a verifiable Binding Update to the correspondent node.

RFC Text:
After the mobile node has created the binding management key (Kbm), it can supply a verifiable Binding Update to the correspondent node. This section provides an overview of this registration.
The below figure shows the message flow.



Identifier: RQ_001_1064
RFC Clause: 5.2.6
Type: Mandatory
Applies to: Node

Requirement:
The contents of the Binding Update message message shall be:
* Source Address = care-of address
* Destination Address = correspondent
* Parameters:
  + home address (within the Home Address destination option if different from the Source Address)
  + sequence number (within the Binding Update message header)
  + home nonce index (within the Nonce Indices option)
  + care-of nonce index (within the Nonce Indices option)
  + First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BU)))

RFC Text:
To authorize a Binding Update, the mobile node creates a binding management key Kbm from the keygen tokens as described in the previous section. **The contents of the Binding Update include the following:**

*** Source Address = care-of address**
*** Destination Address = correspondent**
*** Parameters:**
+ home address (within the Home Address destination option if different from the Source Address)
+ sequence number (within the Binding Update message header)
+ home nonce index (within the Nonce Indices option)
+ care-of nonce index (within the Nonce Indices option)
+ First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BU)))

The Binding Update contains a Nonce Indices option, indicating to the correspondent node which home and care-of nonces to use to recompute Kbm, the binding management key. The MAC is computed as described in Section 6.2.7, using the correspondent node's address as the destination address and the Binding Update message itself ("BU" above) as the MH Data.

Once the correspondent node has verified the MAC, it can create a Binding Cache entry for the mobile.

Identifier: RQ_001_1064
RFC Clause: 5.2.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:

```
The  contents of the Binding Update  message  message shall be:
   *  Source Address = care-of address
      *  Destination Address = correspondent
      *  Parameters:
         +  home address (within the Home Address destination option if
            different from the Source Address)
         +  sequence number (within the Binding Update message header)
         +  home nonce index (within the Nonce Indices option)
         +  care-of nonce index (within the Nonce Indices option)
         +  First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
            | BU)))
```

RFC Text:

To authorize a Binding Update, the mobile node creates a binding management key Kbm from the keygen tokens as described in the previous section. **The contents of the Binding Update include the following:**

- **Source Address = care-of address**
- **Destination Address = correspondent**
- **Parameters:**
  - **home address (within the Home Address destination option if different from the Source Address)**
  - **sequence number (within the Binding Update message header)**
  - **home nonce index (within the Nonce Indices option)**
  - **care-of nonce index (within the Nonce Indices option)**
  - **First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BU)))**

The Binding Update contains a Nonce Indices option, indicating to the correspondent node which home and care-of nonces to use to recompute Kbm, the binding management key. The MAC is computed as described in Section 6.2.7, using the correspondent node's address as the destination address and the Binding Update message itself ("BU" above) as the MH Data.

Once the correspondent node has verified the MAC, it can create a Binding Cache entry for the mobile.

Identifier: RQ_001_1065
RFC Clause: 5.2.6
Type: Optional
Applies to: Correspondent_Node

Requirement:
In response to the binding update, the Correspondent node MAY send a "Binding Acknowledgement (BA)"

RFC Text:
The Binding Update is in some cases acknowledged by the correspondent node. The contents of the message are as follows:

* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + sequence number (within the Binding Update message header)
  + First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BA)))

The Binding Acknowledgement contains the same sequence number as the Binding Update. The MAC is computed as described in Section 6.2.7, using the correspondent node's address as the destination address and the message itself ("BA" above) as the MH Data.
Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFETIME seconds (see Section 12).

The value in the Source Address field in the IPv6 header carrying the Binding Update is normally also the care-of address which is used in the binding. However, a different care-of address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update (see Section 6.2.5). When such a message is sent to the correspondent node and the return routability procedure is used as the authorization method, the Care-of Test Init and Care-of Test messages MUST have been performed for the address in the Alternate Care-of Address option (not the Source Address). The nonce indices and MAC value MUST be based on information gained in this test.

Binding Updates may also be sent to delete a previously established binding. In this case, generation of the binding management key depends exclusively on the home keygen token and the care-of nonce index is ignored.

Identifier: RQ_001_1066
RFC Clause: 5.2.6
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

The contents of the "Binding Acknowledgement (BA)" message are as follows:
* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + sequence number (within the Binding Update message header)
  + First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BA)))

RFC Text:

The Binding Update is in some cases acknowledged by the correspondent node. The contents of the message are as follows:
* **Source Address = correspondent**
* **Destination Address = care-of address**
* **Parameters:**
  + **sequence number (within the Binding Update message header)**
  + **First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BA)))**

The Binding Acknowledgement contains the same sequence number as the Binding Update. The MAC is computed as described in Section 6.2.7, using the correspondent node's address as the destination address and the message itself ("BA" above) as the MH Data.
Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFETIME seconds (see Section 12).

The value in the Source Address field in the IPv6 header carrying the Binding Update is normally also the care-of address which is used in the binding. However, a different care-of address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update (see Section 6.2.5). When such a message is sent to the correspondent node and the return routability procedure is used as the authorization method, the Care-of Test Init and Care-of Test messages MUST have been performed for the address in the Alternate Care-of Address option (not the Source Address). The nonce indices and MAC value MUST be based on information gained in this test.

Binding Updates may also be sent to delete a previously established binding. In this case, generation of the binding management key depends exclusively on the home keygen token and the care-of nonce index is ignored.

Identifier: RQ_001_1067
RFC Clause: 5.2.6
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The "Binding Acknowledgement (BA)" Parameter "sequence number" contains the same sequence number as the Binding Update.

RFC Text:
The Binding Update is in some cases acknowledged by the correspondent node. The contents of the message are as follows:

```
      *  Source Address = correspondent
      *  Destination Address = care-of address
      *  Parameters:
         +  sequence number (within the Binding Update message header)
         +  First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
            | BA)))
```

The Binding Acknowledgement contains the same sequence number as the Binding Update. The MAC is computed as described in Section 6.2.7, using the correspondent node's address as the destination address and the message itself ("BA" above) as the MH Data.
Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFETIME seconds (see Section 12).

The value in the Source Address field in the IPv6 header carrying the Binding Update is normally also the care-of address which is used in the binding. However, a different care-of address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update (see Section 6.2.5). When such a message is sent to the correspondent node and the return routability procedure is used as the authorization method, the Care-of Test Init and Care-of Test messages MUST have been performed for the address in the Alternate Care-of Address option (not the Source Address). The nonce indices and MAC value MUST be based on information gained in this test.

Binding Updates may also be sent to delete a previously established binding. In this case, generation of the binding management key depends exclusively on the home keygen token and the care-of nonce index is ignored.

Identifier: RQ_001_1068
RFC Clause: 5.2.6
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFETIME (420 seconds).

RFC Text:
The Binding Update is in some cases acknowledged by the correspondent node. The contents of the message are as follows:

```
      *  Source Address = correspondent
      *  Destination Address = care-of address
      *  Parameters:
         +  sequence number (within the Binding Update message header)
         +  First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
            | BA)))
```

The Binding Acknowledgement contains the same sequence number as the Binding Update. The MAC is computed as described in Section 6.2.7, using the correspondent node's address as the destination address and the message itself ("BA" above) as the MH Data.
Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFETIME seconds (see Section 12).

The value in the Source Address field in the IPv6 header carrying the Binding Update is normally also the care-of address which is used in the binding. However, a different care-of address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update (see Section 6.2.5). When such a message is sent to the correspondent node and the return routability procedure is used as the authorization method, the Care-of Test Init and Care-of Test messages MUST have been performed for the address in the Alternate Care-of Address option (not the Source Address). The nonce indices and MAC value MUST be based on information gained in this test.

Binding Updates may also be sent to delete a previously established binding. In this case, generation of the binding management key depends exclusively on the home keygen token and the care-of nonce index is ignored.

Identifier: RQ_001_1068
RFC Clause: 5.2.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFETIME (420 seconds).

RFC Text:
The Binding Update is in some cases acknowledged by the correspondent node. The contents of the message are as follows:

* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + sequence number (within the Binding Update message header)
  + First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BA)))

The Binding Acknowledgement contains the same sequence number as the Binding Update. The MAC is computed as described in Section 6.2.7, using the correspondent node's address as the destination address and the message itself ("BA" above) as the MH Data.
Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFETIME seconds (see Section 12).

The value in the Source Address field in the IPv6 header carrying the Binding Update is normally also the care-of address which is used in the binding. However, a different care-of address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update (see Section 6.2.5). When such a message is sent to the correspondent node and the return routability procedure is used as the authorization method, the Care-of Test Init and Care-of Test messages MUST have been performed for the address in the Alternate Care-of Address option (not the Source Address). The nonce indices and MAC value MUST be based on information gained in this test.

Binding Updates may also be sent to delete a previously established binding. In this case, generation of the binding management key depends exclusively on the home keygen token and the care-of nonce index is ignored.

Identifier: RQ_001_1069
RFC Clause: 5.2.6
Type: Optional
Applies to: Mobile_Node

Requirement:
Although the value in the Source Address field in the IPv6 header carrying the Binding Update is normally also the care-of address which is used in the binding, a different care-of address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update.

RFC Text:
The Binding Update is in some cases acknowledged by the correspondent node. The contents of the message are as follows:

* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + sequence number (within the Binding Update message header)
  + First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BA)))

The Binding Acknowledgement contains the same sequence number as the Binding Update. The MAC is computed as described in Section 6.2.7, using the correspondent node's address as the destination address and the message itself ("BA" above) as the MH Data.
Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFETIME seconds (see Section 12).

The value in the Source Address field in the IPv6 header carrying the Binding Update is normally also the care-of address which is used in the binding. However, a different care-of address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update (see Section 6.2.5). When such a message is sent to the correspondent node and the return routability procedure is used as the authorization method, the Care-of Test Init and Care-of Test messages MUST have been performed for the address in the Alternate Care-of Address option (not the Source Address). The nonce indices and MAC value MUST be based on information gained in this test.

Binding Updates may also be sent to delete a previously established binding. In this case, generation of the binding management key depends exclusively on the home keygen token and the care-of nonce index is ignored.

Identifier: RQ_001_1070
RFC Clause: 5.2.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When an Alternate Care-of Address mobility option is included in the Binding Update and is sent to the correspondent node and the return routability procedure is used as the authorization method. The Care-of Test Init and Care-of Test messages MUST have been performed for the address in the Alternate Care-of Address option (not the Source Address). The nonce indices and MAC value MUST be based on information gained in this test.

RFC Text:
The Binding Update is in some cases acknowledged by the correspondent node. The contents of the message are as follows:

* Source Address = correspondent
* Destination Address = care-of address
* Parameters:
  + sequence number (within the Binding Update message header)
  + First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BA)))

The Binding Acknowledgement contains the same sequence number as the Binding Update. The MAC is computed as described in Section 6.2.7, using the correspondent node's address as the destination address and the message itself ("BA" above) as the MH Data.
Bindings established with correspondent nodes using keys created by way of the return routability procedure MUST NOT exceed MAX_RR_BINDING_LIFETIME seconds (see Section 12).

The value in the Source Address field in the IPv6 header carrying the Binding Update is normally also the care-of address which is used in the binding. However, a different care-of address MAY be specified by including an Alternate Care-of Address mobility option in the Binding Update (see Section 6.2.5). **When such a message is sent to the correspondent node and the return routability procedure is used as the authorization method, the Care-of Test Init and Care-of Test messages MUST have been performed for the address in the Alternate Care-of Address option (not the Source Address). The nonce indices and MAC value MUST be based on information gained in this test.**

Binding Updates may also be sent to delete a previously established binding. In this case, generation of the binding management key depends exclusively on the home keygen token and the care-of nonce index is ignored.

Identifier: RQ_001_1071
RFC Clause: 5.2.7
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
It is recommended to keep each nonce (identified by a nonce index) acceptable for at least MAX_TOKEN_LIFETIME (210 seconds) after it has been first used in constructing a return routability message response.

RFC Text:
Correspondent nodes generate nonces at regular intervals. **It is recommended to keep each nonce (identified by a nonce index) acceptable for at least MAX_TOKEN_LIFETIME seconds (see Section 12) after it has been first used in constructing a return routability message response.** However, the correspondent node MUST NOT accept nonces beyond MAX_NONCE_LIFETIME seconds (see Section 12) after the first use. As the difference between these two constants is 30 seconds, a convenient way to enforce the above lifetimes is to generate a new nonce every 30 seconds. The node can then continue to accept tokens that have been based on the last 8 (MAX_NONCE_LIFETIME / 30) nonces. This results in tokens being acceptable MAX_TOKEN_LIFETIME to MAX_NONCE_LIFETIME seconds after they have been sent to the mobile node, depending on whether the token was sent at the beginning or end of the first 30 second period. Note that the correspondent node may also attempt to generate new nonces on demand, or only if the old nonces have been used. This is possible, as long as the correspondent node keeps track of how long a time ago the nonces were used for the first time, and does not generate new nonces on every return routability request.

Identifier: RQ_001_1072
RFC Clause: 5.2.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The correspondent node MUST NOT accept nonces beyond MAX_NONCE_LIFETIME seconds (240 seconds) after the first use

RFC Text:
Correspondent nodes generate nonces at regular intervals. It is recommended to keep each nonce (identified by a nonce index) acceptable for at least MAX_TOKEN_LIFETIME seconds (see Section 12) after it has been first used in constructing a return routability message response. **However, the correspondent node MUST NOT accept nonces beyond MAX_NONCE_LIFETIME seconds (see Section 12) after the first use.** As the difference between these two constants is 30 seconds, a convenient way to enforce the above lifetimes is to generate a new nonce every 30 seconds. The node can then continue to accept tokens that have been based on the last 8 (MAX_NONCE_LIFETIME / 30) nonces. This results in tokens being acceptable MAX_TOKEN_LIFETIME to MAX_NONCE_LIFETIME seconds after they have been sent to the mobile node, depending on whether the token was sent at the beginning or end of the first 30 second period. Note that the correspondent node may also attempt to generate new nonces on demand, or only if the old nonces have been used. This is possible, as long as the correspondent node keeps track of how long a time ago the nonces were used for the first time, and does not generate new nonces on every return routability request.

Identifier: RQ_001_1073
RFC Clause: 5.2.7
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
To avoid nonces being rejected as "beyond MAX_NONCE_LIFETIME" a convenient way is to generate a new nonce every 30 seconds. The node can then continue to accept tokens that have been based on the last 8 nonces.

RFC Text:
Correspondent nodes generate nonces at regular intervals. It is recommended to keep each nonce (identified by a nonce index) acceptable for at least MAX_TOKEN_LIFETIME seconds (see Section 12) after it has been first used in constructing a return routability message response. However, the correspondent node MUST NOT accept nonces beyond MAX_NONCE_LIFETIME seconds (see Section 12) after the first use. **As the difference between these two constants is 30 seconds, a convenient way to enforce the above lifetimes is to generate a new nonce every 30 seconds. The node can then continue to accept tokens that have been based on the last 8 (MAX_NONCE_LIFETIME / 30) nonces.** This results in tokens being acceptable MAX_TOKEN_LIFETIME to MAX_NONCE_LIFETIME seconds after they have been sent to the mobile node, depending on whether the token was sent at the beginning or end of the first 30 second period. Note that the correspondent node may also attempt to generate new nonces on demand, or only if the old nonces have been used. This is possible, as long as the correspondent node keeps track of how long a time ago the nonces were used for the first time, and does not generate new nonces on every return routability request.

Identifier: RQ_001_1074
RFC Clause: 5.2.7
Type: Optional
Applies to: Correspondent_Node

Requirement:
If the correspondent node keeps track of how long a time ago the nonces were used for the first time, and does not generate new nonces on every return routability request, the correspondent node MAY also attempt to generate new nonces on demand, or only if the old nonces have been used.

RFC Text:
Correspondent nodes generate nonces at regular intervals. It is recommended to keep each nonce (identified by a nonce index) acceptable for at least MAX_TOKEN_LIFETIME seconds (see Section 12) after it has been first used in constructing a return routability message response. However, the correspondent node MUST NOT accept nonces beyond MAX_NONCE_LIFETIME seconds (see Section 12) after the first use. As the difference between these two constants is 30 seconds, a convenient way to enforce the above lifetimes is to generate a new nonce every 30 seconds. The node can then continue to accept tokens that have been based on the last 8 (MAX_NONCE_LIFETIME / 30) nonces. This results in tokens being acceptable MAX_TOKEN_LIFETIME to MAX_NONCE_LIFETIME seconds after they have been sent to the mobile node, depending on whether the token was sent at the beginning or end of the first 30 second period. **Note that the correspondent node may also attempt to generate new nonces on demand, or only if the old nonces have been used. This is possible, as long as the correspondent node keeps track of how long a time ago the nonces were used for the first time, and does not generate new nonces on every return routability request.**

Identifier: RQ_001_1075
RFC Clause: 5.2.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If, due to resource limitations, rapid deletion of bindings, or reboots, a nonce index is unrecognized, the correspondent node replies with an error code in the Binding Acknowledgement (either 136, 137, or 138).

RFC Text:
Due to resource limitations, rapid deletion of bindings, or reboots the correspondent node may not in all cases recognize the nonces that the tokens were based on. If a nonce index is unrecognized, the correspondent node replies with an error code in the Binding Acknowledgement (either 136, 137, or 138 as discussed in Section 6.1.8). The mobile node can then retry the return routability procedure.

Identifier: RQ_001_1076
RFC Clause: 5.2.7
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
An update of Kcn SHOULD be done at the same time as an update of a nonce, so that nonce indices can identify both the nonce and the key. Old Kcn values have to be therefore remembered as long as old nonce values.

RFC Text:
An update of Kcn SHOULD be done at the same time as an update of a nonce, so that nonce indices can identify both the nonce and the key. Old Kcn values have to be therefore remembered as long as old nonce values.

Identifier: RQ_001_1076
RFC Clause: 5.2.7
Type: Recommendation
Applies to: Mobile_Node

Requirement:
An update of Kcn SHOULD be done at the same time as an update of a nonce, so that nonce indices can identify both the nonce and the key. Old Kcn values have to be therefore remembered as long as old nonce values.

RFC Text:
An update of Kcn SHOULD be done at the same time as an update of a nonce, so that nonce indices can identify both the nonce and the key. Old Kcn values have to be therefore remembered as long as old nonce values.

Identifier: RQ_001_1077
RFC Clause: 5.2.7
Type: Optional
Applies to: Mobile_Node

Requirement:
Given that the tokens are normally expected to be usable for MAX_TOKEN_LIFETIME (210 seconds), the mobile node MAY use them beyond a single run of the return routability procedure until MAX_TOKEN_LIFETIME (210 seconds) expires.

RFC Text:
Given that the tokens are normally expected to be usable for MAX_TOKEN_LIFETIME seconds, the mobile node MAY use them beyond a single run of the return routability procedure until MAX_TOKEN_LIFETIME expires. After this the mobile node SHOULD NOT use the tokens. A fast moving mobile node MAY reuse a recent home keygen token from a correspondent node when moving to a new location, and just acquire a new care-of keygen token to show routability in the new location.

Identifier: RQ_001_1078
RFC Clause: 5.2.7
Type: Recommendation
Applies to: Mobile_Node

Requirement:
After the MAX_TOKEN_LIFETIME (210 seconds) expires, the mobile node SHOULD NOT use the tokens. A fast moving mobile node MAY reuse a recent home keygen token from a correspondent node when moving to a new location, and just acquire a new care-of keygen token to show routability in the new location.

RFC Text:
Given that the tokens are normally expected to be usable for MAX_TOKEN_LIFETIME seconds, the mobile node MAY use them beyond a single run of the return routability procedure until MAX_TOKEN_LIFETIME expires. **After this the mobile node SHOULD NOT use the tokens. A fast moving mobile node MAY reuse a recent home keygen token from a correspondent node when moving to a new location, and just acquire a new care-of keygen token to show routability in the new location.**

Identifier: RQ_001_1079
RFC Clause: 5.2.7
Type: Optional
Applies to: Mobile_Node

Requirement:
A mobile node that has multiple home addresses, MAY use the same care-of keygen token for Binding Updates concerning all of these addresses.

RFC Text:
While this does not save the number of round-trips due to the simultaneous processing of home and care-of return routability tests, there are fewer messages being exchanged, and a potentially long round-trip through the home agent is avoided. Consequently, this optimization is often useful. **A mobile node that has multiple home addresses, MAY also use the same care-of keygen token for Binding Updates concerning all of these addresses.**

Identifier: RQ_001_1080
RFC Clause: 5.2.8
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent nodes MUST retain bindings and the associated sequence number information at least as long as the nonces used in the authorization of the binding are still valid.

RFC Text:
The return routability procedure also protects the participants against replayed Binding Updates through the use of the sequence number and a MAC. Care must be taken when removing bindings at the correspondent node, however. **Correspondent nodes must retain bindings and the associated sequence number information at least as long as the nonces used in the authorization of the binding are still valid.** Alternatively, if memory is very constrained, the correspondent node MAY invalidate the nonces that were used for the binding being deleted (or some larger group of nonces that they belong to). This may, however, impact the ability to accept Binding Updates from mobile nodes that have recently received keygen tokens.This alternative is therefore recommended only as a last measure.

Identifier: RQ_001_1081
RFC Clause: 5.2.8
Type: Optional
Applies to: Correspondent_Node

Requirement:
If memory is very constrained, the correspondent node MAY invalidate the nonces that were used for the binding being deleted (or some larger group of nonces that they belong to). This alternative is therefore recommended only as a last measure.

RFC Text:
The return routability procedure also protects the participants against replayed Binding Updates through the use of the sequence number and a MAC. Care must be taken when removing bindings at the correspondent node, however. Correspondent nodes must retain bindings and the associated sequence number information at least as long as the nonces used in the authorization of the binding are still valid. Alternatively, **if memory is very constrained, the correspondent node MAY invalidate the nonces that were used for the binding being deleted (or some larger group of nonces that they belong to). This may, however, impact the ability to accept Binding Updates from mobile nodes that have recently received keygen tokens.This alternative is therefore recommended only as a last measure.**

Identifier: RQ_001_1082
RFC Clause: 5.4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The mobile node and the home agent SHOULD use an IPsec security association to protect the integrity and authenticity of the Mobile Prefix Solicitations and Advertisements.

RFC Text:
The mobile node and the home agent SHOULD use an IPsec security association to protect the integrity and authenticity of the Mobile Prefix Solicitations and Advertisements. Both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode with a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

Identifier: RQ_001_1083
RFC Clause: 5.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Both the mobile nodes and the home agents MUST support the Encapsulating Security Payload (ESP) header in transport mode with a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

RFC Text:
The mobile node and the home agent SHOULD use an IPsec security association to protect the integrity and authenticity of the Mobile Prefix Solicitations and Advertisements **Both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode with a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.**

Identifier: RQ_001_1083
RFC Clause: 5.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Both the mobile nodes and the home agents MUST support the Encapsulating Security Payload (ESP) header in transport mode with a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

RFC Text:
The mobile node and the home agent SHOULD use an IPsec security association to protect the integrity and authenticity of the Mobile Prefix Solicitations and Advertisements **Both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode with a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.**

Identifier: RQ_001_1085
RFC Clause: 5.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Payload packets exchanged with mobile nodes SHALL be protected, either, in the same way as stationary hosts can protect them or, using the Home Address destination option, a routing header, and tunneling headers in the payload packets.

RFC Text:
Payload packets exchanged with mobile nodes can be protected in the usual manner, in the same way as stationary hosts can protect them. However, Mobile IPv6 introduces the Home Address destination option, a routing header, and tunneling headers in the payload packets. In the following we define the security measures taken to protect these, and to prevent their use in attacks against other parties.

Identifier: RQ_001_1085
RFC Clause: 5.5
Type: Mandatory
Applies to: Home_Agent

Requirement:
Payload packets exchanged with mobile nodes SHALL be protected, either, in the same way as stationary hosts can protect them or, using the Home Address destination option, a routing header, and tunneling headers in the payload packets.

RFC Text:
Payload packets exchanged with mobile nodes can be protected in the usual manner, in the same way as stationary hosts can protect them. However, Mobile IPv6 introduces the Home Address destination option, a routing header, and tunneling headers in the payload packets. In the following we define the security measures taken to protect these, and to prevent their use in attacks against other parties.

Identifier: RQ_001_1086
RFC Clause: 5.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The use of the Home Address destination option is limited to the situation where the correspondent node already has a Binding Cache entry for the given home address

RFC Text:
This specification limits the use of the Home Address destination option to the situation where the correspondent node already has a Binding Cache entry for the given home address. This avoids the use of the Home Address option in attacks described in Section 15.1.

Identifier: RQ_001_1086
RFC Clause: 5.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The use of the Home Address destination option is limited to the situation where the correspondent node already has a Binding Cache entry for the given home address

RFC Text:
This specification limits the use of the Home Address destination option to the situation where the correspondent node already has a Binding Cache entry for the given home address. This avoids the use of the Home Address option in attacks described in Section 15.1.

Identifier: RQ_001_1087
RFC Clause: 5.5
Type: Optional
Applies to: Home_Agent

Requirement:
For traffic tunneled via the home agent, additional IPsec ESP encapsulation MAY be supported and used

RFC Text:
For traffic tunneled via the home agent, additional IPsec ESP encapsulation MAY be supported and used. If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported.

Identifier: RQ_001_1088
RFC Clause: 5.5
Type: Mandatory
Applies to: Home_Agent

Requirement:
If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported.

RFC Text:
For traffic tunneled via the home agent, additional IPsec ESP encapsulation MAY be supported and used. **If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported.**

Identifier: RQ_001_1089
RFC Clause: 6.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Mobility Header messages MUST ONLY be sent with a type 2 routing header for Binding Acknowledgement.

RFC Text:
Mobility Header messages MUST NOT be sent with a type 2 routing header, except as described in Section 9.5.4 for Binding Acknowledgement. Mobility Header messages also MUST NOT be used with a Home Address destination option, except as described in Section 11.7.1 and Section 11.7.2 for Binding Update. Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages. That is, Mobility Header messages bypass both the Binding Cache check described in Section 9.3.2 and the Binding Update List check described in Section

Identifier: RQ_001_1089
RFC Clause: 6.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Mobility Header messages MUST ONLY be sent with a type 2 routing header for Binding Acknowledgement.

RFC Text:
Mobility Header messages MUST NOT be sent with a type 2 routing header, except as described in Section 9.5.4 for Binding Acknowledgement. Mobility Header messages also MUST NOT be used with a Home Address destination option, except as described in Section 11.7.1 and Section 11.7.2 for Binding Update. Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages. That is, Mobility Header messages bypass both the Binding Cache check described in Section 9.3.2 and the Binding Update List check described in Section

Identifier: RQ_001_1089
RFC Clause: 6.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Mobility Header messages MUST ONLY be sent with a type 2 routing header for Binding Acknowledgement.

RFC Text:
Mobility Header messages MUST NOT be sent with a type 2 routing header, except as described in Section 9.5.4 for Binding Acknowledgement. Mobility Header messages also MUST NOT be used with a Home Address destination option, except as described in Section 11.7.1 and Section 11.7.2 for Binding Update. Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages. That is, Mobility Header messages bypass both the Binding Cache check described in Section 9.3.2 and the Binding Update List check described in Section

Identifier: RQ_001_1090
RFC Clause: 6.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Mobility Header messages MUST ONLY be used with a Home Address destination option for Binding Update

RFC Text:
Mobility Header messages MUST NOT be sent with a type 2 routing header, except as described in Section 9.5.4 for Binding Acknowledgement. **Mobility Header messages also MUST NOT be used with a Home Address destination option, except as described in Section 11.7.1 and Section 11.7.2 for Binding Update.** Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages. That is, Mobility Header messages bypass both the Binding Cache check described in Section 9.3.2 and the Binding Update List check described in Section

Identifier: RQ_001_1090
RFC Clause: 6.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Mobility Header messages MUST ONLY be used with a Home Address destination option for Binding Update

RFC Text:
Mobility Header messages MUST NOT be sent with a type 2 routing header, except as described in Section 9.5.4 for Binding Acknowledgement. **Mobility Header messages also MUST NOT be used with a Home Address destination option, except as described in Section 11.7.1 and Section 11.7.2 for Binding Update.** Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages. That is, Mobility Header messages bypass both the Binding Cache check described in Section 9.3.2 and the Binding Update List check described in Section

Identifier: RQ_001_1090
RFC Clause: 6.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Mobility Header messages MUST ONLY be used with a Home Address destination option for Binding Update

RFC Text:
Mobility Header messages MUST NOT be sent with a type 2 routing header, except as described in Section 9.5.4 for Binding Acknowledgement. **Mobility Header messages also MUST NOT be used with a Home Address destination option, except as described in Section 11.7.1 and Section 11.7.2 for Binding Update.** Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages. That is, Mobility Header messages bypass both the Binding Cache check described in Section 9.3.2 and the Binding Update List check described in Section

Identifier: RQ_001_1091
RFC Clause: 6.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages.

RFC Text:
Mobility Header messages MUST NOT be sent with a type 2 routing header, except as described in Section 9.5.4 for Binding Acknowledgement. Mobility Header messages also MUST NOT be used with a Home Address destination option, except as described in Section 11.7.1 and Section 11.7.2 for Binding Update. **Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages.** That is, Mobility Header messages bypass both the Binding Cache check described in Section 9.3.2 and the Binding Update List check described in Section

Identifier: RQ_001_1091
RFC Clause: 6.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages.

RFC Text:
Mobility Header messages MUST NOT be sent with a type 2 routing header, except as described in Section 9.5.4 for Binding Acknowledgement. Mobility Header messages also MUST NOT be used with a Home Address destination option, except as described in Section 11.7.1 and Section 11.7.2 for Binding Update. **Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages.** That is, Mobility Header messages bypass both the Binding Cache check described in Section 9.3.2 and the Binding Update List check described in Section

Identifier: RQ_001_1091
RFC Clause: 6.1
Type: Mandatory
Applies to: Mobile_Node

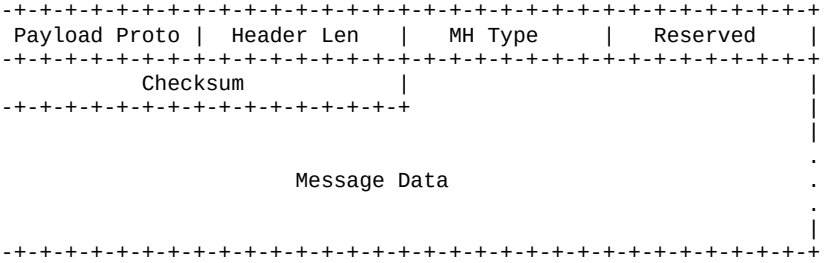
Requirement:
Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages.

RFC Text:
Mobility Header messages MUST NOT be sent with a type 2 routing header, except as described in Section 9.5.4 for Binding Acknowledgement. Mobility Header messages also MUST NOT be used with a Home Address destination option, except as described in Section 11.7.1 and Section 11.7.2 for Binding Update. **Binding Update List or Binding Cache information (when present) for the destination MUST NOT be used in sending Mobility Header messages.** That is, Mobility Header messages bypass both the Binding Cache check described in Section 9.3.2 and the Binding Update List check described in Section

Identifier: RQ_001_1092
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Mobility Header SHALL BE identified by a Next Header value of 135 in the immediately preceding header

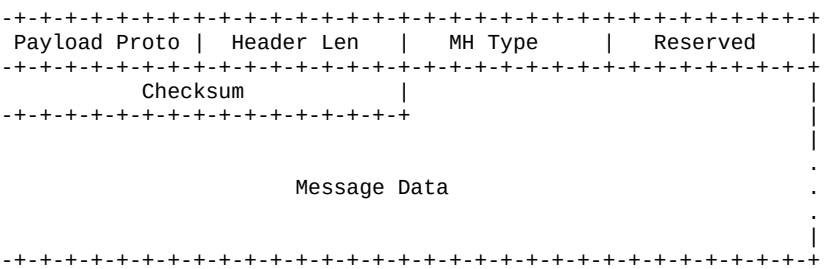
RFC Text:
The Mobility Header is identified by a Next Header value of 135 in the immediately preceding header, and has the following format:



Identifier: RQ_001_1092
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Mobility Header SHALL BE identified by a Next Header value of 135 in the immediately preceding header

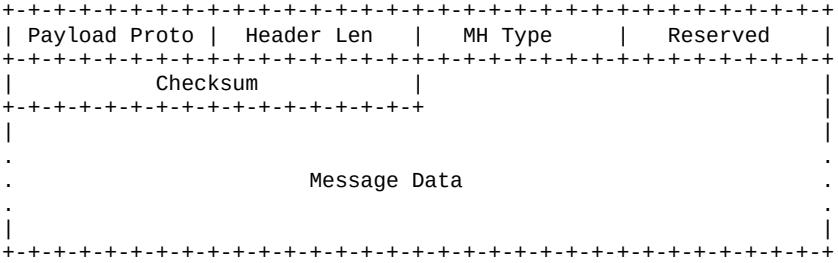
RFC Text:
The Mobility Header is identified by a Next Header value of 135 in the immediately preceding header, and has the following format:



Identifier: RQ_001_1092
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Mobility Header SHALL BE identified by a Next Header value of 135 in the immediately preceding header

RFC Text:
The Mobility Header is identified by a Next Header value of 135 in the immediately preceding header, and has the following format:

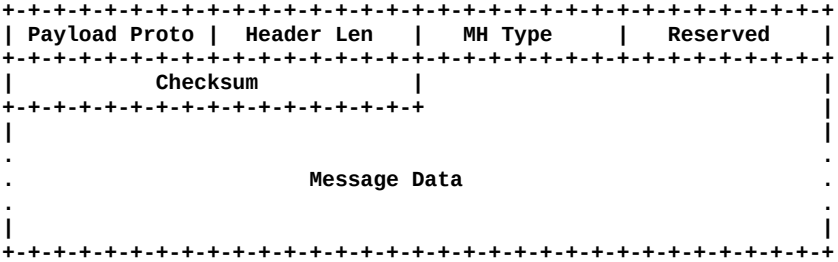


Identifier: RQ_001_1093
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Mobility Header SHALL have the following format;

Bit	Field
1 - 8	Payload Pro,
9 - 16	Header Len,
17 - 24	MH Type,
25 - 32	Reserved,
33 - 48	Checksum
49 - end	Message data fields.

RFC Text:
The Mobility Header is identified by a Next Header value of 135 in the immediately preceding header, and has the following format:

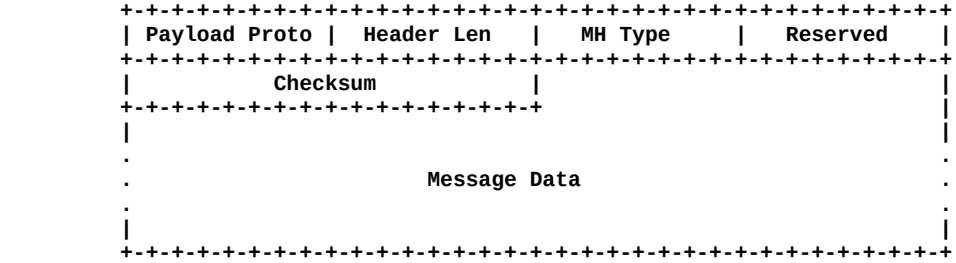


Identifier: RQ_001_1093
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Mobility Header SHALL have the following format;

```
Bit              Field
---------------------------------
1 - 8                  Payload Pro,
9 - 16                Header Len,
17 - 24              MH Type,
25 - 32              Reserved,
33 - 48              Checksum
49 - end            Message data fields.
```

RFC Text:
The Mobility Header is identified by a Next Header value of 135 in the immediately preceding header, and has the following format:

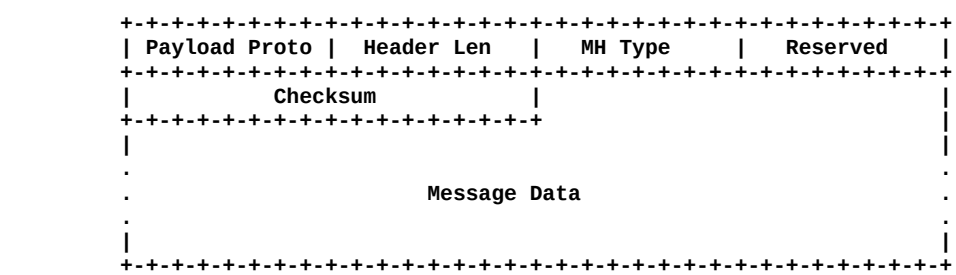


Identifier: RQ_001_1093
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Mobility Header SHALL have the following format;

```
Bit              Field
---------------------------------
1 - 8                  Payload Pro,
9 - 16                Header Len,
17 - 24              MH Type,
25 - 32              Reserved,
33 - 48              Checksum
49 - end            Message data fields.
```

RFC Text:
The Mobility Header is identified by a Next Header value of 135 in the immediately preceding header, and has the following format:



Identifier: RQ_001_1094
RFC Clause: 6.1.1
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
The Mobility Header's, Payload Proto field (payload protocol) is an 8-bit selector and SHOULD set the type to IPPROTO_NONE (59 decimal).

RFC Text:
8-bit selector. Identifies the type of header immediately following the Mobility Header. Uses the same values as the IPv6 Next Header field [11].
This field is intended to be used by a future extension (see Appendix B.1).
Implementations conforming to this specification SHOULD set the payload protocol type to IPPROTO_NONE (59 decimal).

Identifier: RQ_001_1094
RFC Clause: 6.1.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
The Mobility Header's, Payload Proto field (payload protocol) is an 8-bit selector and SHOULD set the type to IPPROTO_NONE (59 decimal).

RFC Text:
8-bit selector. Identifies the type of header immediately following the Mobility Header. Uses the same values as the IPv6 Next Header field [11].
This field is intended to be used by a future extension (see Appendix B.1).
Implementations conforming to this specification SHOULD set the payload protocol type to IPPROTO_NONE (59 decimal).

Identifier: RQ_001_1094
RFC Clause: 6.1.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The Mobility Header's, Payload Proto field (payload protocol) is an 8-bit selector and SHOULD set the type to IPPROTO_NONE (59 decimal).

RFC Text:
8-bit selector. Identifies the type of header immediately following the Mobility Header. Uses the same values as the IPv6 Next Header field [11].
This field is intended to be used by a future extension (see Appendix B.1).
Implementations conforming to this specification SHOULD set the payload protocol type to IPPROTO_NONE (59 decimal).

Identifier: RQ_001_1095
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Mobility Header's, Header Len field MUST be an 8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

RFC Text:
8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

The length of the Mobility Header MUST be a multiple of 8 octets.

Identifier: RQ_001_1095
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Mobility Header's, Header Len field MUST be an 8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

RFC Text:
8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

The length of the Mobility Header MUST be a multiple of 8 octets.

Identifier: RQ_001_1095
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Mobility Header's, Header Len field MUST be an 8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

RFC Text:
8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

The length of the Mobility Header MUST be a multiple of 8 octets.

Identifier: RQ_001_1096
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The length of the Mobility Header field MUST be a multiple of 8 octets.

RFC Text:
8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

The length of the Mobility Header MUST be a multiple of 8 octets.

Identifier: RQ_001_1096
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The length of the Mobility Header field MUST be a multiple of 8 octets.

RFC Text:
8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

The length of the Mobility Header MUST be a multiple of 8 octets.

Identifier: RQ_001_1096
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The length of the Mobility Header field MUST be a multiple of 8 octets.

RFC Text:
8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets.

The length of the Mobility Header MUST be a multiple of 8 octets.

Identifier: RQ_001_1097
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Mobility Header's, MH Type field (Message Header Type) is represented by an 8-bit selector

RFC Text:
8-bit selector. Identifies the particular mobility message in question. Current values are specified in Section 6.1.2 and onward. An unrecognized MH Type field causes an error indication to be sent.

Identifier: RQ_001_1097
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Mobility Header's, MH Type field (Message Header Type) is represented by an 8-bit selector

RFC Text:
8-bit selector. Identifies the particular mobility message in question. Current values are specified in Section 6.1.2 and onward. An unrecognized MH Type field causes an error indication to be sent.

Identifier: RQ_001_1097
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Mobility Header's, MH Type field (Message Header Type) is represented by an 8-bit selector

RFC Text:
8-bit selector. Identifies the particular mobility message in question. Current values are specified in Section 6.1.2 and onward. An unrecognized MH Type field causes an error indication to be sent.

Identifier: RQ_001_1098
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
An unrecognized MH Type (Message Header Type) field in the Mobility Header causes an error indication to be sent.

RFC Text:
8-bit selector. Identifies the particular mobility message in question. Current values are specified in Section 6.1.2 and onward. **An unrecognized MH Type field causes an error indication to be sent.**

Identifier: RQ_001_1098
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
An unrecognized MH Type (Message Header Type) field in the Mobility Header causes an error indication to be sent.

RFC Text:
8-bit selector. Identifies the particular mobility message in question. Current values are specified in Section 6.1.2 and onward. **An unrecognized MH Type field causes an error indication to be sent.**

Identifier: RQ_001_1098
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
An unrecognized MH Type (Message Header Type) field in the Mobility Header causes an error indication to be sent.

RFC Text:
8-bit selector. Identifies the particular mobility message in question. Current values are specified in Section 6.1.2 and onward. **An unrecognized MH Type field causes an error indication to be sent.**

Identifier: RQ_001_1099
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Mobility Header's, Reserved field MUST be an 8-bit field initialized to zero by the sender.

RFC Text:
8-bit field reserved for future use. The value MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1099
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Mobility Header's, Reserved field MUST be an 8-bit field initialized to zero by the sender.

RFC Text:
8-bit field reserved for future use. The value MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1099
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Mobility Header's, Reserved field MUST be an 8-bit field initialized to zero by the sender.

RFC Text:
8-bit field reserved for future use. The value MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1100
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The value of the Mobility Header's, Reserved field MUST be ignored by the receiver.

RFC Text:
8-bit field reserved for future use. **The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.**

Identifier: RQ_001_1100
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The value of the Mobility Header's, Reserved field MUST be ignored by the receiver.

RFC Text:
8-bit field reserved for future use. **The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.**

Identifier: RQ_001_1100
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The value of the Mobility Header's, Reserved field MUST be ignored by the receiver.

RFC Text:
8-bit field reserved for future use. **The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.**

Identifier: RQ_001_1101
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Upper-Layer Packet Length field in the pseudo-header MUST be set to the total length of the Mobility Header. For computing the checksum, the checksum field is set to zero.

RFC Text:
Checksum

16-bit unsigned integer. This field contains the checksum of the Mobility Header. The checksum is calculated from the octet string consisting of a "pseudo-header" followed by the entire Mobility Header starting with the Payload Proto field. The checksum is the 16-bit one's complement of the one's complement sum of this string.

The pseudo-header contains IPv6 header fields, as specified in Section 8.1 of RFC 2460 . The Next Header value used in the pseudo-header is 2. The addresses used in the pseudo-header are the addresses that appear in the Source and Destination Address fields in the IPv6 packet carrying the Mobility Header.

Note that the procedures of calculating upper layer checksums while away from home described in Section 11.3.1 apply even for the Mobility Header. If a mobility message has a Home Address destination option, then the checksum calculation uses the home address in this option as the value of the IPv6 Source Address field. The type 2 routing header is treated as explained in RFC 2460.

The Mobility Header is considered as the upper layer protocol for the purposes of calculating the pseudo-header. **The Upper-Layer Packet Length field in the pseudo-header MUST be set to the total length of the Mobility Header.**

For computing the checksum, the checksum field is set to zero.

Identifier: RQ_001_1101
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Upper-Layer Packet Length field in the pseudo-header MUST be set to the total length of the Mobility Header. For computing the checksum, the checksum field is set to zero.

RFC Text:
Checksum

16-bit unsigned integer. This field contains the checksum of the Mobility Header. The checksum is calculated from the octet string consisting of a "pseudo-header" followed by the entire Mobility Header starting with the Payload Proto field. The checksum is the 16-bit one's complement of the one's complement sum of this string.

The pseudo-header contains IPv6 header fields, as specified in Section 8.1 of RFC 2460 . The Next Header value used in the pseudo-header is 2. The addresses used in the pseudo-header are the addresses that appear in the Source and Destination Address fields in the IPv6 packet carrying the Mobility Header.

Note that the procedures of calculating upper layer checksums while away from home described in Section 11.3.1 apply even for the Mobility Header. If a mobility message has a Home Address destination option, then the checksum calculation uses the home address in this option as the value of the IPv6 Source Address field. The type 2 routing header is treated as explained in RFC 2460.

The Mobility Header is considered as the upper layer protocol for the purposes of calculating the pseudo-header. **The Upper-Layer Packet Length field in the pseudo-header MUST be set to the total length of the Mobility Header.**

For computing the checksum, the checksum field is set to zero.

Identifier: RQ_001_1101
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Upper-Layer Packet Length field in the pseudo-header MUST be set to the total length of the Mobility Header. For computing the checksum, the checksum field is set to zero.

RFC Text:
Checksum

16-bit unsigned integer. This field contains the checksum of the Mobility Header. The checksum is calculated from the octet string consisting of a "pseudo-header" followed by the entire Mobility Header starting with the Payload Proto field. The checksum is the 16-bit one's complement of the one's complement sum of this string.

The pseudo-header contains IPv6 header fields, as specified in Section 8.1 of RFC 2460 . The Next Header value used in the pseudo-header is 2. The addresses used in the pseudo-header are the addresses that appear in the Source and Destination Address fields in the IPv6 packet carrying the Mobility Header.

Note that the procedures of calculating upper layer checksums while away from home described in Section 11.3.1 apply even for the Mobility Header. If a mobility message has a Home Address destination option, then the checksum calculation uses the home address in this option as the value of the IPv6 Source Address field. The type 2 routing header is treated as explained in RFC 2460.

The Mobility Header is considered as the upper layer protocol for the purposes of calculating the pseudo-header. **The Upper-Layer Packet Length field in the pseudo-header MUST be set to the total length of the Mobility Header.**

For computing the checksum, the checksum field is set to zero.

Identifier: RQ_001_1102
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Mobility Header's, Message Data field is a variable length field containing the data specific to the indicated Mobility Header type. If included, any "mobility options" MUST appear after the fixed portion of the message data specified.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; **if included, any options MUST appear after the fixed portion of the message data** specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1102
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Mobility Header's, Message Data field is a variable length field containing the data specific to the indicated Mobility Header type. If included, any "mobility options" MUST appear after the fixed portion of the message data specified.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; **if included, any options MUST appear after the fixed portion of the message data** specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1102
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Mobility Header's, Message Data field is a variable length field containing the data specific to the indicated Mobility Header type. If included, any "mobility options" MUST appear after the fixed portion of the message data specified.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; **if included, any options MUST appear after the fixed portion of the message data** specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1103
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1103
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1103
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

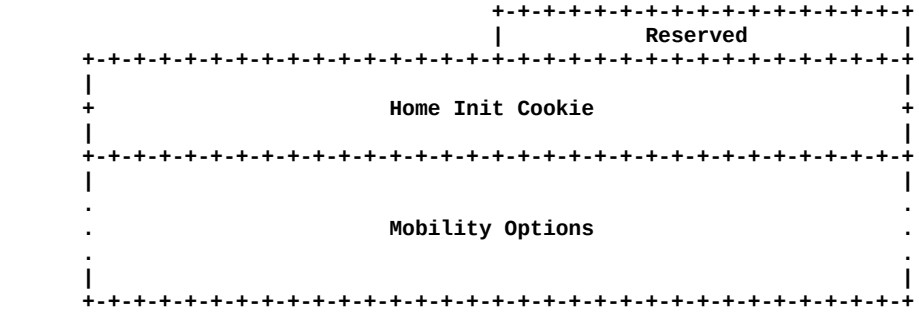
Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1104
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Refresh Request message uses the MH Type value 0. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is is as follows

Bit	Field
1 - 16	Reserved field
17 - end	Mobility Options field

RFC Text:
The Binding Refresh Request message uses the MH Type value 0. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Identifier: RQ_001_1105
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Refresh request Message's Reserved field MUST be 16-bit field initialized to zero by the sender.

RFC Text:
Reserved

16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Identifier: RQ_001_1106
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Binding Refresh request Message's Reserved field MUST be ignored by the receiver.

RFC Text:
Reserved

16-bit field reserved for future use. **The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.**

Identifier: RQ_001_1107
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Refresh request Message's Mobility Options field is a variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Refresh Request message that need not be present in all Binding Refresh Request messages sent. Mobility options allow future extensions to the format of the Binding Refresh Request message to be defined. This specification does not define any options valid for the Binding Refresh Request message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 0.

Identifier: RQ_001_1108
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The receiver MUST ignore and skip any options which it does not understand in the Binding Refresh request Message's Mobility Options field.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. **The receiver MUST ignore and skip any options which it does not understand.**

There MAY be additional information, associated with this Binding Refresh Request message that need not be present in all Binding Refresh Request messages sent. Mobility options allow future extensions to the format of the Binding Refresh Request message to be defined. This specification does not define any options valid for the Binding Refresh Request message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 0.

Identifier: RQ_001_1109
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If no actual options are present in the Binding Refresh request Message, no padding is necessary and the Header Len field will be set to 0.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Refresh Request message that need not be present in all Binding Refresh Request messages sent. Mobility options allow future extensions to the format of the Binding Refresh Request message to be defined. This specification does not define any options valid for the Binding Refresh Request message.

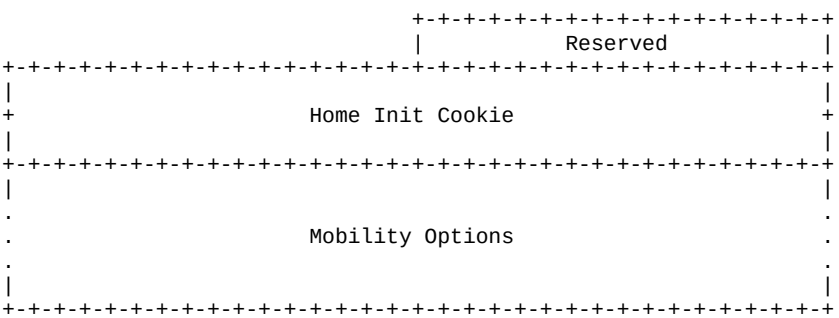
If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 0.

Identifier: RQ_001_1110
RFC Clause: 6.1.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Home Test Init message uses the MH Type value 1. When this value is indicated in the MH Type field, the format of the the Message Data field in the Mobility Header is as follows:

Bit	Field
1 - 16	Reserved Field
17 - 80	Home Init Cookie Field
81- end	Mobility Options Field.

RFC Text:
A mobile node uses the Home Test Init (HoTI) message to initiate the return routability procedure and request a home keygen token from a correspondent node (see Section 11.6.1). **The Home Test Init message uses the MH Type value 1. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:**



Identifier: RQ_001_1111
RFC Clause: 6.1.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Home Test Init Message's Reserved field MUST be 16-bit field initialized to zero by the sender.

RFC Text:
Reserved

16-bit field reserved for future use. This value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Identifier: RQ_001_1112
RFC Clause: 6.1.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Home Test Init Message's Reserved field MUST be ignored by the receiver.

RFC Text:
Reserved

16-bit field reserved for future use. **This value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.**

Identifier: RQ_001_1113
RFC Clause: 6.1.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Home Test Init Message's Home Init Cookie field is a 64-bit field containig the home init cookie.

RFC Text:
Home Init Cookie

64-bit field which contains a random value, the home init cookie.

Identifier: RQ_001_1114
RFC Clause: 6.1.3
Type: Mandatory
Applies to: Node

Requirement:
The Home Test Init Message's Mobility Options field is a variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Home Test Init message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 1.

This message is tunneled through the home agent when the mobile node is away from home. Such tunneling SHOULD employ IPsec ESP in tunnel mode between the home agent and the mobile node. This protection is indicated by the IPsec security policy database. The protection of Home Test Init messages is unrelated to the requirement to protect regular payload traffic, which MAY use such tunnels as well.

Identifier: RQ_001_1115
RFC Clause: 6.1.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The receiver MUST ignore and skip any options which it does not understand in the the Home Test Init message's Mobility Options field.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. **The receiver MUST ignore and skip any options which it does not understand.** This specification does not define any options valid for the Home Test Init message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 1.

This message is tunneled through the home agent when the mobile node is away from home. Such tunneling SHOULD employ IPsec ESP in tunnel mode between the home agent and the mobile node. This protection is indicated by the IPsec security policy database. The protection of Home Test Init messages is unrelated to the requirement to protect regular payload traffic, which MAY use such tunnels as well.

Identifier: RQ_001_1116
RFC Clause: 6.1.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If no actual options are present in the Home Test Init Message, no padding is necessary and the Header Len field will be set to 1.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Home Test Init message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 1.

This message is tunneled through the home agent when the mobile node is away from home. Such tunneling SHOULD employ IPsec ESP in tunnel mode between the home agent and the mobile node. This protection is indicated by the IPsec security policy database. The protection of Home Test Init messages is unrelated to the requirement to protect regular payload traffic, which MAY use such tunnels as well.

Identifier: RQ_001_1117
RFC Clause: 6.1.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
the Home Test Init Message tunneled through the home agent when the mobile node is away from home. Such tunneling SHOULD employ IPsec ESP in tunnel mode between the home agent and the mobile node. This protection is indicated by the IPsec security policy database. The protection of Home Test Init messages is unrelated to the requirement to protect regular payload traffic, which MAY use such tunnels as well.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Home Test Init message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 1.

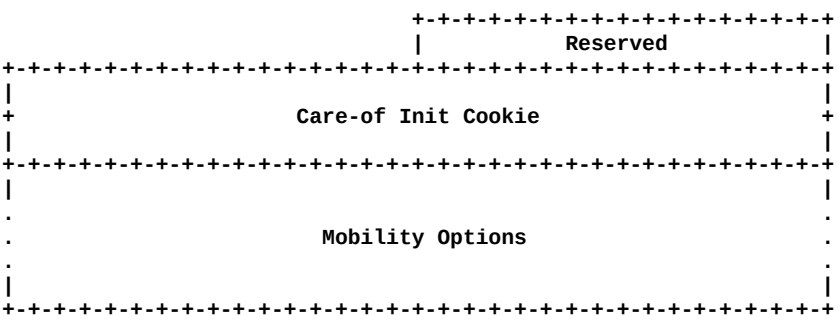
This message is tunneled through the home agent when the mobile node is away from home. Such tunneling SHOULD employ IPsec ESP in tunnel mode between the home agent and the mobile node. This protection is indicated by the IPsec security policy database. The protection of Home Test Init messages is unrelated to the requirement to protect regular payload traffic, which MAY use such tunnels as well.

Identifier: RQ_001_1118
RFC Clause: 6.1.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Care-of Test Init (CoTI) message uses the MH Type value 2. When this value is indicated in the MH Type field, the format of the the Message Data field in the Mobility Header is as follows:

```
Bit                 Field
-------------------------------------
1 - 16           Reserved Field
17 - 80         Care-of Init Cookie Field
81 - end       Mobility Options Field.
```

RFC Text:
A mobile node uses the Care-of Test Init (CoTI) message to initiate the return routability procedure and request a care-of keygen token from a correspondent node (see Section 11.6.1). The Care-of Test Init message uses the MH Type value 2. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Identifier: RQ_001_1119
RFC Clause: 6.1.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Care-of Test Init Message's Reserved field MUST be 16-bit field initialized to zero by the sender.

RFC Text:
Reserved

16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Identifier: RQ_001_1120
RFC Clause: 6.1.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Care-of Test Init Message's Reserved field MUST be ignored by the receiver..

RFC Text:
Reserved

16-bit field reserved for future use. **The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.**

Identifier: RQ_001_1121
RFC Clause: 6.1.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Care-of Test Init Message's Home Init Cookie field is a 64-bit field containig the home init cookie.

RFC Text:
Care-of Init Cookie

64-bit field which contains a random value, the care-of init cookie.

Identifier: RQ_001_1122
RFC Clause: 6.1.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Care-of Test Init Message's Mobility Options field is a variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Care-of Test Init message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 1.

Identifier: RQ_001_1123
RFC Clause: 6.1.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The receiver MUST ignore and skip any options which it does not understand in the the Care-of Test Init message's Mobility Options field.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. **The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Care-of Test Init message.**

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 1.

Identifier: RQ_001_1124
RFC Clause: 6.1.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If no actual options are present in the Care-of Test Init Message, no padding is necessary and the Header Len field will be set to 1.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Care-of Test Init message.

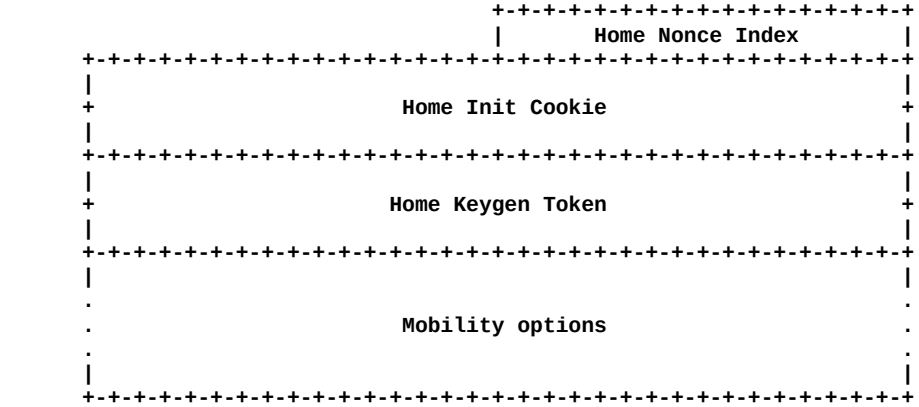
If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 1.

Identifier: RQ_001_1125
RFC Clause: 6.1.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Home Test (HoT) message uses the MH Type value 3. When this value is indicated in the MH Type field, the format of the the Message Data field in the Mobility Header is as follows:

```
Bit               Field
--------------------------------
1 - 16           Home Nonce Index field
17 - 80         Home Init Cookie Field
81 - 144       Home |Keygen Token Field
145 - end     Mobility Options Field.
```

RFC Text:
The Home Test (HoT) message is a response to the Home Test Init message, and is sent from the correspondent node to the mobile node (see Section 5.2.5). The Home Test message uses the MH Type value 3. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Identifier: RQ_001_1126
RFC Clause: 6.1.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Home Test Message's Home Init Cookie field is a 64-bit field containig the home init cookie.

RFC Text:
Home Init Cookie

64-bit field which contains the home init cookie.

Identifier: RQ_001_1127
RFC Clause: 6.1.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Home Test Message's Home Keygen Token field is a 64-bit field containig the home keygen token .

RFC Text:
Home Keygen Token

This field contains the 64 bit home keygen token used in the return routability procedure.

Identifier: RQ_001_1128
RFC Clause: 6.1.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Home Test Message's Mobility Options field is a variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Home Test message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

Identifier: RQ_001_1129
RFC Clause: 6.1.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The receiver MUST ignore and skip any options which it does not understand in the the Home Test message's Mobility Options field.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. **The receiver MUST ignore and skip any options which it does not understand.** This specification does not define any options valid for the Home Test message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

Identifier: RQ_001_1130
RFC Clause: 6.1.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If no actual options are present in the Home Test Message, no padding is necessary and the Header Len field will be set to 2.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Home Test message.

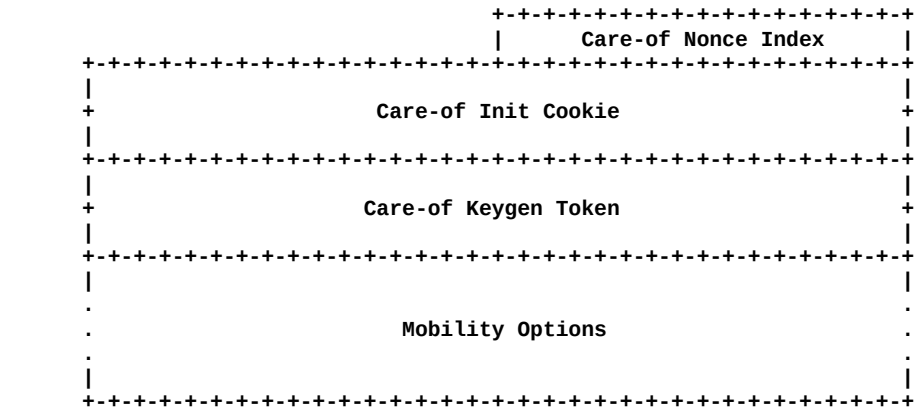
If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

Identifier: RQ_001_1131
RFC Clause: 6.1.6
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Care-of Test (CoT) message uses the MH Type value 4. When this value is indicated in the MH Type field, the format of the the Message Data field in the Mobility Header is as follows:

```
Bit                Field
--------------------------------
1 - 16            Care-of Nonce Index Field
17 - 80          Care-of Init Cookie Field
81 - 144        Care-of Keygen Token Field
145 - end      Mobility Options Field.
```

RFC Text:
The Care-of Test (CoT) message is a response to the Care-of Test Init message, and is sent from the correspondent node to the mobile node (see Section 11.6.2). The Care-of Test message uses the MH Type value 4. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Identifier: RQ_001_1132
RFC Clause: 6.1.6
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Care-of Test Message's Care-of Init Cookie field is a 64-bit field containig the care-of init cookie.

RFC Text:
Care-of Init Cookie

64-bit field which contains the care-of init cookie.

Identifier: RQ_001_1133
RFC Clause: 6.1.6
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Care-of Test Message's Care-of Keygen Token Field is a 64-bit field containig the care-of keygen token.

RFC Text:
Care-of Keygen Token

This field contains the 64 bit care-of keygen token used in the return routability procedure.

Identifier: RQ_001_1134
RFC Clause: 6.1.6
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Care-of Test Message's Mobility Options field is a variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Care-of Test message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

Identifier: RQ_001_1135
RFC Clause: 6.1.6
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If no actual options are present in the Care of Test Message, no padding is necessary and the Header Len field will be set to 2.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for the Care-of Test message.

If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

Identifier: RQ_001_1136
RFC Clause: 6.1.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The receiver MUST ignore and skip any options in the Care-of test Message which it does not understand.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. **The receiver MUST ignore and skip any options which it does not understand.** This specification does not define any options valid for the Care-of Test message.
{If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

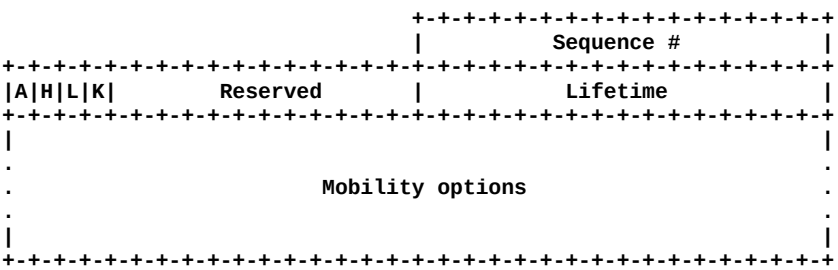
Identifier: RQ_001_1138
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Binding Update message uses the MH Type value 5. When this value is indicated in the MH Type field, the format of the the Message Data field in the Mobility Header is as follows:

Bit	Field
1 - 16	Sequence # Field
17	A Bit
18	H Bit
19	L Bit
20	K Bit
21 - 32	Reserved Field
33 - 48	Lifetime Field
49 - end	Mobility Options Field.

RFC Text:
The Binding Update (BU) message is used by a mobile node to notify other nodes of a new care-of address for itself. Binding Updates are sent as described in Section 11.7.1 and Section 11.7.2.

The Binding Update uses the MH Type value 5. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Identifier: RQ_001_1139
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the Binding Update Message's Acknowledge (A) bit is is set by the sending mobile node, the receiving node is requested to returned a Binding Acknowledgement upon receipt of the Binding Update.

RFC Text:
The Acknowledge (A) bit is set by the sending mobile node to request a Binding Acknowledgement (Section 6.1.8) be returned upon receipt of the Binding Update.

Identifier: RQ_001_1140
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The destination of the packet carrying a Binding Update Message with the Home Registration (H) bit set, MUST be that of a router sharing the same subnet prefix as the home address of the mobile node in the binding.

RFC Text:
The Home Registration (H) bit is set by the sending mobile node to request that the receiving node should act as this node's home agent. The destination of the packet carrying this message MUST be that of a router sharing the same subnet prefix as the home address of the mobile node in the binding.

Identifier: RQ_001_1141
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Update Message, the Link-Local Address Compatibility (L) bit MUST BE set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.

RFC Text:
The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.

Identifier: RQ_001_1142
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the Binding Update Message's Key Management Mobility Capability (K) bit is cleared, the protocol used for establishing the IPsec security associations between the mobile node and the home agent does not survive movements and may then have to be rerun.

RFC Text:
Key Management Mobility Capability (K)

If this bit is cleared, the protocol used for establishing the IPsec security associations between the mobile node and the home agent does not survive movements. It may then have to be rerun. (Note that the IPsec security associations themselves are expected to survive movements.) If manual IPsec configuration is used, the bit MUST be cleared.

This bit is valid only in Binding Updates sent to the home agent, and MUST be cleared in other Binding Updates. Correspondent nodes MUST ignore this bit.

Identifier: RQ_001_1143
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If manual IPsec configuration is used, the Binding Update Message's Key Management Mobility Capability (K) bit MUST be cleared.

RFC Text:
Key Management Mobility Capability (K)

If this bit is cleared, the protocol used for establishing the IPsec security associations between the mobile node and the home agent does not survive movements. It may then have to be rerun. (Note that the IPsec security associations themselves are expected to survive movements.) **If manual IPsec configuration is used, the bit MUST be cleared.**

This bit is valid only in Binding Updates sent to the home agent, and MUST be cleared in other Binding Updates. Correspondent nodes MUST ignore this bit.

Identifier: RQ_001_1144
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Binding Update Message's Reserved field MUST be set to zero by the sender

RFC Text:

Reserved

These fields are unused. They MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1145
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Update Message's Reserved field MUST be ignored by the receiver.

RFC Text:

Reserved

These fields are unused. They MUST be initialized to zero by the sender and **MUST be ignored by the receiver.**

Identifier: RQ_001_1146
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Binding Update Message's Sequence # field is a 16-bit unsigned integer which SHALL be used by the receiving node to sequence Binding Updates

RFC Text:
Sequence #

A 16-bit unsigned integer used by the receiving node to sequence Binding Updates and by the sending node to match a returned Binding Acknowledgement with this Binding Update.

Identifier: RQ_001_1147
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Binding Update Message's Sequence # field is a 16-bit unsigned integer which SHALL be used by the sending node to match a returned Binding Acknowledgement with this Binding Update.

RFC Text:
Sequence #

A 16-bit unsigned integer used by the receiving node to sequence Binding Updates and by the sending node to match a returned Binding Acknowledgement with this Binding Update.

Identifier: RQ_001_1148
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Binding Update Message's Lifetime field is a 16-bit unsigned integer. The number of time units remaining before the binding MUST be considered expired.

RFC Text:
Lifetime

16-bit unsigned integer. The number of time units remaining before the binding MUST be considered expired. A value of zero indicates that the Binding Cache entry for the mobile node MUST be deleted. (In this case the specified care-of address MUST also be set equal to the home address.) One time unit is 4 seconds.

Identifier: RQ_001_1149
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Update Message's Lifetime field, a value of zero indicates that the Binding Cache entry for the mobile node MUST be deleted.

RFC Text:
Lifetime

16-bit unsigned integer. The number of time units remaining before the binding MUST be considered expired. **A value of zero indicates that the Binding Cache entry for the mobile node MUST be deleted.** (In this case the specified care-of address MUST also be set equal to the home address.) One time unit is 4 seconds.

Identifier: RQ_001_1150
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the Binding Update Message's Lifetime field is set to zero, the specified care-of address MUST also be set equal to the home address.

RFC Text:
Lifetime

16-bit unsigned integer. The number of time units remaining before the binding MUST be considered expired. A value of zero indicates that the Binding Cache entry for the mobile node MUST be deleted. **(In this case the specified care-of address MUST also be set equal to the home address.)** One time unit is 4 seconds.

Identifier: RQ_001_1151
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Binding Update Message's Mobility Options field is a variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. The receiver MUST ignore and skip any options which it does not understand.

The following options are valid in a Binding Update:

* Binding Authorization Data option (this option is mandatory in Binding Updates sent to a correspondent node)

* Nonce Indices option.

* Alternate Care-of Address option

Identifier: RQ_001_1152
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Update Message's Mobility Options field, the valid options are:
* Binding Authorization Data option (this option is mandatory in Binding Updates sent to a correspondent node)
* Nonce Indices option.
* Alternate Care-of Address option

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. The receiver MUST ignore and skip any options which it does not understand.

The following options are valid in a Binding Update:

*** Binding Authorization Data option (this option is mandatory in Binding Updates sent to a correspondent node)**

*** Nonce Indices option.**

*** Alternate Care-of Address option**

Identifier: RQ_001_1153
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Update Message's Mobility Options field, the receiver MUST ignore and skip any options which it does not understand.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. **The receiver MUST ignore and skip any options which it does not understand.**

The following options are valid in a Binding Update:

* Binding Authorization Data option (this option is mandatory in Binding Updates sent to a correspondent node)

* Nonce Indices option.

* Alternate Care-of Address option

Identifier: RQ_001_1154
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Update Message's Mobility Options field, if no options are present in this message, 4 octets of padding are necessary and the Header Len field will be set to 1.

RFC Text:
If no options are present in this message, 4 octets of padding are necessary and the Header Len field will be set to 1.

Identifier: RQ_001_1155
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Update Message, the care-of address is specified either by the Source Address field in the IPv6 header or by the Alternate Care-of Address option, if present.

RFC Text:
The care-of address is specified either by the Source Address field in the IPv6 header or by the Alternate Care-of Address option, if present. The care-of address MUST be a unicast routable address. IPv6 Source Address MUST be a topologically correct source address. Binding Updates for a care-of address which is not a unicast routable address MUST be silently discarded. Similarly, the Binding Update MUST be silently discarded if the care-of address appears as a home address in an existing Binding Cache entry, with its current location creating a circular reference back to the home address specified in the Binding Update (possibly through additional entries).

Identifier: RQ_001_1156
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Update Message's Mobility Options field, the IPv6 Source Address MUST be a topologically correct source address.

RFC Text:
The care-of address is specified either by the Source Address field in the IPv6 header or by the Alternate Care-of Address option, if present. The care-of address MUST be a unicast routable address. **IPv6 Source Address MUST be a topologically correct source address.** Binding Updates for a care-of address which is not a unicast routable address MUST be silently discarded. Similarly, the Binding Update MUST be silently discarded if the care-of address appears as a home address in an existing Binding Cache entry, with its current location creating a circular reference back to the home address specified in the Binding Update (possibly through additional entries).

Identifier: RQ_001_1157
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Binding Updates for a care-of address which is not a unicast routable address MUST be silently discarded.

RFC Text:
The care-of address is specified either by the Source Address field in the IPv6 header or by the Alternate Care-of Address option, if present. The care-of address MUST be a unicast routable address. IPv6 Source Address MUST be a topologically correct source address. **Binding Updates for a care-of address which is not a unicast routable address MUST be silently discarded.** Similarly, the Binding Update MUST be silently discarded if the care-of address appears as a home address in an existing Binding Cache entry, with its current location creating a circular reference back to the home address specified in the Binding Update (possibly through additional entries).

Identifier: RQ_001_1158
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Binding Update MUST be silently discarded if the care-of address appears as a home address in an existing Binding Cache entry, with its current location.

RFC Text:
The care-of address is specified either by the Source Address field in the IPv6 header or by the Alternate Care-of Address option, if present. The care-of address MUST be a unicast routable address. IPv6 Source Address MUST be a topologically correct source address. Binding Updates for a care-of address which is not a unicast routable address MUST be silently discarded. **Similarly, the Binding Update MUST be silently discarded if the care-of address appears as a home address in an existing Binding Cache entry, with its current location creating a circular reference back to the home address specified in the Binding Update (possibly through additional entries).**

Identifier: RQ_001_1159
RFC Clause: 6.1.7
Type: Optional
Applies to: Mobile_Node

Requirement:
The deletion of a binding CAN be indicated within the Binding Update Message by setting the Lifetime field to 0 and by setting the care-of address equal to the home address.

RFC Text:
The deletion of a binding can be indicated by setting the Lifetime field to 0 and by setting the care-of address equal to the home address. In deletion, the generation of the binding management key depends exclusively on the home keygen token, as explained in Section 5.2.5. (Note that while the senders are required to set both the Lifetime field to 0 and the care-of address equal to the home address, Section 9.5.1 rules for receivers are more liberal, and interpret either condition as a deletion.)

Identifier: RQ_001_1160
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent nodes SHOULD NOT delete the Binding Cache entry before the lifetime expires,

RFC Text:
Correspondent nodes SHOULD NOT delete the Binding Cache entry before the lifetime expires, if any application hosted by the correspondent node is still likely to require communication with the mobile node. A Binding Cache entry that is de-allocated prematurely might cause subsequent packets to be dropped from the mobile node, if they contain the Home Address destination option. This situation is recoverable, since a Binding Error message is sent to the mobile node

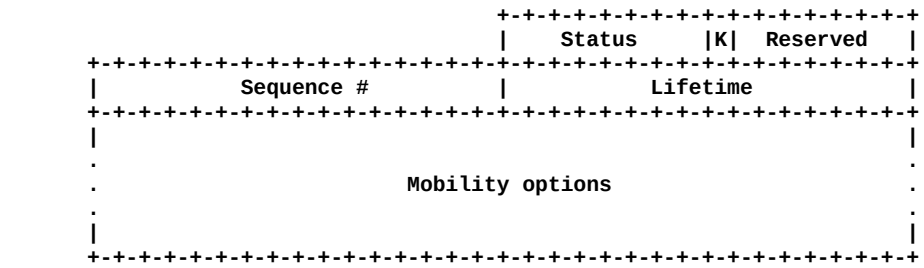
Identifier: RQ_001_1161
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Acknowledgement has the MH Type value 6. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is

Bits	Field
1 - 8	Status Field
9	K bit
10 - 16	Reserved Field
17 - 32	Sequence # Field
33 - 48	Lifetime Field
49 - end	Mobility Options Field

RFC Text:
The Binding Acknowledgement is used to acknowledge receipt of a Binding Update (Section 6.1.7). This packet is sent as described in Section 9.5.4 and Section 10.3.1.

The Binding Acknowledgement has the MH Type value 6. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Identifier: RQ_001_1163
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Acknowledgement Message, correspondent nodes MUST set the K bit to 0.

RFC Text:
Key Management Mobility Capability (K)

If this bit is cleared, the protocol used by the home agent for establishing the IPsec security associations between the mobile node and the home agent does not survive movements. It may then have to be rerun. (Note that the IPsec security associations themselves are expected to survive movements.)

Correspondent nodes MUST set the K bit to 0.

Identifier: RQ_001_1164
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Acknowledgement Message, the Reserved Field MUST be initialized to zero by the sender.

RFC Text:
Reserved

These fields are unused. **They MUST be initialized to zero by the sender** and MUST be ignored by the receiver.

Identifier: RQ_001_1165
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Acknowledgement Message, the Reserved Field MUST be ignored by the receiver..

RFC Text:
Reserved

These fields are unused. They MUST be initialized to zero by the sender and **MUST be ignored by the receiver.**

Identifier: RQ_001_1166
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

```
In the Binding Acknowledgement Message, the Status Field is an 8-bit unsigned integer is set as
follows:
        0 Binding Update accepted
        1 Accepted but prefix discovery necessary
      128 Reason unspecified
      129 Administratively prohibited
      130 Insufficient resources
      131 Home registration not supported
      132 Not home subnet
      133 Not home agent for this mobile node
      134 Duplicate Address Detection failed
      135 Sequence number out of window
      136 Expired home nonce index
      137 Expired care-of nonce index
      138 Expired nonces
      139 Registration type change disallowed
```

RFC Text:

Status

8-bit unsigned integer indicating the disposition of the Binding Update. Values of the Status field less than 128 indicate that the Binding Update was accepted by the receiving node. Values greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following Status values are currently defined:

0 Binding Update accepted

1 Accepted but prefix discovery necessary

128 Reason unspecified

129 Administratively prohibited

130 Insufficient resources

131 Home registration not supported

132 Not home subnet

133 Not home agent for this mobile node

134 Duplicate Address Detection failed

135 Sequence number out of window

136 Expired home nonce index

137 Expired care-of nonce index

138 Expired nonces

139 Registration type change disallowed

Up-to-date values of the Status field are to be specified in the IANA registry of assigned numbers [19].

Identifier: RQ_001_1167
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Acknowledgement Message, the Sequence Number in the Binding Acknowledgement is copied from the Sequence Number field in the Binding Update.

RFC Text:
Sequence #

The Sequence Number in the Binding Acknowledgement is copied from the Sequence Number field in the Binding Update. It is used by the mobile node in matching this Binding Acknowledgement with an outstanding Binding Update.

Identifier: RQ_001_1168
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Acknowledgement Message the Lifetime Field shall indicate, in time units of 4 seconds, the granted lifetime for which this node SHOULD retain the entry for this mobile node in its Binding Cache.

RFC Text:
Lifetime

The granted lifetime, in time units of 4 seconds, for which this node SHOULD retain the entry for this mobile node in its Binding Cache. The value of this field is undefined if the Status field indicates that the Binding Update was rejected.

Identifier: RQ_001_1169
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Acknowledgement Message the Mobility Options Field is a variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Acknowledgement that need not be present in all Binding Acknowledgements sent. Mobility options allow future extensions to the format of the Binding Acknowledgement to be defined. The following options are valid for the Binding Acknowledgement:

* Binding Authorization Data option (this option is mandatory in Binding Acknowledgements sent by a correspondent node, except where otherwise noted in Section 9.5.4)

* Binding Refresh Advice option

If no options are present in this message, 4 octets of padding are necessary and the Header Len field will be set to 1.

Identifier: RQ_001_1170
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The receiver of the Binding Acknowledgement Message MUST ignore and skip any Mobility options which it does not understand.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. **The receiver MUST ignore and skip any options which it does not understand.**

There MAY be additional information, associated with this Binding Acknowledgement that need not be present in all Binding Acknowledgements sent. Mobility options allow future extensions to the format of the Binding Acknowledgement to be defined. The following options are valid for the Binding Acknowledgement:
* Binding Authorization Data option (this option is mandatory in Binding Acknowledgements sent by a correspondent node, except
where otherwise noted in Section 9.5.4)

* Binding Refresh Advice option

If no options are present in this message, 4 octets of padding are necessary and the Header Len field will be set to 1.

Identifier: RQ_001_1171
RFC Clause: 6.1.8
Type: Optional
Applies to: Correspondent_Node

Requirement:
In the Binding Acknowledgement Message the Mobility Options Field there MAY be additional information, associated with this Binding Acknowledgement that need not be present in all Binding Acknowledgements sent. The following options are valid for the Binding Acknowledgement:
* Binding Authorization Data option
* Binding Refresh Advice option

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Acknowledgement that need not be present in all Binding Acknowledgements sent. Mobility options allow future extensions to the format of the Binding Acknowledgement to be defined. The following options are valid for the Binding Acknowledgement:
*** Binding Authorization Data option (this option is mandatory in Binding Acknowledgements sent by a correspondent node, except**
where otherwise noted in Section 9.5.4)

*** Binding Refresh Advice option**

If no options are present in this message, 4 octets of padding are necessary and the Header Len field will be set to 1.

Identifier: RQ_001_1172
RFC Clause: 6.1.8
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Acknowledgement Message, if no options are present in this message, 4 octets of padding are necessary and the Header Len field will be set to 1.

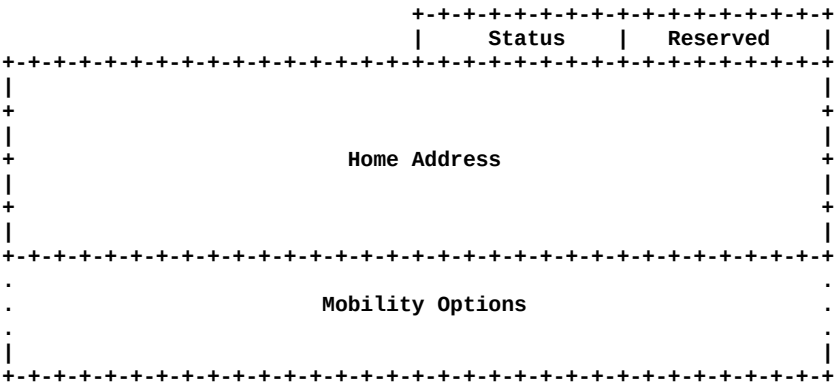
RFC Text:
If no options are present in this message, 4 octets of padding are necessary and the Header Len field will be set to 1.

Identifier: RQ_001_1173
RFC Clause: 6.1.9
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Error (BE) message uses the MH Type value 7. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is Status field, followed by Reserved Field, followed by Home Address and Mobility Oprions Field

RFC Text:
The Binding Error (BE) message is used by the correspondent node to signal an error related to mobility, such as an inappropriate attempt to use the Home Address destination option without an existing binding; see Section 9.3.3 for details.

The Binding Error message uses the MH Type value 7. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Identifier: RQ_001_1174
RFC Clause: 6.1.9
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Error (BE) message's Status Field is an 8-bit unsigned integer indicating the reason for this message. The following values are currently defined:
1 Unknown binding for Home Address destination option
2 Unrecognized MH Type value

RFC Text:
Status

8-bit unsigned integer indicating the reason for this message. The following values are currently defined:

1 Unknown binding for Home Address destination option
2 Unrecognized MH Type value

Identifier: RQ_001_1175
RFC Clause: 6.1.9
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Error (BE) message's Reserved Field, the value MUST be initialized to zero by the sender

RFC Text:
Reserved

A 8-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Identifier: RQ_001_1176
RFC Clause: 6.1.9
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Error (BE) message's Reserved Field, the value MUST be ignored by the receiver.

RFC Text:
Reserved

A 8-bit field reserved for future use. The value MUST be initialized to zero by the sender, and **MUST be ignored by the receiver.**

Identifier: RQ_001_1177
RFC Clause: 6.1.9
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Error (BE) message's Home Address Field shall contain the home address that was contained in the Home Address destination option.

RFC Text:
Home Address

The home address that was contained in the Home Address destination option. The mobile node uses this information to determine which binding does not exist, in cases where the mobile node has several home addresses.

Identifier: RQ_001_1178
RFC Clause: 6.1.9
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Binding Error (BE) message's Mobility Options Field is a variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Error message that need not be present in all Binding Error messages sent. Mobility options allow future extensions to the format of the format of the Binding Error message to be defined. The encoding and format of defined options are described in Section 6.2. This specification does not define any options valid for the Binding Error message.

Identifier: RQ_001_1178
RFC Clause: 6.1.9
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Binding Error (BE) message's Mobility Options Field is a variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Error message that need not be present in all Binding Error messages sent. Mobility options allow future extensions to the format of the format of the Binding Error message to be defined. The encoding and format of defined options are described in Section 6.2. This specification does not define any options valid for the Binding Error message.

Identifier: RQ_001_1179
RFC Clause: 6.1.9
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The receiver MUST ignore and skip any options which it does not understand in the Binding Error (BE) message's Mobility Options Field

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. **The receiver MUST ignore and skip any options which it does not understand.**

There MAY be additional information, associated with this Binding Error message that need not be present in all Binding Error messages sent. Mobility options allow future extensions to the format of the format of the Binding Error message to be defined. The encoding and format of defined options are described in Section 6.2. This specification does not define any options valid for the Binding Error message.

Identifier: RQ_001_1180
RFC Clause: 6.1.9
Type: Optional
Applies to: Correspondent_Node

Requirement:
In the Binding Error (BE) message's Mobility Options Field there MAY be additional information, associated with this Binding Error message that need not be present in all Binding Error messages sent. Mobility options allow future extensions to the format of the format of the Binding Error message to be defined.

RFC Text:
Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand.

There MAY be additional information, associated with this Binding Error message that need not be present in all Binding Error messages sent. Mobility options allow future extensions to the format of the format of the Binding Error message to be defined. The encoding and format of defined options are described in Section 6.2. This specification does not define any options valid for the Binding Error message.

Identifier: RQ_001_1181
RFC Clause: 6.1.9
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If no actual options are present in the Binding Error (BE) message, no padding is necessary and the Header Len field will be set to 2.

RFC Text:
If no actual options are present in this message, no padding is necessary and the Header Len field will be set to 2.

Identifier: RQ_001_1182
RFC Clause: 6.2
Type: Optional
Applies to: Correspondent_Node

Requirement:
Mobility messages can include zero or more mobility options, the presence of options will be indicated by the Header Len of the Mobility Header.

RFC Text:
Mobility messages can include zero or more mobility options. This allows optional fields that may not be needed in every use of a particular Mobility Header, as well as future extensions to the format of the messages. Such options are included in the Message Data field of the message itself, after the fixed portion of the message data specified in the message subsections of Section 6.1.

The presence of such options will be indicated by the Header Len of the Mobility Header.

If included, the Binding Authorization Data option (Section 6.2.7) MUST be the last option and MUST NOT have trailing padding. Otherwise, options can be placed in any order.

Identifier: RQ_001_1182
RFC Clause: 6.2
Type: Optional
Applies to: Home_Agent

Requirement:
Mobility messages can include zero or more mobility options, the presence of options will be indicated by the Header Len of the Mobility Header.

RFC Text:
Mobility messages can include zero or more mobility options. This allows optional fields that may not be needed in every use of a particular Mobility Header, as well as future extensions to the format of the messages. Such options are included in the Message Data field of the message itself, after the fixed portion of the message data specified in the message subsections of Section 6.1.

The presence of such options will be indicated by the Header Len of the Mobility Header.

If included, the Binding Authorization Data option (Section 6.2.7) MUST be the last option and MUST NOT have trailing padding. Otherwise, options can be placed in any order.

Identifier: RQ_001_1182
RFC Clause: 6.2
Type: Optional
Applies to: Mobile_Node

Requirement:
Mobility messages can include zero or more mobility options, the presence of options will be indicated by the Header Len of the Mobility Header.

RFC Text:
Mobility messages can include zero or more mobility options. This allows optional fields that may not be needed in every use of a particular Mobility Header, as well as future extensions to the format of the messages. Such options are included in the Message Data field of the message itself, after the fixed portion of the message data specified in the message subsections of Section 6.1.

The presence of such options will be indicated by the Header Len of the Mobility Header.

If included, the Binding Authorization Data option (Section 6.2.7) MUST be the last option and MUST NOT have trailing padding. Otherwise, options can be placed in any order.

Identifier: RQ_001_1183
RFC Clause: 6.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If Mobility messages include the Binding Authorization Data option, this MUST be the last option and MUST NOT have trailing padding.

RFC Text:
Mobility messages can include zero or more mobility options. This allows optional fields that may not be needed in every use of a particular Mobility Header, as well as future extensions to the format of the messages. Such options are included in the Message Data field of the message itself, after the fixed portion of the message data specified in the message subsections of Section 6.1.

The presence of such options will be indicated by the Header Len of the Mobility Header. **If included, the Binding Authorization Data option (Section 6.2.7) MUST be the last option and MUST NOT have trailing padding. Otherwise, options can be placed in any order.**

Identifier: RQ_001_1183
RFC Clause: 6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
If Mobility messages include the Binding Authorization Data option, this MUST be the last option and MUST NOT have trailing padding.

RFC Text:
Mobility messages can include zero or more mobility options. This allows optional fields that may not be needed in every use of a particular Mobility Header, as well as future extensions to the format of the messages. Such options are included in the Message Data field of the message itself, after the fixed portion of the message data specified in the message subsections of Section 6.1.

The presence of such options will be indicated by the Header Len of the Mobility Header. **If included, the Binding Authorization Data option (Section 6.2.7) MUST be the last option and MUST NOT have trailing padding. Otherwise, options can be placed in any order.**

Identifier: RQ_001_1183
RFC Clause: 6.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If Mobility messages include the Binding Authorization Data option, this MUST be the last option and MUST NOT have trailing padding.

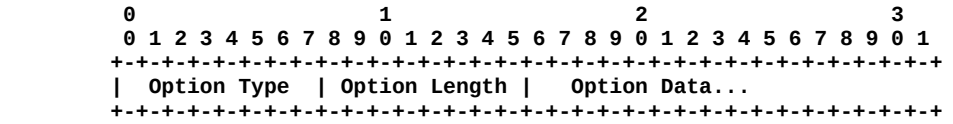
RFC Text:
Mobility messages can include zero or more mobility options. This allows optional fields that may not be needed in every use of a particular Mobility Header, as well as future extensions to the format of the messages. Such options are included in the Message Data field of the message itself, after the fixed portion of the message data specified in the message subsections of Section 6.1.

The presence of such options will be indicated by the Header Len of the Mobility Header. **If included, the Binding Authorization Data option (Section 6.2.7) MUST be the last option and MUST NOT have trailing padding. Otherwise, options can be placed in any order.**

Identifier: RQ_001_1184
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Mobility options are encoded within the remaining space of the Message Data field of a mobility message, using a type-length-value (TLV) format

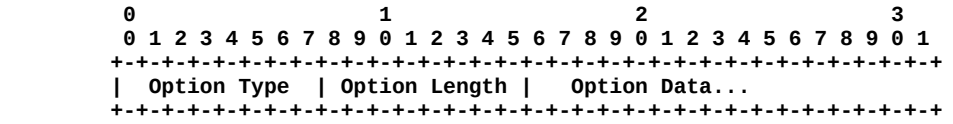
RFC Text:
Mobility options are encoded within the remaining space of the Message Data field of a mobility message, using a type-length-value (TLV) format as follows:



Identifier: RQ_001_1184
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Mobility options are encoded within the remaining space of the Message Data field of a mobility message, using a type-length-value (TLV) format

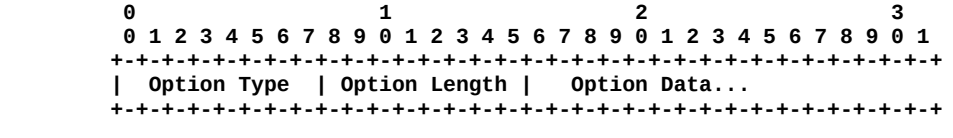
RFC Text:
Mobility options are encoded within the remaining space of the Message Data field of a mobility message, using a type-length-value (TLV) format as follows:



Identifier: RQ_001_1184
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Mobility options are encoded within the remaining space of the Message Data field of a mobility message, using a type-length-value (TLV) format

RFC Text:
Mobility options are encoded within the remaining space of the Message Data field of a mobility message, using a type-length-value (TLV) format as follows:



Identifier: RQ_001_1185
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
When processing a Mobility Header containing an option for which the Option Type value is not recognized by the receiver, the receiver MUST quietly ignore and skip over the option, correctly handling any remaining options in the message.

RFC Text:
Option Type

8-bit identifier of the type of mobility option. **When processing a Mobility Header containing an option for which the Option Type value is not recognized by the receiver, the receiver MUST quietly ignore and skip over the option, correctly handling any remaining options in the message.**

Identifier: RQ_001_1185
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When processing a Mobility Header containing an option for which the Option Type value is not recognized by the receiver, the receiver MUST quietly ignore and skip over the option, correctly handling any remaining options in the message.

RFC Text:
Option Type

8-bit identifier of the type of mobility option. **When processing a Mobility Header containing an option for which the Option Type value is not recognized by the receiver, the receiver MUST quietly ignore and skip over the option, correctly handling any remaining options in the message.**

Identifier: RQ_001_1185
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When processing a Mobility Header containing an option for which the Option Type value is not recognized by the receiver, the receiver MUST quietly ignore and skip over the option, correctly handling any remaining options in the message.

RFC Text:
Option Type

8-bit identifier of the type of mobility option. **When processing a Mobility Header containing an option for which the Option Type value is not recognized by the receiver, the receiver MUST quietly ignore and skip over the option, correctly handling any remaining options in the message.**

Identifier: RQ_001_1186
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Within Mobility messages, the Option Length field shall be an 8-bit unsigned integer, representing the length in octets of the mobility option, not including the Option Type and Option Length fields.

RFC Text:
Option Length

8-bit unsigned integer, representing the length in octets of the mobility option, not including the Option Type and Option Length fields.

Identifier: RQ_001_1186
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Within Mobility messages, the Option Length field shall be an 8-bit unsigned integer, representing the length in octets of the mobility option, not including the Option Type and Option Length fields.

RFC Text:
Option Length

8-bit unsigned integer, representing the length in octets of the mobility option, not including the Option Type and Option Length fields.

Identifier: RQ_001_1186
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages, the Option Length field shall be an 8-bit unsigned integer, representing the length in octets of the mobility option, not including the Option Type and Option Length fields.

RFC Text:
Option Length

8-bit unsigned integer, representing the length in octets of the mobility option, not including the Option Type and Option Length fields.

Identifier: RQ_001_1187
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Within Mobility messages the Option data Field is a variable length field that contains data specific to the option. These options are aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries.

RFC Text:
Option Data

A variable length field that contains data specific to the option.

The following subsections specify the Option types which are currently defined for use in the Mobility Header.

Implementations MUST silently ignore any mobility options that they do not understand.

Mobility options may have alignment requirements. **Following the convention in IPv6, these options are aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries (i.e., fields of width n octets are placed at an integer multiple of n octets from the start of the header, for n = 1, 2, 4, or 8) [11].**

Identifier: RQ_001_1187
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Within Mobility messages the Option data Field is a variable length field that contains data specific to the option. These options are aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries.

RFC Text:
Option Data

A variable length field that contains data specific to the option.

The following subsections specify the Option types which are currently defined for use in the Mobility Header.

Implementations MUST silently ignore any mobility options that they do not understand.

Mobility options may have alignment requirements. **Following the convention in IPv6, these options are aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries (i.e., fields of width n octets are placed at an integer multiple of n octets from the start of the header, for n = 1, 2, 4, or 8) [11].**

Identifier: RQ_001_1187
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages the Option data Field is a variable length field that contains data specific to the option. These options are aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries.

RFC Text:
Option Data

A variable length field that contains data specific to the option.

The following subsections specify the Option types which are currently defined for use in the Mobility Header.

Implementations MUST silently ignore any mobility options that they do not understand.

Mobility options may have alignment requirements. **Following the convention in IPv6, these options are aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries (i.e., fields of width n octets are placed at an integer multiple of n octets from the start of the header, for n = 1, 2, 4, or 8) [11].**

Identifier: RQ_001_1188
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Within Mobility messages, if the Option data Field contains options that they do not understand, Implementations MUST silently ignore any mobility options that they do not understand.

RFC Text:
Option Data

A variable length field that contains data specific to the option.

The following subsections specify the Option types which are currently defined for use in the Mobility Header.

Implementations MUST silently ignore any mobility options that they do not understand.

Mobility options may have alignment requirements. Following the convention in IPv6, these options are aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries (i.e., fields of width n octets are placed at an integer multiple of n octets from the start of the header, for n = 1, 2, 4, or 8) [11].

Identifier: RQ_001_1188
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Within Mobility messages, if the Option data Field contains options that they do not understand, Implementations MUST silently ignore any mobility options that they do not understand.

RFC Text:
Option Data

A variable length field that contains data specific to the option.

The following subsections specify the Option types which are currently defined for use in the Mobility Header.

Implementations MUST silently ignore any mobility options that they do not understand.

Mobility options may have alignment requirements. Following the convention in IPv6, these options are aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries (i.e., fields of width n octets are placed at an integer multiple of n octets from the start of the header, for n = 1, 2, 4, or 8) [11].

Identifier: RQ_001_1188
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages, if the Option data Field contains options that they do not understand, Implementations MUST silently ignore any mobility options that they do not understand.

RFC Text:
Option Data

A variable length field that contains data specific to the option.

The following subsections specify the Option types which are currently defined for use in the Mobility Header.

Implementations MUST silently ignore any mobility options that they do not understand.

Mobility options may have alignment requirements. Following the convention in IPv6, these options are aligned in a packet so that multi-octet values within the Option Data field of each option fall on natural boundaries (i.e., fields of width n octets are placed at an integer multiple of n octets from the start of the header, for n = 1, 2, 4, or 8) [11].

Identifier: RQ_001_1189
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Within Mobility messages, the Pad1 option shall be used wher there is a need to insert one octet of padding in the Mobility Options area of a Mobility Header.

RFC Text:
The Pad1 option does not have any alignment requirements. Its format is as follows:

```
      0
      0 1 2 3 4 5 6 7
     +-+-+-+-+-+-+-+-+
     |   Type = 0    |
     +-+-+-+-+-+-+-+-+
```

NOTE! the format of the Pad1 option is a special case - it has neither Option Length nor Option Data fields.

The Pad1 option is used to insert one octet of padding in the Mobility Options area of a Mobility Header. If more than one octet of padding is required, the PadN option, described next, should be used rather than multiple Pad1 options.

Identifier: RQ_001_1189
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
Within Mobility messages, the Pad1 option shall be used wher there is a need to insert one octet of padding in the Mobility Options area of a Mobility Header.

RFC Text:
The Pad1 option does not have any alignment requirements. Its format is as follows:

```
      0
      0 1 2 3 4 5 6 7
     +-+-+-+-+-+-+-+-+
     |   Type = 0    |
     +-+-+-+-+-+-+-+-+
```

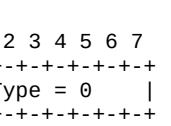
NOTE! the format of the Pad1 option is a special case - it has neither Option Length nor Option Data fields.

The Pad1 option is used to insert one octet of padding in the Mobility Options area of a Mobility Header. If more than one octet of padding is required, the PadN option, described next, should be used rather than multiple Pad1 options.

Identifier: RQ_001_1189
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages, the Pad1 option shall be used wher there is a need to insert one octet of padding in the Mobility Options area of a Mobility Header.

RFC Text:
The Pad1 option does not have any alignment requirements. Its format is as follows:



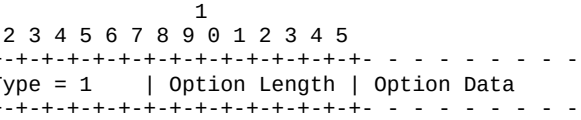
NOTE! the format of the Pad1 option is a special case - it has neither Option Length nor Option Data fields.

The Pad1 option is used to insert one octet of padding in the Mobility Options area of a Mobility Header. If more than one octet of padding is required, the PadN option, described next, should be used rather than multiple Pad1 options.

Identifier: RQ_001_1190
RFC Clause: 6.2.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Within Mobility messages, the PadN option shall be used wher there is a need to insert two or more octets of padding in the Mobility Options area of a Mobility Header. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets

RFC Text:
The PadN option does not have any alignment requirements. Its format is as follows:



The PadN option is used to insert two or more octets of padding in the Mobility Options area of a mobility message. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets. PadN Option data MUST be ignored by the receiver.

Identifier: RQ_001_1190
RFC Clause: 6.2.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
Within Mobility messages, the PadN option shall be used wher there is a need to insert two or more octets of padding in the Mobility Options area of a Mobility Header. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets

RFC Text:
The PadN option does not have any alignment requirements. Its format is as follows:

```
0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
|   Type = 1    | Option Length | Option Data
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
```

The PadN option is used to insert two or more octets of padding in the Mobility Options area of a mobility message. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets. PadN Option data MUST be ignored by the receiver.

Identifier: RQ_001_1190
RFC Clause: 6.2.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages, the PadN option shall be used wher there is a need to insert two or more octets of padding in the Mobility Options area of a Mobility Header. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets

RFC Text:
The PadN option does not have any alignment requirements. Its format is as follows:

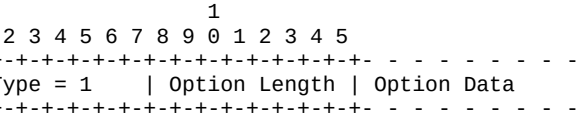
```
0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
|   Type = 1    | Option Length | Option Data
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
```

The PadN option is used to insert two or more octets of padding in the Mobility Options area of a mobility message. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets. PadN Option data MUST be ignored by the receiver.

Identifier: RQ_001_1191
RFC Clause: 6.2.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Within Mobility messages, PadN Option data MUST be ignored by the receiver.

RFC Text:
The PadN option does not have any alignment requirements. Its format is as follows:

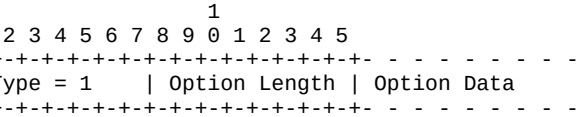


The PadN option is used to insert two or more octets of padding in the Mobility Options area of a mobility message. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets. **PadN Option data MUST be ignored by the receiver.**

Identifier: RQ_001_1191
RFC Clause: 6.2.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
Within Mobility messages, PadN Option data MUST be ignored by the receiver.

RFC Text:
The PadN option does not have any alignment requirements. Its format is as follows:

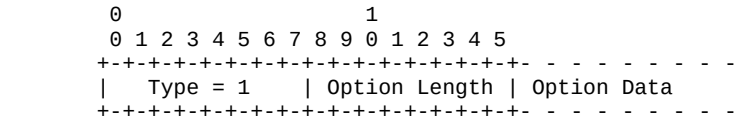


The PadN option is used to insert two or more octets of padding in the Mobility Options area of a mobility message. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets. **PadN Option data MUST be ignored by the receiver.**

Identifier: RQ_001_1191
RFC Clause: 6.2.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages, PadN Option data MUST be ignored by the receiver.

RFC Text:
The PadN option does not have any alignment requirements. Its format is as follows:

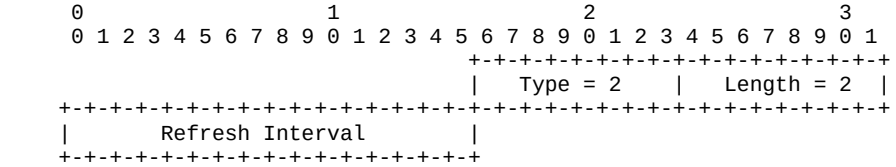


The PadN option is used to insert two or more octets of padding in the Mobility Options area of a mobility message. For N octets of padding, the Option Length field contains the value N-2, and the Option Data consists of N-2 zero-valued octets. **PadN Option data MUST be ignored by the receiver.**

Identifier: RQ_001_1192
RFC Clause: 6.2.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Within Mobility messages, the Binding Refresh Advice option has an alignment requirement of 2n

RFC Text:
The Binding Refresh Advice option has an alignment requirement of 2n. Its format is as follows:

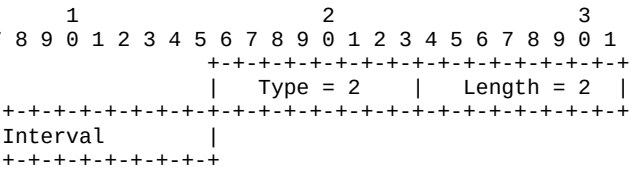


The Binding Refresh Advice option is only valid in the Binding Acknowledgement, and only on Binding Acknowledgements sent from the mobile node's home agent in reply to a home registration. The Refresh Interval is measured in units of four seconds, and indicates remaining time until the mobile node SHOULD send a new home registration to the home agent. The Refresh Interval MUST be set to indicate a smaller time interval than the Lifetime value of the Binding Acknowledgement.

Identifier: RQ_001_1193
RFC Clause: 6.2.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Within Mobility messages, the Binding Refresh Advice option is only valid in the Binding Acknowledgement, and only on Binding Acknowledgements sent from the mobile node's home agent in reply to a home registration.

RFC Text:
The Binding Refresh Advice option has an alignment requirement of 2n. Its format is as follows:

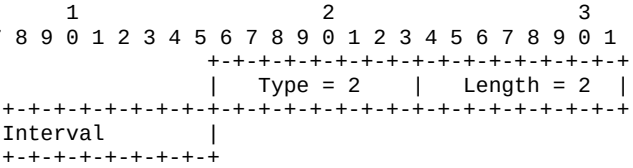


The Binding Refresh Advice option is only valid in the Binding Acknowledgement, and only on Binding Acknowledgements sent from the mobile node's home agent in reply to a home registration. The Refresh Interval is measured in units of four seconds, and indicates remaining time until the mobile node SHOULD send a new home registration to the home agent. The Refresh Interval MUST be set to indicate a smaller time interval than the Lifetime value of the Binding Acknowledgement.

Identifier: RQ_001_1194
RFC Clause: 6.2.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Within Mobility messages, the Binding Refresh Advice option Refresh Interval MUST be set to indicate a smaller time interval than the Lifetime value of the Binding Acknowledgement.

RFC Text:
The Binding Refresh Advice option has an alignment requirement of 2n. Its format is as follows:

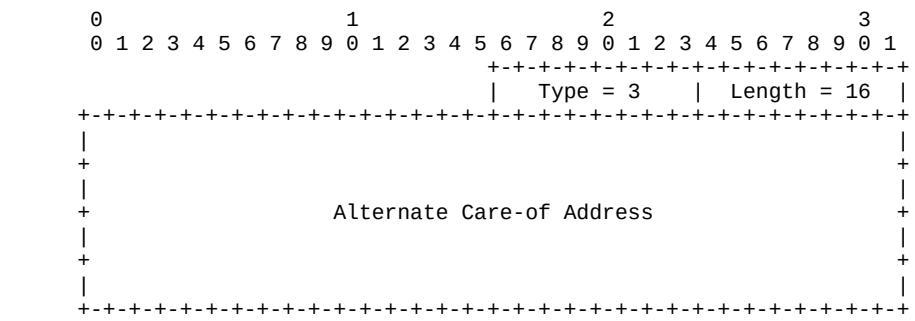


The Binding Refresh Advice option is only valid in the Binding Acknowledgement, and only on Binding Acknowledgements sent from the mobile node's home agent in reply to a home registration. The Refresh Interval is measured in units of four seconds, and indicates remaining time until the mobile node SHOULD send a new home registration to the home agent. **The Refresh Interval MUST be set to indicate a smaller time interval than the Lifetime value of the Binding Acknowledgement.**

Identifier: RQ_001_1195
RFC Clause: 6.2.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages, the Alternate Care-of Address option is valid only in Binding Update. The Alternate Care-of Address field contains an address to use as the care-of address for the binding, rather than using the Source Address of the packet as the care-of address.

RFC Text:
The Alternate Care-of Address option has an alignment requirement of 8n+6. Its format is as follows:



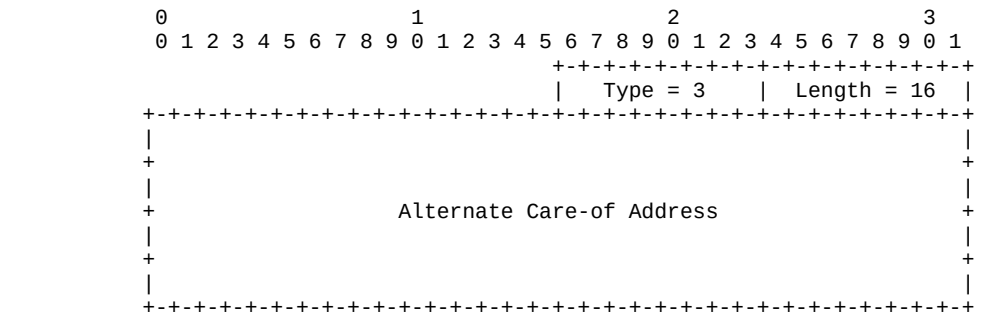
Normally, a Binding Update specifies the desired care-of address in the Source Address field of the IPv6 header. However, this is not possible in some cases, such as when the mobile node wishes to indicate a care-of address which it cannot use as a topologically correct source address (Section 6.1.7 and Section 11.7.2) or when the used security mechanism does not protect the IPv6 header (Section 11.7.1).

The Alternate Care-of Address option is provided for these situations. This option is valid only in Binding Update. The Alternate Care-of Address field contains an address to use as the care-of address for the binding, rather than using the Source Address of the packet as the care-of address.

Identifier: RQ_001_1196
RFC Clause: 6.2.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages, the Alternate Care-of Address field has an alignment requirement of 8n+6.

RFC Text:
The Alternate Care-of Address option has an alignment requirement of 8n+6. Its format is as follows:



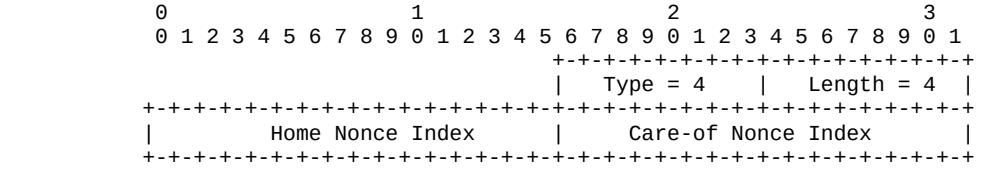
Normally, a Binding Update specifies the desired care-of address in the Source Address field of the IPv6 header. However, this is not possible in some cases, such as when the mobile node wishes to indicate a care-of address which it cannot use as a topologically correct source address (Section 6.1.7 and Section 11.7.2) or when the used security mechanism does not protect the IPv6 header (Section 11.7.1).

The Alternate Care-of Address option is provided for these situations. This option is valid only in Binding Update. The Alternate Care-of Address field contains an address to use as the care-of address for the binding, rather than using the Source Address of the packet as the care-of address.

Identifier: RQ_001_1197
RFC Clause: 6.2.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages the Nonce Indices option has an alignment requirement of 2n

RFC Text:
The Nonce Indices option has an alignment requirement of 2n. Its format is as follows:



The Nonce Indices option is valid only in the Binding Update message sent to a correspondent node, and only when present together with a Binding Authorization Data option. When the correspondent node authorizes the Binding Update, it needs to produce home and care-of keygen tokens from its stored random nonce values.

The Home Nonce Index field tells the correspondent node which nonce value to use when producing the home keygen token.

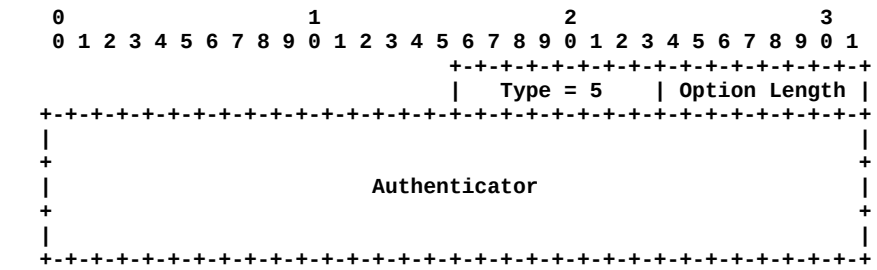
The Care-of Nonce Index field is ignored in requests to delete a binding. Otherwise, it tells the correspondent node which nonce value to use when producing the care-of keygen token.

Identifier: RQ_001_1198
RFC Clause: 6.2.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Within Mobility messages the Binding Authorization Data option must be the last mobility option and has an implicit alignment requirement is 8n + 2. The format of this option is as follows:

Bits	Field
1 - 8	Type Field =5
9 - 16	Option Length Field
17 - 112	Authenticator Field.

RFC Text:
The Binding Authorization Data option does not have alignment requirements as such. However, since this option must be the last mobility option, an implicit alignment requirement is 8n + 2. The format of this option is as follows:



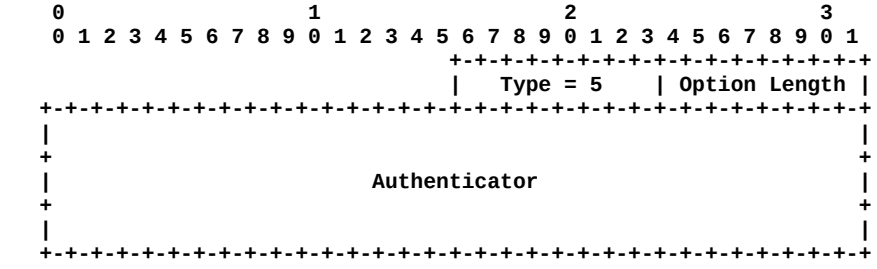
The Binding Authorization Data option is valid in the Binding Update and Binding Acknowledgement.

Identifier: RQ_001_1198
RFC Clause: 6.2.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages the Binding Authorization Data option must be the last mobility option and has an implicit alignment requirement is 8n + 2. The format of this option is as follows:

Bits	Field
1 - 8	Type Field =5
9 - 16	Option Length Field
17 - 112	Authenticator Field.

RFC Text:
The Binding Authorization Data option does not have alignment requirements as such. However, since this option must be the last mobility option, an implicit alignment requirement is 8n + 2. The format of this option is as follows:



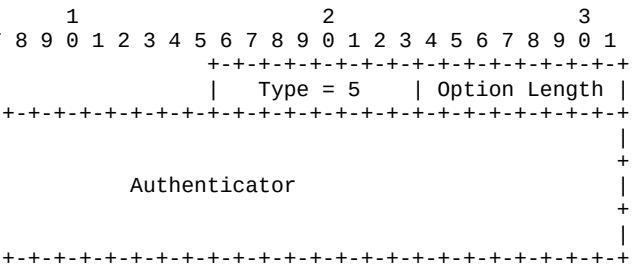
The Binding Authorization Data option is valid in the Binding Update and Binding Acknowledgement.

Identifier: RQ_001_1199
RFC Clause: 6.2.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Within Mobility messages the Binding Authorization Data option is valid in the Binding Update and Binding Acknowledgement.

RFC Text:

The Binding Authorization Data option does not have alignment requirements as such. However, since this option must be the last mobility option, an implicit alignment requirement is 8n + 2. The format of this option is as follows:



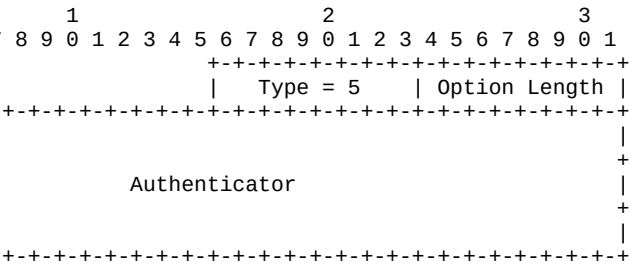
The Binding Authorization Data option is valid in the Binding Update and Binding Acknowledgement.

Identifier: RQ_001_1199
RFC Clause: 6.2.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages the Binding Authorization Data option is valid in the Binding Update and Binding Acknowledgement.

RFC Text:

The Binding Authorization Data option does not have alignment requirements as such. However, since this option must be the last mobility option, an implicit alignment requirement is 8n + 2. The format of this option is as follows:



The Binding Authorization Data option is valid in the Binding Update and Binding Acknowledgement.

Identifier: RQ_001_1200
RFC Clause: 6.2.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Within Mobility messages the Binding Authorization Data option's Option Length Field contains the length of the authenticator in octets.

RFC Text:
The Option Length field contains the length of the authenticator in octets.

The Authenticator field contains a cryptographic value which can be used to determine that the message in question comes from the right authority. Rules for calculating this value depends on the used authorization procedure.

For the return routability procedure, this option can appear in the Binding Update and Binding Acknowledgements. Rules for calculating the Authenticator value are the following:

```
Mobility Data = care-of address | correspondent | MH Data
Authenticator = First (96, HMAC_SHA1 (Kbm, Mobility Data))
```

Where | denotes concatenation. "Care-of address" is the care-of address which will be registered for the mobile node if the Binding Update succeeds, or the home address of the mobile node if this option is used in de-registration. Note also that this address might be different from the source address of the Binding Update message, if the Alternative Care-of Address mobility option is used, or when the lifetime of the binding is set to zero.

The "correspondent" is the IPv6 address of the correspondent node. Note that, if the message is sent to a destination which is itself mobile, the "correspondent" address may not be the address found in the Destination Address field of the IPv6 header; instead the home address from the type 2 Routing header should be used.

"MH Data" is the content of the Mobility Header, excluding the Authenticator field itself. The Authenticator value is calculated as if the Checksum field in the Mobility Header was zero. The Checksum in the transmitted packet is still calculated in the usual manner, with the calculated Authenticator being a part of the packet protected by the Checksum. Kbm is the binding management key, which is typically created using nonces provided by the correspondent node (see Section 9.4). Note that while the contents of a potential Home Address destination option are not covered in this formula, the rules for the calculation of the Kbm do take the home address in account. This ensures that the MAC will be different for different home addresses.

The first 96 bits from the MAC result are used as the Authenticator field.

Identifier: RQ_001_1200
RFC Clause: 6.2.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within Mobility messages the Binding Authorization Data option's Option Length Field contains the length of the authenticator in octets.

RFC Text:
The Option Length field contains the length of the authenticator in octets.

The Authenticator field contains a cryptographic value which can be used to determine that the message in question comes from the right authority. Rules for calculating this value depends on the used authorization procedure.

For the return routability procedure, this option can appear in the Binding Update and Binding Acknowledgements. Rules for calculating the Authenticator value are the following:

```
Mobility Data = care-of address | correspondent | MH Data
Authenticator = First (96, HMAC_SHA1 (Kbm, Mobility Data))
```

Where | denotes concatenation. "Care-of address" is the care-of address which will be registered for the mobile node if the Binding Update succeeds, or the home address of the mobile node if this option is used in de-registration. Note also that this address might be different from the source address of the Binding Update message, if the Alternative Care-of Address mobility option is used, or when the lifetime of the binding is set to zero.

The "correspondent" is the IPv6 address of the correspondent node. Note that, if the message is sent to a destination which is itself mobile, the "correspondent" address may not be the address found in the Destination Address field of the IPv6 header; instead the home address from the type 2 Routing header should be used.

"MH Data" is the content of the Mobility Header, excluding the Authenticator field itself. The Authenticator value is calculated as if the Checksum field in the Mobility Header was zero. The Checksum in the transmitted packet is still calculated in the usual manner, with the calculated Authenticator being a part of the packet protected by the Checksum. Kbm is the binding management key, which is typically created using nonces provided by the correspondent node (see Section 9.4). Note that while the contents of a potential Home Address destination option are not covered in this formula, the rules for the calculation of the Kbm do take the home address in account. This ensures that the MAC will be different for different home addresses.

The first 96 bits from the MAC result are used as the Authenticator field.

Identifier: RQ_001_1201
RFC Clause: 6.2.7
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

Within Mobility messages the Binding Authorization Data option's Authenticator Field, the rules for calculating the Authenticator value are the following:

```
Mobility Data = care-of address | correspondent | MH Data
Authenticator = First (96, HMAC_SHA1 (Kbm, Mobility Data))
```

Where | denotes concatenation.

RFC Text:

The Option Length field contains the length of the authenticator in octets.

The Authenticator field contains a cryptographic value which can be used to determine that the message in question comes from the right authority. Rules for calculating this value depends on the used authorization procedure.

For the return routability procedure, this option can appear in the Binding Update and Binding Acknowledgements. **Rules for calculating the Authenticator value are the following:**

```
Mobility Data = care-of address | correspondent | MH Data
Authenticator = First (96, HMAC_SHA1 (Kbm, Mobility Data))
```

Where | denotes concatenation. "Care-of address" is the care-of address which will be registered for the mobile node if the Binding Update succeeds, or the home address of the mobile node if this option is used in de-registration. Note also that this address might be different from the source address of the Binding Update message, if the Alternative Care-of Address mobility option is used, or when the lifetime of the binding is set to zero.

The "correspondent" is the IPv6 address of the correspondent node. Note that, if the message is sent to a destination which is itself mobile, the "correspondent" address may not be the address found in the Destination Address field of the IPv6 header; instead the home address from the type 2 Routing header should be used.

"MH Data" is the content of the Mobility Header, excluding the Authenticator field itself. The Authenticator value is calculated as if the Checksum field in the Mobility Header was zero. The Checksum in the transmitted packet is still calculated in the usual manner, with the calculated Authenticator being a part of the packet protected by the Checksum. Kbm is the binding management key, which is typically created using nonces provided by the correspondent node (see Section 9.4). Note that while the contents of a potential Home Address destination option are not covered in this formula, the rules for the calculation of the Kbm do take the home address in account. This ensures that the MAC will be different for different home addresses.

The first 96 bits from the MAC result are used as the Authenticator field.

Identifier: RQ_001_1201
RFC Clause: 6.2.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:

Within Mobility messages the Binding Authorization Data option's Authenticator Field, the rules for calculating the Authenticator value are the following:

```
Mobility Data = care-of address | correspondent | MH Data
Authenticator = First (96, HMAC_SHA1 (Kbm, Mobility Data))
```

Where | denotes concatenation.

RFC Text:

The Option Length field contains the length of the authenticator in octets.

The Authenticator field contains a cryptographic value which can be used to determine that the message in question comes from the right authority. Rules for calculating this value depends on the used authorization procedure.

For the return routability procedure, this option can appear in the Binding Update and Binding Acknowledgements. **Rules for calculating the Authenticator value are the following:**

```
Mobility Data = care-of address | correspondent | MH Data
Authenticator = First (96, HMAC_SHA1 (Kbm, Mobility Data))
```

Where | denotes concatenation. "Care-of address" is the care-of address which will be registered for the mobile node if the Binding Update succeeds, or the home address of the mobile node if this option is used in de-registration. Note also that this address might be different from the source address of the Binding Update message, if the Alternative Care-of Address mobility option is used, or when the lifetime of the binding is set to zero.

The "correspondent" is the IPv6 address of the correspondent node. Note that, if the message is sent to a destination which is itself mobile, the "correspondent" address may not be the address found in the Destination Address field of the IPv6 header; instead the home address from the type 2 Routing header should be used.

"MH Data" is the content of the Mobility Header, excluding the Authenticator field itself. The Authenticator value is calculated as if the Checksum field in the Mobility Header was zero. The Checksum in the transmitted packet is still calculated in the usual manner, with the calculated Authenticator being a part of the packet protected by the Checksum. Kbm is the binding management key, which is typically created using nonces provided by the correspondent node (see Section 9.4). Note that while the contents of a potential Home Address destination option are not covered in this formula, the rules for the calculation of the Kbm do take the home address in account. This ensures that the MAC will be different for different home addresses.

The first 96 bits from the MAC result are used as the Authenticator field.

Identifier: RQ_001_1202
RFC Clause: 6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:

The Home Address option is carried by the Destination Option extension header (Next Header value = 60) and is encoded in type-length-value (TLV) format as follows:

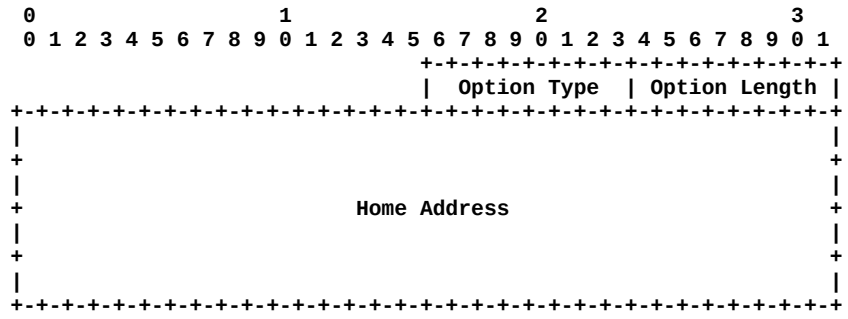
```
Bit                      Field
--------------------------------
1 - 8              Option Type Field,
9 -16              Option Length Field
17 - 144         Home Address Field.
```

RFC Text:

The Home Address option is carried by the Destination Option extension header (Next Header value = 60). It is used in a packet sent by a mobile node while away from home, to inform the recipient of the mobile node's home address.

The Home Address option is carried by the Destination Option extension header (Next Header value = 60). It is used in a packet sent by a mobile node while away from home, to inform the recipient of the mobile node's home address.

The Home Address option is encoded in type-length-value (TLV) format as follows:



Identifier: RQ_001_1203
RFC Clause: 6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the Home Address Option, the Option Type field is set to 201

RFC Text:

Option Type
201 = 0xC9

Identifier: RQ_001_1204
RFC Clause: 6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Home Address Option, the Option Length Field is an 8-bit unsigned integer.This field MUST be set to 16.

RFC Text:
Option Length

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields. This field MUST be set to 16.

Identifier: RQ_001_1205
RFC Clause: 6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The home address of the mobile node sending the packet MUST be a unicast routable address.

RFC Text:
The home address of the mobile node sending the packet. This address MUST be a unicast routable address.

The alignment requirement [11] for the Home Address option is 8n+6.

The three highest-order bits of the Option Type field are encoded to indicate specific processing of the option [11]; for the Home Address option, these three bits are set to 110. This indicates the following processing requirements:

o Any IPv6 node that does not recognize the Option Type must discard the packet, and if the packet's Destination Address was not a
multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address. The Pointer field in the
ICMP message SHOULD point at the Option Type field. Otherwise, for multicast addresses, the ICMP message MUST NOT be sent.

o The data within the option cannot change en route to the packet's final destination.

The Home Address option MUST be placed as follows:

o After the routing header, if that header is present

o Before the Fragment Header, if that header is present

o Before the AH Header or ESP Header, if either one of those headers
are present

For each IPv6 packet header, the Home Address Option MUST NOT appear more than once. However, an encapsulated packet [15] MAY contain a separate Home Address option associated with each encapsulating IP header.

The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet. In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

Identifier: RQ_001_1206
RFC Clause: 6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The alignment requirement for the Home Address option is 8n+6.

RFC Text:
The home address of the mobile node sending the packet. This address MUST be a unicast routable address.

The alignment requirement [11] for the Home Address option is 8n+6.

The three highest-order bits of the Option Type field are encoded to indicate specific processing of the option [11]; for the Home Address option, these three bits are set to 110. This indicates the following processing requirements:

o Any IPv6 node that does not recognize the Option Type must discard the packet, and if the packet's Destination Address was not a
multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address. The Pointer field in the
ICMP message SHOULD point at the Option Type field. Otherwise, for multicast addresses, the ICMP message MUST NOT be sent.

o The data within the option cannot change en route to the packet's final destination.

The Home Address option MUST be placed as follows:

o After the routing header, if that header is present

o Before the Fragment Header, if that header is present

o Before the AH Header or ESP Header, if either one of those headers
are present

For each IPv6 packet header, the Home Address Option MUST NOT appear more than once. However, an encapsulated packet [15] MAY contain a separate Home Address option associated with each encapsulating IP header.

The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet. In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

Identifier: RQ_001_1207
RFC Clause: 6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
For the Home Address option, the three highest-order bits of the Option Type field SHALL BE set to 110.

RFC Text:
The three highest-order bits of the Option Type field are encoded to indicate specific processing of the option [11]; for the Home Address option, these three bits are set to 110. This indicates the following processing requirements:

o Any IPv6 node that does not recognize the Option Type must discard the packet, and if the packet's Destination Address was not a
multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address. The Pointer field in the
ICMP message SHOULD point at the Option Type field. Otherwise, for multicast addresses, the ICMP message MUST NOT be sent.

o The data within the option cannot change en route to the packet's final destination.

The Home Address option MUST be placed as follows:

o After the routing header, if that header is present

o Before the Fragment Header, if that header is present

o Before the AH Header or ESP Header, if either one of those headers
are present

For each IPv6 packet header, the Home Address Option MUST NOT appear more than once. However, an encapsulated packet [15] MAY contain a separate Home Address option associated with each encapsulating IP header.

The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet. In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

Identifier: RQ_001_1208
RFC Clause: 6.3
Type: Mandatory
Applies to: Node

Requirement:
Any IPv6 node that does not recognize the Home Address Option Type must discard the packet.

RFC Text:
The three highest-order bits of the Option Type field are encoded to indicate specific processing of the option [11]; for the Home Address option, these three bits are set to 110. This indicates the following processing requirements:

o **Any IPv6 node that does not recognize the Option Type must discard the packet,** and if the packet's Destination Address was not a
multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address. The Pointer field in the
ICMP message SHOULD point at the Option Type field. Otherwise, for multicast addresses, the ICMP message MUST NOT be sent.

o The data within the option cannot change en route to the packet's final destination.

Identifier: RQ_001_1209
RFC Clause: 6.3
Type: Mandatory
Applies to: Node

Requirement:
Any IPv6 node that does not recognize the Home Address Option Type and if the packet's Destination Address was not a multicast address SHALL return an ICMP Parameter Problem, Code 2, message to the packet's Source Address

RFC Text:
The three highest-order bits of the Option Type field are encoded to indicate specific processing of the option [11]; for the Home Address option, these three bits are set to 110. This indicates the following processing requirements:

o **Any IPv6 node that does not recognize the Option Type must discard the packet, and if the packet's Destination Address was not a multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address.** The Pointer field in the ICMP message SHOULD point at the Option Type field. Otherwise, for multicast addresses, the ICMP message MUST NOT be sent.

o The data within the option cannot change en route to the packet's final destination.

Identifier: RQ_001_1210
RFC Clause: 6.3
Type: Recommendation
Applies to: Node

Requirement:
When sent in response to an unrecognized Home Address Option Type, the Pointer field in the ICMP Parameter Problem, Code 2, message SHOULD point at the Option Type field.

RFC Text:
The three highest-order bits of the Option Type field are encoded to indicate specific processing of the option [11]; for the Home Address option, these three bits are set to 110. This indicates the following processing requirements:

o Any IPv6 node that does not recognize the Option Type must discard the packet, and if the packet's Destination Address was not a multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address. **The Pointer field in the ICMP message SHOULD point at the Option Type field.** Otherwise, for multicast addresses, the ICMP message MUST NOT be sent.

o The data within the option cannot change en route to the packet's final destination.

Identifier: RQ_001_1211
RFC Clause: 6.3
Type: Mandatory
Applies to: Node

Requirement:
The ICMP Parameter Problem, Code 2, message MUST NOT be sent for multicast addresses.

RFC Text:
The three highest-order bits of the Option Type field are encoded to indicate specific processing of the option [11]; for the Home Address option, these three bits are set to 110. This indicates the following processing requirements:

o Any IPv6 node that does not recognize the Option Type must discard the packet, and if the packet's Destination Address was not a
multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address. The Pointer field in the
ICMP message SHOULD point at the Option Type field. **Otherwise, for multicast addresses, the ICMP message MUST NOT be sent.**

o The data within the option cannot change en route to the packet's final destination.

Identifier: RQ_001_1212
RFC Clause: 6.3
Type: Mandatory
Applies to: Node

Requirement:
The data within the the Home Address Option cannot change en route to the packet's final destination.

RFC Text:
The three highest-order bits of the Option Type field are encoded to indicate specific processing of the option [11]; for the Home Address option, these three bits are set to 110. This indicates the following processing requirements:

o Any IPv6 node that does not recognize the Option Type must discard the packet, and if the packet's Destination Address was not a
multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address. The Pointer field in the
ICMP message SHOULD point at the Option Type field. Otherwise, for multicast addresses, the ICMP message MUST NOT be sent.

o The data within the option cannot change en route to the packet's final destination.

Identifier: RQ_001_1213
RFC Clause: 6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Home Address option MUST be placed as follows; after the routing header(if that header is present), before the Fragment Header (if that header is present) and before the AH Header or ESP Header(if either one of those headers are present)

RFC Text:
The Home Address option MUST be placed as follows:

o After the routing header, if that header is present

o Before the Fragment Header, if that header is present

o Before the AH Header or ESP Header, if either one of those headers are present

Identifier: RQ_001_1214
RFC Clause: 6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
For each IPv6 packet header, the Home Address Option MUST NOT appear more than once.

RFC Text:
For each IPv6 packet header, the Home Address Option MUST NOT appear more than once. However, an encapsulated packet [15] MAY contain a separate Home Address option associated with each encapsulating IP header.

Identifier: RQ_001_1215
RFC Clause: 6.3
Type: Optional
Applies to: Mobile_Node

Requirement:
An encapsulated packet MAY contain a separate Home Address option associated with each encapsulating IP header.

RFC Text:
For each IPv6 packet header, the Home Address Option MUST NOT appear more than once. **However, an encapsulated packet [15] MAY contain a separate Home Address option associated with each encapsulating IP header.**

Identifier: RQ_001_1216
RFC Clause: 6.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
No state SHALL BE created or modified in the receiving node as a result of receiving a Home Address option in a packet.

RFC Text:
The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. **No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet.** In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

Identifier: RQ_001_1216
RFC Clause: 6.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
No state SHALL BE created or modified in the receiving node as a result of receiving a Home Address option in a packet.

RFC Text:
The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. **No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet.** In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

Identifier: RQ_001_1217
RFC Clause: 6.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache.

RFC Text:
The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet. **In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache** and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

Identifier: RQ_001_1217
RFC Clause: 6.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
The presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache.

RFC Text:
The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet. **In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache** and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

Identifier: RQ_001_1218
RFC Clause: 6.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The presence of a Home Address option in a received packet MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

RFC Text:
The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet. **In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.**

Identifier: RQ_001_1218
RFC Clause: 6.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
The presence of a Home Address option in a received packet MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.

RFC Text:
The inclusion of a Home Address destination option in a packet affects the receiving node's processing of only this single packet. No state is created or modified in the receiving node as a result of receiving a Home Address option in a packet. **In particular, the presence of a Home Address option in a received packet MUST NOT alter the contents of the receiver's Binding Cache and MUST NOT cause any changes in the routing of subsequent packets sent by this receiving node.**

Identifier: RQ_001_1219
RFC Clause: 6.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Type 2 Routing Header type is restricted to carry only one IPv6 address

RFC Text:
The new routing header uses a different type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to Mobile IPv6. **This routing header type (type 2) is restricted to carry only one IPv6 address.** All IPv6 nodes which process this routing header MUST verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node. The IP address contained in the routing header, since it is the mobile node's home address, MUST be a unicast routable address. Furthermore, if the scope of the home address is smaller than the scope of the care-of address, the mobile node MUST discard the packet (see Section 4.6).

Identifier: RQ_001_1219
RFC Clause: 6.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Type 2 Routing Header type is restricted to carry only one IPv6 address

RFC Text:
The new routing header uses a different type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to Mobile IPv6. **This routing header type (type 2) is restricted to carry only one IPv6 address.** All IPv6 nodes which process this routing header MUST verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node. The IP address contained in the routing header, since it is the mobile node's home address, MUST be a unicast routable address. Furthermore, if the scope of the home address is smaller than the scope of the care-of address, the mobile node MUST discard the packet (see Section 4.6).

Identifier: RQ_001_1220
RFC Clause: 6.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
All IPv6 nodes which process the type 2 routing header MUST verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node.

RFC Text:
The new routing header uses a different type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to Mobile IPv6. This routing header type (type 2) is restricted to carry only one IPv6 address. **All IPv6 nodes which process this routing header MUST verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node.** The IP address contained in the routing header, since it is the mobile node's home address, MUST be a unicast routable address. Furthermore, if the scope of the home address is smaller than the scope of the care-of address, the mobile node MUST discard the packet (see Section 4.6).

Identifier: RQ_001_1220
RFC Clause: 6.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
All IPv6 nodes which process the type 2 routing header MUST verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node.

RFC Text:
The new routing header uses a different type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to Mobile IPv6. This routing header type (type 2) is restricted to carry only one IPv6 address. **All IPv6 nodes which process this routing header MUST verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node.** The IP address contained in the routing header, since it is the mobile node's home address, MUST be a unicast routable address. Furthermore, if the scope of the home address is smaller than the scope of the care-of address, the mobile node MUST discard the packet (see Section 4.6).

Identifier: RQ_001_1221
RFC Clause: 6.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The IP address contained in the type 2 routing header MUST be a unicast routable address.

RFC Text:
The new routing header uses a different type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to Mobile IPv6. This routing header type (type 2) is restricted to carry only one IPv6 address. All IPv6 nodes which process this routing header MUST verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node. **The IP address contained in the routing header, since it is the mobile node's home address, MUST be a unicast routable address.** Furthermore, if the scope of the home address is smaller than the scope of the care-of address, the mobile node MUST discard the packet (see Section 4.6).

Identifier: RQ_001_1221
RFC Clause: 6.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
The IP address contained in the type 2 routing header MUST be a unicast routable address.

RFC Text:
The new routing header uses a different type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to Mobile IPv6. This routing header type (type 2) is restricted to carry only one IPv6 address. All IPv6 nodes which process this routing header MUST verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node. **The IP address contained in the routing header, since it is the mobile node's home address, MUST be a unicast routable address.** Furthermore, if the scope of the home address is smaller than the scope of the care-of address, the mobile node MUST discard the packet (see Section 4.6).

Identifier: RQ_001_1222
RFC Clause: 6.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Within the type 2 routing header, if the scope of the home address is smaller than the scope of the care-of address, the mobile node MUST discard the packet.

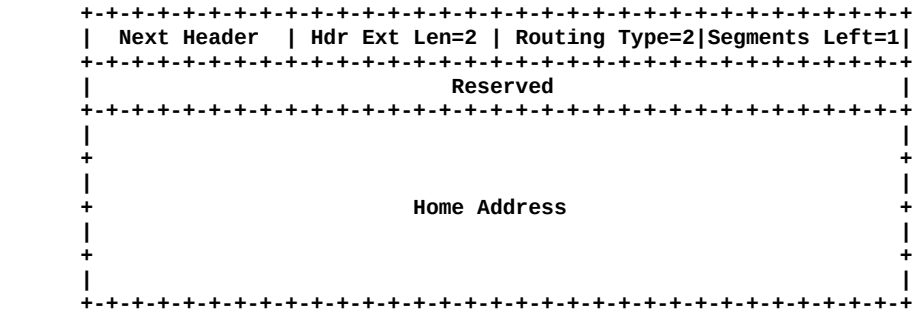
RFC Text:
The new routing header uses a different type than defined for "regular" IPv6 source routing, enabling firewalls to apply different rules to source routed packets than to Mobile IPv6. This routing header type (type 2) is restricted to carry only one IPv6 address. All IPv6 nodes which process this routing header MUST verify that the address contained within is the node's own home address in order to prevent packets from being forwarded outside the node. The IP address contained in the routing header, since it is the mobile node's home address, MUST be a unicast routable address. **Furthermore, if the scope of the home address is smaller than the scope of the care-of address, the mobile node MUST discard the packet (see Section 4.6).**

Identifier: RQ_001_1223
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The type 2 routing header has the following format;

Bits	Field
1 -8	Next Header Field,
9 - 16	Hdr Ext Len=2 Field,
17 - 24	Routing Type=2 Field,
25 - 32	Segments Left=1 Field,
33 - 64	Reserved Field
65 - 192	Home Address Field

RFC Text:
The type 2 routing header has the following format:

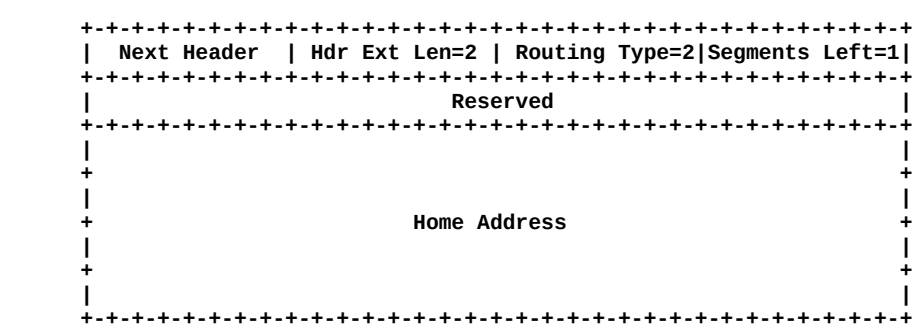


Identifier: RQ_001_1223
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The type 2 routing header has the following format;

```
Bits                    Field
-----------------------------
1 -8                    Next Header Field,
9 - 16                 Hdr Ext Len=2 Field,
17 - 24               Routing Type=2 Field,
25 - 32               Segments Left=1 Field,
33 - 64               Reserved Field
65 - 192             Home Address Field
```

RFC Text:
The type 2 routing header has the following format:



Identifier: RQ_001_1224
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Next Header Field of the Type 2 Routing Header SHALL BE an 8-bit selector

RFC Text:
Next Header

8-bit selector. Identifies the type of header immediately following the routing header. Uses the same values as the IPv6 Next Header field [11].

Identifier: RQ_001_1224
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Next Header Field of the Type 2 Routing Header SHALL BE an 8-bit selector

RFC Text:
Next Header

8-bit selector. Identifies the type of header immediately following the routing header. Uses the same values as the IPv6 Next Header field [11].

Identifier: RQ_001_1225
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Hdr Ext Len=2 Field of the Type 2 Routing Header SHALL BE an 8-bit unsigned integer

RFC Text:
Hdr Ext Len

2 (8-bit unsigned integer); length of the routing header in 8-octet units, not including the first 8 octets.

Identifier: RQ_001_1225
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Hdr Ext Len=2 Field of the Type 2 Routing Header SHALL BE an 8-bit unsigned integer

RFC Text:
Hdr Ext Len

2 (8-bit unsigned integer); length of the routing header in 8-octet units, not including the first 8 octets.

Identifier: RQ_001_1226
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Routing Type=2 Field of the Type 2 Routing Header SHALL BE an 8-bit unsigned integer

RFC Text:
Routing Type

2 (8-bit unsigned integer).

Identifier: RQ_001_1226
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Routing Type=2 Field of the Type 2 Routing Header SHALL BE an 8-bit unsigned integer

RFC Text:
Routing Type

2 (8-bit unsigned integer).

Identifier: RQ_001_1227
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Segments Left=1 Field of the Type 2 Routing Header SHALL BE an 8-bit unsigned integer

RFC Text:
Segments Left

1 (8-bit unsigned integer).

Identifier: RQ_001_1227
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Segments Left=1 Field of the Type 2 Routing Header SHALL BE an 8-bit unsigned integer

RFC Text:
Segments Left

1 (8-bit unsigned integer).

Identifier: RQ_001_1228
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Reserved Field of the Type 2 Routing Header SHALL BE a 32-bit reserved field.

RFC Text:
Reserved

> **32-bit reserved field.** The value MUST be initialized to zero by
> the sender, and MUST be ignored by the receiver.

Identifier: RQ_001_1228
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Reserved Field of the Type 2 Routing Header SHALL BE a 32-bit reserved field.

RFC Text:
Reserved

> **32-bit reserved field.** The value MUST be initialized to zero by
> the sender, and MUST be ignored by the receiver.

Identifier: RQ_001_1229
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The value of the Reserved Field of the Type 2 Routing Header MUST be initialized to zero the sender

RFC Text:
Reserved

32-bit reserved field. **The value MUST be initialized to zero by the sender,** and MUST be ignored by the receiver.

Identifier: RQ_001_1229
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The value of the Reserved Field of the Type 2 Routing Header MUST be initialized to zero the sender

RFC Text:
Reserved

32-bit reserved field. **The value MUST be initialized to zero by the sender,** and MUST be ignored by the receiver.

Identifier: RQ_001_1230
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The value of the Reserved Field of the Type 2 Routing Header MUST be ignored by the receiver

RFC Text:
Reserved

32-bit reserved field. The value MUST be initialized to zero by the sender, and **MUST be ignored by the receiver.**

Identifier: RQ_001_1231
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Home Address Field of the Type 2 Routing Header SHALL contain the Home Address of the destination Mobile Node.

RFC Text:
Home Address

The Home Address of the destination Mobile Node.

Identifier: RQ_001_1231
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Home Address Field of the Type 2 Routing Header SHALL contain the Home Address of the destination Mobile Node.

RFC Text:
Home Address

The Home Address of the destination Mobile Node.

Identifier: RQ_001_1232
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
For a type 2 routing header, the Hdr Ext Len MUST be 2.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Segments Left MUST be 1. The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers. If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header. A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

Identifier: RQ_001_1232
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
For a type 2 routing header, the Hdr Ext Len MUST be 2.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Segments Left MUST be 1. The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers. If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header. A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

Identifier: RQ_001_1233
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
For a type 2 routing header, the Segments Left MUST be 1.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. **Segments Left MUST be 1.** The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers. If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header. A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

Identifier: RQ_001_1233
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
For a type 2 routing header, the Segments Left MUST be 1.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. **Segments Left MUST be 1.** The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers. If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header. A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

Identifier: RQ_001_1234
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Segments Left MUST be 1. The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. **The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers.** If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header. A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

Identifier: RQ_001_1234
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Segments Left MUST be 1. The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. **The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers.** If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header. A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

Identifier: RQ_001_1235
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Segments Left MUST be 1. The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers. **If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header.** A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

Identifier: RQ_001_1235
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Segments Left MUST be 1. The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers. **If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header.** A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

Identifier: RQ_001_1236
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
A packet containing both a type 0 and a type 2 routing headers should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Segments Left MUST be 1. The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers. If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header. **A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.**

Identifier: RQ_001_1236
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
A packet containing both a type 0 and a type 2 routing headers should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.

RFC Text:
For a type 2 routing header, the Hdr Ext Len MUST be 2. The Segments Left value describes the number of route segments remaining; i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination. Segments Left MUST be 1. The ordering rules for extension headers in an IPv6 packet are described in Section 4.1 of RFC 2460 [11]. The type 2 routing header defined for Mobile IPv6 follows the same ordering as other routing headers. If both a type 0 and a type 2 routing header are present, the type 2 routing header should follow the other routing header. **A packet containing such nested encapsulation should be created as if the inner (type 2) routing header was constructed first and then treated as an original packet by the outer (type 0) routing header construction process.**

Identifier: RQ_001_1237
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The general procedures defined by IPv6 for routing headers suggest that a received routing header MAY be automatically "reversed" to construct a routing header for use in any response packets sent by upper-layer protocols, if the received packet is authenticated. This MUST NOT be done automatically for type 2 routing headers.

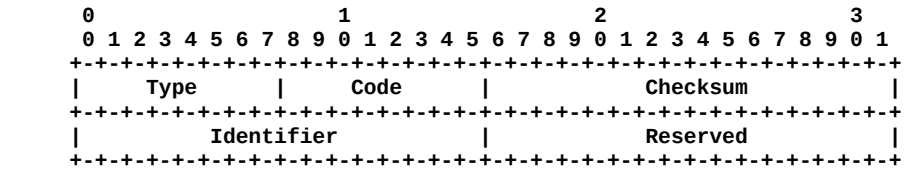
RFC Text:
In addition, the general procedures defined by IPv6 for routing headers suggest that a received routing header MAY be automatically "reversed" to construct a routing header for use in any response packets sent by upper-layer protocols, if the received packet is authenticated [6]. This MUST NOT be done automatically for type 2 routing headers.

Identifier: RQ_001_1238
RFC Clause: 6.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The ICMP Home Agent Address Discovery Request message has the following format;

Bit	Field
1 -8	Type Field,
9 - 16	Code Field,
17 - 32	Checksum Field,
33 - 48	Identifier Field
49 - 64	Reserved Field.

RFC Text:
The ICMP Home Agent Address Discovery Request message is used by a mobile node to initiate the dynamic home agent address discovery mechanism, as described in Section 11.4.1. The mobile node sends the Home Agent Address Discovery Request message to the Mobile IPv6 Home-Agents anycast address [16] for its own home subnet prefix. (Note that the currently defined anycast addresses may not work with all prefix lengths other than those defined in RFC 2373 [3, 35].)



Identifier: RQ_001_1239
RFC Clause: 6.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The ICMP Home Agent Address Discovery Request message's Type Field shall have the value 144

RFC Text:
Type

144

Identifier: RQ_001_1240
RFC Clause: 6.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The ICMP Home Agent Address Discovery Request message's Code Field shall have the value 0

RFC Text:
Code

0

Identifier: RQ_001_1241
RFC Clause: 6.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The ICMP Home Agent Address Discovery Request message's Checksum Field shall contain the ICMP checksum

RFC Text:
Checksum

The ICMP checksum [14].

Identifier: RQ_001_1242
RFC Clause: 6.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The ICMP Home Agent Address Discovery Request message's Identifier Field shall contain an identifier to aid in matching Home Agent Address Discovery Reply messages to this Home Agent Address Discovery Request message.

RFC Text:
Identifier

An identifier to aid in matching Home Agent Address Discovery Reply messages to this Home Agent Address Discovery Request message.

Identifier: RQ_001_1243
RFC Clause: 6.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The ICMP Home Agent Address Discovery Request message's Reserved Field MUST be initialized to zero by the sender

RFC Text:
Reserved

This field is unused. **It MUST be initialized to zero by the sender** and MUST be ignored by the receiver.

Identifier: RQ_001_1244
RFC Clause: 6.5
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Home Agent Address Discovery Request message's Reserved Field MUST be ignored by the receiver.

RFC Text:
Reserved

This field is unused. It MUST be initialized to zero by the sender and **MUST be ignored by the receiver.**

Identifier: RQ_001_1245
RFC Clause: 6.5
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the Source Address of the Home Agent Address Discovery Request message packet is not registered with the home agent, then the home agent MUST return the Home Agent Address Discovery Reply message directly to the Source Address chosen by the mobile node.

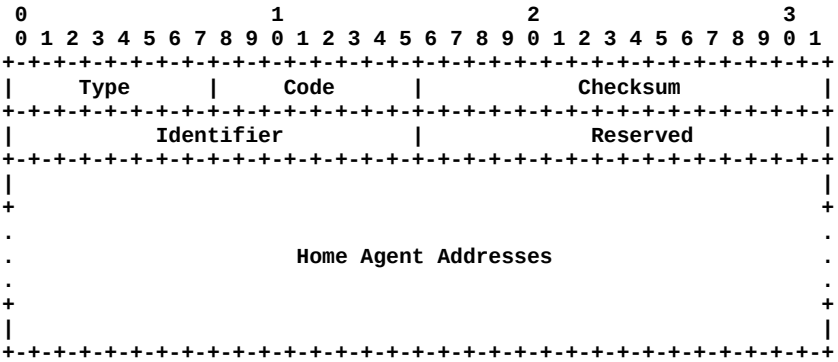
RFC Text:
The Source Address of the Home Agent Address Discovery Request message packet is typically one of the mobile node's current care-of addresses. At the time of performing this dynamic home agent address discovery procedure, it is likely that the mobile node is not registered with any home agent. Therefore, neither the nature of the address nor the identity of the mobile node can be established at this time. The home agent MUST then return the Home Agent Address Discovery Reply message directly to the Source Address chosen by the mobile node.

Identifier: RQ_001_1246
RFC Clause: 6.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Home Agent Address Discovery Reply message has the following format;

Bits	Field
1 -8	Type Field
9 - 16	Code Field
17 - 32	Checksum Field
33 - 48	Identifier Field
49 - 64	Reserved Field
65 - end	Home Agent Address

RFC Text:
The ICMP Home Agent Address Discovery Reply message is used by a home agent to respond to a mobile node that uses the dynamic home agent address discovery mechanism, as described in Section 10.5.



Identifier: RQ_001_1247
RFC Clause: 6.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Home Agent Address Discovery Reply message Type Field shall have the value 145

RFC Text:
Type

145

Identifier: RQ_001_1248
RFC Clause: 6.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Home Agent Address Discovery Reply message Checksum Field shall have contain the ICMP checksum

RFC Text:
Checksum

The ICMP checksum [14].

Identifier: RQ_001_1249
RFC Clause: 6.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Home Agent Address Discovery Reply message Identifier Field shall contain the identifier from the invoking Home Agent Address Discovery Request message.

RFC Text:
Identifier

The identifier from the invoking Home Agent Address Discovery Request message.

Identifier: RQ_001_1250
RFC Clause: 6.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Home Agent Address Discovery Reply message Reserved Field MUST be initialized to zero by the sender

RFC Text:
Reserved

This field is unused. **It MUST be initialized to zero by the sender** and MUST be ignored by the receiver.

Identifier: RQ_001_1251
RFC Clause: 6.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Home Agent Address Discovery Reply message Home Agent Addresses Field shall contain a list of addresses of home agents on the home link for the mobile node.

RFC Text:
Home Agent Addresses

A list of addresses of home agents on the home link for the mobile node. The number of addresses presented in the list is indicated by the remaining length of the IPv6 packet carrying the Home Agent Address Discovery Reply message.

Identifier: RQ_001_1252
RFC Clause: 6.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The ICMP Home Agent Address Discovery Reply message Reserved Field MUST be ignored by the receiver

RFC Text:
Reserved

This field is unused. It MUST be initialized to zero by the sender and **MUST be ignored by the receiver.**

Identifier: RQ_001_1253
RFC Clause: 6.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Home Agent Address Discovery Reply message Code Field shall have the value 0

RFC Text:
Code

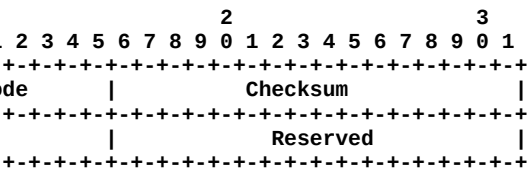
0

Identifier: RQ_001_1254
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The ICMP Mobile Prefix Solicitation Message message has the following format;

Bits	Field
1 -8	Type Field
9 - 16	Code Field
17 - 32	Checksum Field
33 - 48	Identifier Field
49 - 64	Reserved Field

RFC Text:
The ICMP Mobile Prefix Solicitation Message is sent by a mobile node to its home agent while it is away from home. The purpose of the message is to solicit a Mobile Prefix Advertisement from the home agent, which will allow the mobile node to gather prefix information about its home network. This information can be used to configure and update home address(es) according to changes in prefix information supplied by the home agent.



Identifier: RQ_001_1255
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the ICMP Mobile Prefix Solicitation Message, the Source Address field SHALL contain the mobile node's care-of address.

RFC Text:
IP Fields:

Source Address

The mobile node's care-of address.

Destination Address

The address of the mobile node's home agent. This home agent must be on the link that the mobile node wishes to learn prefix information about.

Hop Limit

Set to an initial hop limit value, similarly to any other unicast packet sent by the mobile node.

Identifier: RQ_001_1256
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the ICMP Mobile Prefix Solicitation Message, the Destination Address field SHALL contain the address of the mobile node's home agent.

RFC Text:
IP Fields:

Source Address

The mobile node's care-of address.

Destination Address

The address of the mobile node's home agent. This home agent must be on the link that the mobile node wishes to learn prefix information about.

Hop Limit

Set to an initial hop limit value, similarly to any other unicast packet sent by the mobile node.

Identifier: RQ_001_1257
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the ICMP Mobile Prefix Solicitation Message, the Hop Limit field SHALL be set to an initial hop limit value, similarly to any other unicast packet sent by the mobile node.

RFC Text:
IP Fields:

Source Address

The mobile node's care-of address.

Destination Address

The address of the mobile node's home agent. This home agent must be on the link that the mobile node wishes to learn prefix information about.

Hop Limit

Set to an initial hop limit value, similarly to any other unicast packet sent by the mobile node.

Identifier: RQ_001_1258
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Destination Option Extension Header for the ICMP Mobile Prefix Solicitation Message, the Home Address destination option MUST be included.

RFC Text:
Destination Option:

A Home Address destination option MUST be included.

Identifier: RQ_001_1259
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Mobile Prefix Solicitation Message, IPsec headers MUST be supported

RFC Text:
ESP header:

IPsec headers MUST be supported and SHOULD be used as described in Section 5.4.

Identifier: RQ_001_1260
RFC Clause: 6.7
Type: Recommendation
Applies to: Mobile_Node

Requirement:
In the ICMP Mobile Prefix Solicitation Message, IPsec headers SHOULD be used as described in Section 5.4.

RFC Text:
ESP header:

IPsec headers MUST be supported and **SHOULD be used as described in Section 5.4.**

Identifier: RQ_001_1261
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Mobile Prefix Solicitation Message, the Type field shall have the value 146

RFC Text:
Type

146

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching a future Mobile Prefix
Advertisement to this Mobile Prefix Solicitation.

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1262
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Mobile Prefix Solicitation Message, the Code field shall have the value 0

RFC Text:
Type

146

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching a future Mobile Prefix
Advertisement to this Mobile Prefix Solicitation.

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1263
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Mobile Prefix Solicitation Message, the Checksum field shall contain the ICMP checksum.

RFC Text:
Type

146

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching a future Mobile Prefix
Advertisement to this Mobile Prefix Solicitation.

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1264
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Mobile Prefix Solicitation Message, the Identifier field shall contain an identifier to aid in matching a future Mobile Prefix Advertisement to this Mobile Prefix Solicitation.

RFC Text:
Type

146

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching a future Mobile Prefix Advertisement to this Mobile Prefix Solicitation.

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1265
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Mobile Prefix Solicitation Message, the Reserved field shall MUST be initialized to zero by the sender.

RFC Text:
Type

146

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching a future Mobile Prefix Advertisement to this Mobile Prefix Solicitation.

Reserved

This field is unused. **It MUST be initialized to zero by the sender** and MUST be ignored by the receiver.

Identifier: RQ_001_1266
RFC Clause: 6.7
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Solicitation Message, the Reserved field MUST be ignored by the receiver.

RFC Text:
Type

146

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching a future Mobile Prefix Advertisement to this Mobile Prefix Solicitation.

Reserved

This field is unused. It MUST be initialized to zero by the sender and **MUST be ignored by the receiver.**

Identifier: RQ_001_1267
RFC Clause: 6.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When they are used, the options in a Mobile Prefix Solicitation message MUST respect the option format defined in RFC 2461.

RFC Text:
The Mobile Prefix Solicitation messages may have options. These options MUST use the option format defined in RFC 2461. This document does not define any option types for the Mobile Prefix Solicitation message, but future documents may define new options. Home agents MUST silently ignore any options they do not recognize and continue processing the message.

Identifier: RQ_001_1268
RFC Clause: 6.7
Type: Mandatory
Applies to: Home_Agent

Requirement:
If a Home agent doe not recognize some options in a Mobile Prefix Solicitation message it MUSTsilently ignore them and continue processing the message.

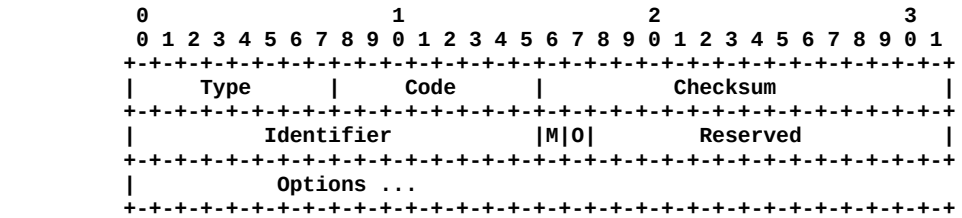
RFC Text:
The Mobile Prefix Solicitation messages may have options. These options MUST use the option format defined in RFC 2461. This document does not define any option types for the Mobile Prefix Solicitation message, but future documents may define new options. **Home agents MUST silently ignore any options they do not recognize and continue processing the message.**

Identifier: RQ_001_1269
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Mobile Prefix Advertisement Message has the following format;

Bits	Field
1 - 8	Type Field,
9 - 16	Code Field,
17 - 32	Checksum Field,
33 - 48	Identifier Field
49	M Bit
50	O Bit
51 - 64	Reserved Field
65 - end	Options Field.

RFC Text:
A home agent will send a Mobile Prefix Advertisement to a mobile node to distribute prefix information about the home link while the mobile node is traveling away from the home network. This will occur in response to a Mobile Prefix Solicitation with an Advertisement, or by an unsolicited Advertisement sent according to the rules in Section 10.6.



Identifier: RQ_001_1270
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the IP Header for the ICMP Mobile Prefix Advertisement Message, the Source Address field SHALL contain the home agent's address as the mobile node would expect to see it (i.e., same network prefix).

RFC Text:
IP Fields:

Source Address

The home agent's address as the mobile node would expect to see it (i.e., same network prefix).

Destination Address

If this message is a response to a Mobile Prefix Solicitation, this field contains the Source Address field from that packet. For unsolicited messages, the mobile node's care-of address SHOULD be used. Note that unsolicited messages can only be sent if the mobile node is currently registered with the home agent.

Identifier: RQ_001_1271
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the the ICMP Mobile Prefix Advertisement Message is a response to a Mobile Prefix Solicitation, the Destination Address field of the IP Header, SHALL contain the the Source Address field from that packet

RFC Text:
IP Fields:

Source Address

The home agent's address as the mobile node would expect to see it (i.e., same network prefix).

Destination Address

If this message is a response to a Mobile Prefix Solicitation, this field contains the Source Address field from that packet. For unsolicited messages, the mobile node's care-of address SHOULD be used. Note that unsolicited messages can only be sent if the mobile node is currently registered with the home agent.

Identifier: RQ_001_1272
RFC Clause: 6.8
Type: Recommendation
Applies to: Home_Agent

Requirement:
If the the ICMP Mobile Prefix Advertisement Message is an unsolicited message, the Destination Address field of the IP Header, SHOULD contain the mobile node's care-of address.

RFC Text:
IP Fields:

Source Address

The home agent's address as the mobile node would expect to see it (i.e., same network prefix).

Destination Address

If this message is a response to a Mobile Prefix Solicitation, this field contains the Source Address field from that packet. **For unsolicited messages, the mobile node's care-of address SHOULD be used.** Note that unsolicited messages can only be sent if the mobile node is currently registered with the home agent.

Identifier: RQ_001_1273
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Destination Option Extension Header for the ICMP Mobile Prefix Advertisement Message, the Routing header MUST include a type 2 routing header.

RFC Text:
Routing header:

A type 2 routing header MUST be included.

Identifier: RQ_001_1274
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Advertisement Message, IPsec headers MUST be supported.

RFC Text:
ESP header:

IPsec headers MUST be supported and SHOULD be used as described in Section 5.4.

Identifier: RQ_001_1275
RFC Clause: 6.8
Type: Recommendation
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Advertisement Message, IPsec headers SHOULD be used as described in Section 5.4..

RFC Text:
ESP header:

IPsec headers MUST be supported and **SHOULD be used as described in Section 5.4.**

Identifier: RQ_001_1276
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Advertisement Message, the Type Field shall have the value 147

RFC Text:
ICMP Fields:

Type

147

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

M

1-bit Managed Address Configuration flag. When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is described in [12, 13].

O

1-bit Other Stateful Configuration flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information. The use of this flag is described in [12, 13].

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1277
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Advertisement Message, the Code Field shall have the value 0

RFC Text:
ICMP Fields:

Type

147

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

M

1-bit Managed Address Configuration flag. When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is described in [12, 13].

O

1-bit Other Stateful Configuration flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information. The use of this flag is described in [12, 13].

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1278
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Advertisement Message, the Checksum Field shall contain the ICMP checksum.

RFC Text:
ICMP Fields:

Type

147

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

M

1-bit Managed Address Configuration flag. When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is described in [12, 13].

O

1-bit Other Stateful Configuration flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information. The use of this flag is described in [12, 13].

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1279
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Advertisement Message, the Identifier Field shall contain an identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

RFC Text:
ICMP Fields:

Type

147

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

M

1-bit Managed Address Configuration flag. When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is described in [12, 13].

O

1-bit Other Stateful Configuration flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information. The use of this flag is described in [12, 13].

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1280
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Advertisement Message, the M Bit shall contain a 1-bit Managed Address Configuration flag.

RFC Text:
ICMP Fields:

Type

147

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

M

1-bit Managed Address Configuration flag. When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is described in [12, 13].

O

1-bit Other Stateful Configuration flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information. The use of this flag is described in [12, 13].

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1281
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Advertisement Message, the O Bit shall contain a 1-bit Other Stateful Configuration flag.

RFC Text:
ICMP Fields:

Type

147

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

M

1-bit Managed Address Configuration flag. When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is described in [12, 13].

O

1-bit Other Stateful Configuration flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information. The use of this flag is described in [12, 13].

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1282
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the ICMP Mobile Prefix Advertisement Message, the Reserved field MUST be initialized to zero by the sender

RFC Text:
ICMP Fields:

Type

147

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

M

1-bit Managed Address Configuration flag. When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is described in [12, 13].

O

1-bit Other Stateful Configuration flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information. The use of this flag is described in [12, 13].

Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1283
RFC Clause: 6.8
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Mobile Prefix Advertisement Message, the Reserved field MUST be ignored by the receiver.

RFC Text:
ICMP Fields:

Type

147

Code

0

Checksum

The ICMP checksum [14].

Identifier

An identifier to aid in matching this Mobile Prefix Advertisement to a previous Mobile Prefix Solicitation.

M

1-bit Managed Address Configuration flag. When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is described in [12, 13].

O

1-bit Other Stateful Configuration flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information. The use of this flag is described in [12, 13].

Reserved

This field is unused. It MUST be initialized to zero by the sender and **MUST be ignored by the receiver.**

Identifier: RQ_001_1284
RFC Clause: 6.8
Type: Optional
Applies to: Home_Agent

Requirement:
The ICMP Mobile Prefix Advertisement Message, may have options

RFC Text:
The Mobile Prefix Advertisement messages may have options. These options MUST use the option format defined in RFC 2461 [12]. This document defines one option which may be carried in a Mobile Prefix Advertisement message, but future documents may define new options. Mobile nodes MUST silently ignore any options they do not recognize and continue processing the message.

Identifier: RQ_001_1285
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
The ICMP Mobile Prefix Advertisement Message, any options present MUST use the option format defined in RFC 2461

RFC Text:
The Mobile Prefix Advertisement messages may have options. **These options MUST use the option format defined in RFC 2461 [12].** This document defines one option which may be carried in a Mobile Prefix Advertisement message, but future documents may define new options. Mobile nodes MUST silently ignore any options they do not recognize and continue processing the message.

Identifier: RQ_001_1286
RFC Clause: 6.8
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Mobile nodes MUST silently ignore any options they do not recognize and continue processing the ICMP Mobile Prefix Advertisement Message.

RFC Text:
The Mobile Prefix Advertisement messages may have options. These options MUST use the option format defined in RFC 2461 [12]. This document defines one option which may be carried in a Mobile Prefix Advertisement message, but future documents may define new options. **Mobile nodes MUST silently ignore any options they do not recognize and continue processing the message.**

Identifier: RQ_001_1287
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
Each ICMP Mobile Prefix Advertisement Message, contains one or more Prefix Information options.

RFC Text:
Prefix Information

Each message contains one or more Prefix Information options. Each option carries the prefix(es) that the mobile node should use to configure its home address(es). Section 10.6 describes which prefixes should be advertised to the mobile node.

The Prefix Information option is defined in Section 4.6.2 of RFC 2461 [12], with modifications defined in Section 7.2 of this specification. The home agent MUST use this modified Prefix Information option to send home network prefixes as defined in Section 10.6.1.

Identifier: RQ_001_1288
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST use ICMP Mobile Prefix Advertisement Message's Prefix Information option to send home network prefixes as defined in Section 10.6.1.

RFC Text:
Prefix Information

Each message contains one or more Prefix Information options. Each option carries the prefix(es) that the mobile node should use to configure its home address(es). Section 10.6 describes which prefixes should be advertised to the mobile node.

The Prefix Information option is defined in Section 4.6.2 of RFC 2461 [12], with modifications defined in Section 7.2 of this specification. **The home agent MUST use this modified Prefix Information option to send home network prefixes as defined in Section 10.6.1.**

Identifier: RQ_001_1289
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the ICMP Mobile Prefix Advertisement Message is sent in response to a Mobile Prefix Solicitation, the home agent MUST copy the Identifier value from that message into the Identifier field of the Advertisement.

RFC Text:
If the Advertisement is sent in response to a Mobile Prefix Solicitation, the home agent MUST copy the Identifier value from that message into the Identifier field of the Advertisement.

Identifier: RQ_001_1290
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST NOT send more than one Mobile Prefix Advertisement message per second to any mobile node.

RFC Text:
The home agent MUST NOT send more than one Mobile Prefix Advertisement message per second to any mobile node.

Identifier: RQ_001_1291
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

Requirement:
The M and O bits in the Mobile Prefix Advertisement message MUST be cleared if the Home Agent DHCPv6 support is not provided.

RFC Text:
The M and O bits MUST be cleared if the Home Agent DHCPv6 support is not provided. If such support is provided then they are set in concert with the home network's administrative settings.

Identifier: RQ_001_1292
RFC Clause: 6.8
Type: Mandatory
Applies to: Home_Agent

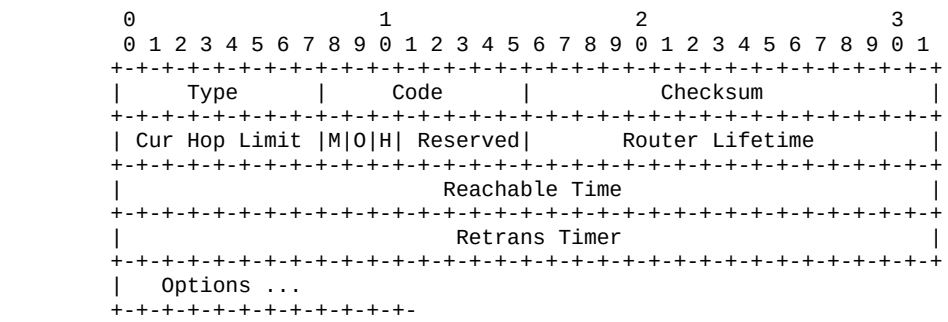
Requirement:
If Home Agent DHCPv6 support is provided, the M and O bits in the Mobile Prefix Advertisement message are set in concert with the home network's administrative settings.

RFC Text:
The M and O bits MUST be cleared if the Home Agent DHCPv6 support is not provided. **If such support is provided then they are set in concert with the home network's administrative settings.**

Identifier: RQ_001_1293
RFC Clause: 7.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Modified Router Advertisement message modifies the format specified for Neighbourhood Discovery by the addition of a single flag bit (H bit), before the Reserved Field, to indicate that the router sending the Advertisement message is serving as a home agent on this link.

RFC Text:
Mobile IPv6 modifies the format of the Router Advertisement message [12] by the addition of a single flag bit to indicate that the router sending the Advertisement message is serving as a home agent on this link. The format of the Router Advertisement message is as follows:



Identifier: RQ_001_1294
RFC Clause: 7.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Modified Router Advertisement message, the Home Agent (H) bit is set.

RFC Text:
Home Agent (H)

The Home Agent (H) bit is set in a Router Advertisement to indicate that the router sending this Router Advertisement is also functioning as a Mobile IPv6 home agent on this link.

Identifier: RQ_001_1295
RFC Clause: 7.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Modified Router Advertisement message, the Reserved Field is reduced from a 6-bit field to a 5-bit field to account for the addition of the H bit.

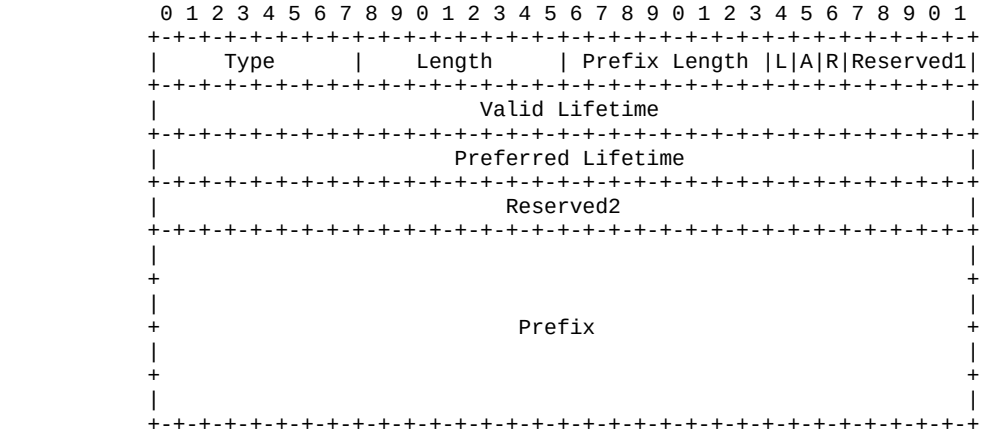
RFC Text:
Reserved

Reduced from a 6-bit field to a 5-bit field to account for the addition of the above bit.

Identifier: RQ_001_1296
RFC Clause: 7.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Modified Prefix Information Option message modifies the format specified for Neighbourhood Discovery by the addition of a single flag bit (R), before the Reserved1 Field, in the format of a Prefix Information option for use in Router Advertisement messages.

RFC Text:
Mobile IPv6 extends Neighbor Discovery to allow a router to advertise its global address, by the addition of a single flag bit in the format of a Prefix Information option for use in Router Advertisement messages. The format of the Prefix Information option is as follows:



Identifier: RQ_001_1297
RFC Clause: 7.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
When, in the Modified Prefix Information Option message, the 1 bit Router Address (R) bit is set, it indicates that the Prefix field contains a complete IP address assigned to the sending router.

RFC Text:
Router Address (R)

1-bit router address flag. When set, indicates that the Prefix field contains a complete IP address assigned to the sending router. The indicated prefix is the first Prefix Length bits of the Prefix field. The router IP address has the same scope and conforms to the same lifetime values as the advertised prefix. This use of the Prefix field is compatible with its use in advertising the prefix itself, since Prefix Advertisement uses only the leading bits. Interpretation of this flag bit is thus independent of the processing required for the On-Link (L) and Autonomous Address-Configuration (A) flag bits.

Identifier: RQ_001_1298
RFC Clause: 7.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Modified Prefix Information Option message, the Reserved1 Field is reduced from a 6-bit field to a 5-bit field to account for the addition of the R bit.

RFC Text:
Reserved1

Reduced from a 6-bit field to a 5-bit field to account for the addition of the above bit.

Identifier: RQ_001_1299
RFC Clause: 7.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In a Router Advertisement, a home agent MUST include at least one Prefix Information option with the Router Address (R) bit set.

RFC Text:
In a Router Advertisement, a home agent MUST, and all other routers MAY, include at least one Prefix Information option with the Router Address (R) bit set. Neighbor Discovery specifies that, if including all options in a Router Advertisement causes the size of the Advertisement to exceed the link MTU, multiple Advertisements can be sent, each containing a subset of the options [12]. Also, when sending unsolicited multicast Router Advertisements more frequently than the limit specified in RFC 2461 [12], the sending router need not include all options in each of these Advertisements. However, in both of these cases the router SHOULD include at least one Prefix Information option with the Router Address (R) bit set in each such advertisement, if this bit is set in some advertisement sent by the router.

Identifier: RQ_001_1300
RFC Clause: 7.2
Type: Optional
Applies to: Router

Requirement:
In a Router Advertisement routers MAY include at least one Prefix Information option with the Router Address (R) bit set.

RFC Text:
In a Router Advertisement, a home agent MUST, and all other routers MAY, include at least one Prefix Information option with the Router Address (R) bit set. Neighbor Discovery specifies that, if including all options in a Router Advertisement causes the size of the Advertisement to exceed the link MTU, multiple Advertisements can be sent, each containing a subset of the options [12]. Also, when sending unsolicited multicast Router Advertisements more frequently than the limit specified in RFC 2461 [12], the sending router need not include all options in each of these Advertisements. However, in both of these cases the router SHOULD include at least one Prefix Information option with the Router Address (R) bit set in each such advertisement, if this bit is set in some advertisement sent by the router.

Identifier: RQ_001_1301
RFC Clause: 7.2
Type: Recommendation
Applies to: Router

Requirement:
Barring changes in the prefixes for the link, routers that send multiple Router Advertisements with the Router Address (R) bit set in some of the included Prefix Information options SHOULD provide at least one option and router address which stays the same in all of the Advertisements.

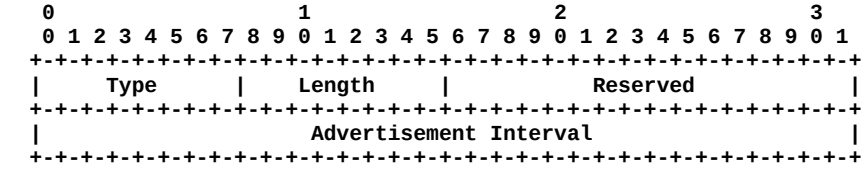
RFC Text:
In addition, the following requirement can assist mobile nodes in movement detection. **Barring changes in the prefixes for the link, routers that send multiple Router Advertisements with the Router Address (R) bit set in some of the included Prefix Information options SHOULD provide at least one option and router address which stays the same in all of the Advertisements.**

Identifier: RQ_001_1302
RFC Clause: 7.3
Type: Mandatory
Applies to: Router

Requirement:
The New Advertisement Interval option message has the following format;

Bit	Field
1 - 8	Type field,
9 - 16	Length field,
17 - 32	Reserved field
33 - 64	Advertisement Interval field.

RFC Text:
Mobile IPv6 defines a new Advertisement Interval option, used in Router Advertisement messages to advertise the interval at which the sending router sends unsolicited multicast Router Advertisements. The format of the Advertisement Interval option is as follows:



Identifier: RQ_001_1303
RFC Clause: 7.3
Type: Mandatory
Applies to: Router

Requirement:
In the New Advertisement Interval option message, the Type field has a value of 7

RFC Text:
Type

7

Identifier: RQ_001_1304
RFC Clause: 7.3
Type: Mandatory
Applies to: Router

Requirement:
In the New Advertisement Interval option message, the Length field is an 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value of this field MUST be 1.

RFC Text:
Length

8-bit unsigned integer. The length of the option (including the type and length fields) is in units of 8 octets. The value of this field MUST be 1.

Identifier: RQ_001_1305
RFC Clause: 7.3
Type: Mandatory
Applies to: Router

Requirement:
In the New Advertisement Interval option message, the Reserved field MUST be initialized to zero by the sender

RFC Text:
Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1306
RFC Clause: 7.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the New Advertisement Interval option message, the Reserved field MUST be ignored by the receiver.

RFC Text:
Reserved

This field is unused. It MUST be initialized to zero by the sender and **MUST be ignored by the receiver.**

Identifier: RQ_001_1307
RFC Clause: 7.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the New Advertisement Interval option message, the Advertisement Interval field is a 32-bit unsigned integer which MUST be equal to the value MaxRtrAdvInterval, expressed in milliseconds.

RFC Text:
Advertisement Interval

32-bit unsigned integer. The maximum time, in milliseconds, between successive unsolicited Router Advertisement messages sent by this router on this network interface. **Using the conceptual router configuration variables defined by Neighbor Discovery [12], this field MUST be equal to the value MaxRtrAdvInterval, expressed in milliseconds.**

Identifier: RQ_001_1308
RFC Clause: 7.3
Type: Optional
Applies to: Home_Agent

Requirement:
Routers MAY include the New Advertisement Interval option message in their Router Advertisements.

RFC Text:
Routers MAY include this option in their Router Advertisements. A mobile node receiving a Router Advertisement containing this option SHOULD utilize the specified Advertisement Interval for that router in its movement detection algorithm, as described in Section 11.5.1.

Identifier: RQ_001_1309
RFC Clause: 7.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
A mobile node receiving a Router Advertisement containing the New Advertisement Interval option SHOULD utilize the specified Advertisement Interval for that router in its movement detection algorithm, as described in Section 11.5.1.

RFC Text:
Routers MAY include this option in their Router Advertisements. **A mobile node receiving a Router Advertisement containing this option SHOULD utilize the specified Advertisement Interval for that router in its movement detection algorithm, as described in Section 11.5.1.**

Identifier: RQ_001_1310
RFC Clause: 7.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The New Advertisement Interval option MUST be silently ignored for other Neighbor Discovery messages.

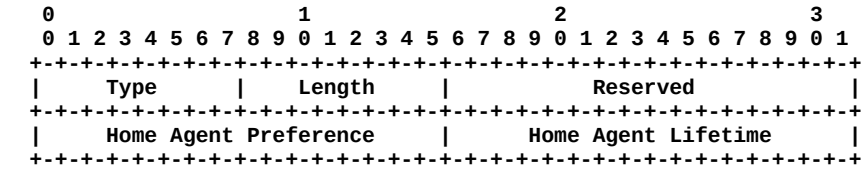
RFC Text:
This option MUST be silently ignored for other Neighbor Discovery messages.

Identifier: RQ_001_1311
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
The new Home Agent Information option message has the following format;

Bit	Field
1 - 8	Type field,
9 - 16	Length field,
17 - 32	Reserved field
33 - 48	Home Agent Preference field
49 - 64	Home Agent Lifetime field

RFC Text:
Mobile IPv6 defines a new Home Agent Information option, used in Router Advertisements sent by a home agent to advertise information specific to this router's functionality as a home agent. The format of the Home Agent Information option is as follows:



Identifier: RQ_001_1312
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the new Home Agent Information option message the Type field has a value of 8

RFC Text:
Type

8

Identifier: RQ_001_1313
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the new Home Agent Information option message the Length field is an 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value of this field MUST be 1.

RFC Text:
Length

8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value of this field MUST be 1.

Identifier: RQ_001_1314
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the new Home Agent Information option message the Reserved field MUST be initialized to zero by the sender.

RFC Text:
Reserved

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_1315
RFC Clause: 7.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the new Home Agent Information option message the Reserved field MUST be ignored by the receiver.

RFC Text:
Reserved

This field is unused. It MUST be initialized to zero by the sender **and MUST be ignored by the receiver.**

Identifier: RQ_001_1316
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
The new Home Agent Information option is a 16-bit unsigned integer.

RFC Text:
Home Agent Preference

16-bit unsigned integer. The preference for the home agent sending this Router Advertisement, for use in ordering the addresses returned to a mobile node in the Home Agent Addresses field of a Home Agent Address Discovery Reply message. Higher values mean more preferable. If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the preference value for this home agent MUST be considered to be 0. Greater values indicate a more preferable home agent than lower values.

The manual configuration of the Home Agent Preference value is described in Section 8.4. In addition, the sending home agent MAY dynamically set the Home Agent Preference value, for example basing it on the number of mobile nodes it is currently serving or on its remaining resources for serving additional mobile nodes; such dynamic settings are beyond the scope of this document. Any such dynamic setting of the Home Agent Preference, however, MUSTset the preference appropriately, relative to the default Home Agent Preference value of 0 that may be in use by some home agents on this link (i.e., a home agent not including a Home Agent Information option in its Router Advertisements will be considered to have a Home Agent Preference value of 0).

Identifier: RQ_001_1317
RFC Clause: 7.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If new Home Agent Information option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the preference value for this home agent MUST be considered to be 0.

RFC Text:
Home Agent Preference

16-bit unsigned integer. The preference for the home agent sending this Router Advertisement, for use in ordering the addresses returned to a mobile node in the Home Agent Addresses field of a Home Agent Address Discovery Reply message. Higher values mean more preferable. **If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the preference value for this home agent MUST be considered to be 0. Greater values indicate a more preferable home agent than lower values.**

The manual configuration of the Home Agent Preference value is described in Section 8.4. In addition, the sending home agent MAY dynamically set the Home Agent Preference value, for example basing it on the number of mobile nodes it is currently serving or on its remaining resources for serving additional mobile nodes; such dynamic settings are beyond the scope of this document. Any such dynamic setting of the Home Agent Preference, however, MUSTset the preference appropriately, relative to the default Home Agent Preference value of 0 that may be in use by some home agents on this link (i.e., a home agent not including a Home Agent Information option in its Router Advertisements will be considered to have a Home Agent Preference value of 0).

Identifier: RQ_001_1318
RFC Clause: 7.4
Type: Optional
Applies to: Home_Agent

Requirement:
The sending home agent MAY dynamically set the Home Agent Preference value in the new Home Agent Information option message.

RFC Text:
Home Agent Preference

16-bit unsigned integer. The preference for the home agent sending this Router Advertisement, for use in ordering the addresses returned to a mobile node in the Home Agent Addresses field of a Home Agent Address Discovery Reply message. Higher values mean more preferable. If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the preference value for this home agent MUST be considered to be 0. Greater values indicate a more preferable home agent than lower values.

The manual configuration of the Home Agent Preference value is described in Section 8.4. **In addition, the sending home agent MAY dynamically set the Home Agent Preference value, for example basing it on the number of mobile nodes it is currently serving or on its remaining resources for serving additional mobile nodes; such dynamic settings are beyond the scope of this document.** Any such dynamic setting of the Home Agent Preference, however, MUSTset the preference appropriately, relative to the default Home Agent Preference value of 0 that may be in use by some home agents on this link (i.e., a home agent not including a Home Agent Information option in its Router Advertisements will be considered to have a Home Agent Preference value of 0).

Identifier: RQ_001_1319
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the sending home agent dynamically sets the Home Agent Preference value in the new Home Agent Information option message, it MUSTset the preference appropriately, relative to the default Home Agent Preference value of 0 that may be in use by some home agents on this link.

RFC Text:
Home Agent Preference

16-bit unsigned integer. The preference for the home agent sending this Router Advertisement, for use in ordering the addresses returned to a mobile node in the Home Agent Addresses field of a Home Agent Address Discovery Reply message. Higher values mean more preferable. If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the preference value for this home agent MUST be considered to be 0. Greater values indicate a more preferable home agent than lower values.

The manual configuration of the Home Agent Preference value is described in Section 8.4. In addition, the sending home agent MAY dynamically set the Home Agent Preference value, for example basing it on the number of mobile nodes it is currently serving or on its remaining resources for serving additional mobile nodes; such dynamic settings are beyond the scope of this document. **Any such dynamic setting of the Home Agent Preference, however, MUSTset the preference appropriately, relative to the default Home Agent Preference value of 0 that may be in use by some home agents on this link (i.e., a home agent not including a Home Agent Information option in its Router Advertisements will be considered to have a Home Agent Preference value of 0).**

Identifier: RQ_001_1320
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the new Home Agent Information option message the Home Agent Lifetime field is a 16-bit unsigned integer with a default value which is the same as the Router Lifetime, as specified in the main body of the Router Advertisement.

RFC Text:
Home Agent Lifetime

16-bit unsigned integer. The lifetime associated with the home agent in units of seconds. The default value is the same as the Router Lifetime, as specified in the main body of the Router Advertisement. The maximum value corresponds to 18.2 hours. A value of 0 MUST NOT be used. The Home Agent Lifetime applies only to this router's usefulness as a home agent; it does not apply to information contained in other message fields or options.

Identifier: RQ_001_1321
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the new Home Agent Information option message the maximum value of the Home Agent Lifetime field corresponds to 18.2 hours.

RFC Text:
Home Agent Lifetime

16-bit unsigned integer. The lifetime associated with the home agent in units of seconds. The default value is the same as the Router Lifetime, as specified in the main body of the Router Advertisement. **The maximum value corresponds to 18.2 hours.** A value of 0 MUST NOT be used. The Home Agent Lifetime applies only to this router's usefulness as a home agent; it does not apply to information contained in other message fields or options.

Identifier: RQ_001_1322
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the new Home Agent Information option message . A value of 0 MUST NOT be used for the Home Agent Lifetime field.

RFC Text:
Home Agent Lifetime

16-bit unsigned integer. The lifetime associated with the home agent in units of seconds. The default value is the same as the Router Lifetime, as specified in the main body of the Router Advertisement. The maximum value corresponds to 18.2 hours. **A value of 0 MUST NOT be used. The Home Agent Lifetime applies only to this router's usefulness as a home agent; it does not apply to information contained in other message fields or options.**

Identifier: RQ_001_1323
RFC Clause: 7.4
Type: Optional
Applies to: Home_Agent

Requirement:
Home agents MAY include the Home Agent Information option in their Router Advertisements.

RFC Text:
Home agents MAY include this option in their Router Advertisements. This option MUST NOT be included in a Router Advertisement in which the Home Agent (H) bit (see Section 7.1) is not set. If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the lifetime for this home agent MUST be considered to be the same as the Router Lifetime in the Router Advertisement. If multiple Advertisements are being sent instead of a single larger unsolicited multicast Advertisement, all of the multiple Advertisements with the Router Address (R) bit set MUST include this option with the same contents, otherwise this option MUST be omitted from all Advertisements.

Identifier: RQ_001_1324
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Home Agent Information option MUST NOT be included in a Router Advertisement in which the Home Agent (H) bit is not set.

RFC Text:
Home agents MAY include this option in their Router Advertisements. **This option MUST NOT be included in a Router Advertisement in which the Home Agent (H) bit (see Section 7.1) is not set.** If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the lifetime for this home agent MUST be considered to be the same as the Router Lifetime in the Router Advertisement. If multiple Advertisements are being sent instead of a single larger unsolicited multicast Advertisement, all of the multiple Advertisements with the Router Address (R) bit set MUST include this option with the same contents, otherwise this option MUST be omitted from all Advertisements.

Identifier: RQ_001_1325
RFC Clause: 7.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the Home Agent Information option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the lifetime for this home agent MUST be considered to be the same as the Router Lifetime in the Router Advertisement.

RFC Text:
Home agents MAY include this option in their Router Advertisements. This option MUST NOT be included in a Router Advertisement in which the Home Agent (H) bit (see Section 7.1) is not set. **If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the lifetime for this home agent MUST be considered to be the same as the Router Lifetime in the Router Advertisement.** If multiple Advertisements are being sent instead of a single larger unsolicited multicast Advertisement, all of the multiple Advertisements with the Router Address (R) bit set MUST include this option with the same contents, otherwise this option MUST be omitted from all Advertisements.

Identifier: RQ_001_1326
RFC Clause: 7.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
If multiple Router Advertisements are being sent instead of a single larger unsolicited multicast Advertisement, and the Home Agent Information option is included, then the Home Agent Lifetime option content MUST be identical for all of the multiple Advertisements sent.

RFC Text:
Home Agent Lifetime

[...]
Home agents MAY include this option in their Router Advertisements. This option MUST NOT be included in a Router Advertisement in which the Home Agent (H) bit (see Section 7.1) is not set. If this option is not included in a Router Advertisement in which the Home Agent (H) bit is set, the lifetime for this home agent MUST be considered to be the same as the Router Lifetime in the Router Advertisement. **If multiple Advertisements are being sent instead of a single larger unsolicited multicast Advertisement, all of the multiple Advertisements with the Router Address (R) bit set MUST include this option with the same contents, otherwise this option MUST be omitted from all Advertisements.**

Identifier: RQ_001_1328
RFC Clause: 7.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Home Agent Information option MUST be silently ignored for other Neighbor Discovery messages.

RFC Text:
This option MUST be silently ignored for other Neighbor Discovery messages.

Identifier: RQ_001_1329
RFC Clause: 7.4
Type: Recommendation
Applies to: Home_Agent

Requirement:
If both the Home Agent Preference and Home Agent Lifetime are set to their default values, the Home Agent Information SHOULD NOT be included in the Router Advertisement messages sent by this home agent.

RFC Text:
If both the Home Agent Preference and Home Agent Lifetime are set to their default values specified above, this option SHOULD NOT be included in the Router Advertisement messages sent by this home agent.

Identifier: RQ_001_1330
RFC Clause: 7.5
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
Routers supporting mobility SHOULD be able to be configured with a smaller MinRtrAdvInterval value and MaxRtrAdvInterval value to allow sending of unsolicited multicast Router Advertisements more often.

RFC Text:
Routers supporting mobility SHOULD be able to be configured with a smaller MinRtrAdvInterval value and MaxRtrAdvInterval value to allow sending of unsolicited multicast Router Advertisements more often. The minimum allowed values are:

- o MinRtrAdvInterval 0.03 seconds
- o MaxRtrAdvInterval 0.07 seconds

Identifier: RQ_001_1331
RFC Clause: 7.5
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
For Routers supporting mobility the minimum allowed value is 0.03 seconds for MinRtrAdvInterval.

RFC Text:
Routers supporting mobility SHOULD be able to be configured with a smaller MinRtrAdvInterval value and MaxRtrAdvInterval value to allow sending of unsolicited multicast Router Advertisements more often. **The minimum allowed values are:**

- **o MinRtrAdvInterval 0.03 seconds**
- o MaxRtrAdvInterval 0.07 seconds

Identifier: RQ_001_1332
RFC Clause: 7.5
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
For Routers supporting mobility the minimum allowed value is 0.07 seconds for MaxRtrAdvInterval

RFC Text:
Routers supporting mobility SHOULD be able to be configured with a smaller MinRtrAdvInterval value and MaxRtrAdvInterval value to allow sending of unsolicited multicast Router Advertisements more often. **The minimum allowed values are:**

o MinRtrAdvInterval 0.03 seconds

o MaxRtrAdvInterval 0.07 seconds

Identifier: RQ_001_1333
RFC Clause: 7.5
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
Where modified minimum intervals and delays are used, use of these modified limits MUST be configurable.

RFC Text:
In the case where the minimum intervals and delays are used, the mean time between unsolicited multicast router advertisements is 50 ms. Use of these modified limits MUST be configurable (see also the configuration variable MinDelayBetweenRas in Section 13 which may also have to be modified accordingly). Systems where these values are available MUST NOT default to them, and SHOULD default to values specified in RFC 2461. Knowledge of the type of network interface and operating environment SHOULD be taken into account in configuring these limits for each network interface. This is important with some wireless links, where increasing the frequency of multicast beacons can cause considerable overhead. Routers SHOULD adhere to the intervals specified in RFC 2461 [12], if this overhead is likely to cause service degradation.

Identifier: RQ_001_1334
RFC Clause: 7.5
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
Systems where modified minimum intervals and delays are available MUST NOT default to them.

RFC Text:
In the case where the minimum intervals and delays are used, the mean time between unsolicited multicast router advertisements is 50 ms. Use of these modified limits MUST be configurable (see also the configuration variable MinDelayBetweenRas in Section 13 which may also have to be modified accordingly). Systems where these values are available MUST NOT default to them, and SHOULD default to values specified in RFC 2461. Knowledge of the type of network interface and operating environment SHOULD be taken into account in configuring these limits for each network interface. This is important with some wireless links, where increasing the frequency of multicast beacons can cause considerable overhead. Routers SHOULD adhere to the intervals specified in RFC 2461 [12], if this overhead is likely to cause service degradation.

Identifier: RQ_001_1335
RFC Clause: 7.5
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
Systems where modified minimum intervals and delays are available SHOULD default to values specified in RFC 2461.

RFC Text:
In the case where the minimum intervals and delays are used, the mean time between unsolicited multicast router advertisements is 50 ms. Use of these modified limits MUST be configurable (see also the configuration variable MinDelayBetweenRas in Section 13 which may also have to be modified accordingly). Systems where these values are available MUST NOT default to them, and SHOULD default to values specified in RFC 2461. Knowledge of the type of network interface and operating environment SHOULD be taken into account in configuring these limits for each network interface. This is important with some wireless links, where increasing the frequency of multicast beacons can cause considerable overhead. Routers SHOULD adhere to the intervals specified in RFC 2461 [12], if this overhead is likely to cause service degradation.

Identifier: RQ_001_1336
RFC Clause: 7.5
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
Routers SHOULD add 20 ms to any Advertisement Intervals sent in RAs, which are below 200 ms,

RFC Text:
Additionally, the possible low values of MaxRtrAdvInterval may cause some problems with movement detection in some mobile nodes. To ensure that this is not a problem, Routers SHOULD add 20 ms to any Advertisement Intervals sent in RAs, which are below 200 ms, in order to account for scheduling granularities on both the MN and the Router.

Identifier: RQ_001_1337
RFC Clause: 7.5
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
In wireless networks that have limited bandwidth Router advertisements SHOULD be sent only when solicited.

RFC Text:
Note that multicast Router Advertisements are not always required in certain wireless networks that have limited bandwidth. Mobility detection or link changes in such networks may be done at lower layers. Router advertisements in such networks SHOULD be sent only when solicited. In such networks it SHOULD be possible to disable unsolicited multicast Router Advertisements on specific interfaces. The MinRtrAdvInterval and MaxRtrAdvInterval in such a case can be set to some high values.

Identifier: RQ_001_1338
RFC Clause: 7.5
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
In wireless networks that have limited bandwidth, it SHOULD be possible to disable unsolicited multicast Router Advertisements on specific interfaces.

RFC Text:
Note that multicast Router Advertisements are not always required in certain wireless networks that have limited bandwidth. Mobility detection or link changes in such networks may be done at lower layers. Router advertisements in such networks SHOULD be sent only when solicited. **In such networks it SHOULD be possible to disable unsolicited multicast Router Advertisements on specific interfaces.** The MinRtrAdvInterval and MaxRtrAdvInterval in such a case can be set to some high values.

Identifier: RQ_001_1339
RFC Clause: 7.5
Type: Mandatory
Applies to: Home_Agent

Requirement:
Home agents MUST include the Source Link-Layer Address option in all Router Advertisements they send.

RFC Text:
Home agents MUST include the Source Link-Layer Address option in all Router Advertisements they send. This simplifies the process of returning home, as discussed in Section 11.5.4.

Identifier: RQ_001_1340
RFC Clause: 7.5
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
Routers SHOULD keep AdvDefaultLifetime in at least one second, even if the use of MaxRtrAdvInterval would result in a smaller value.

RFC Text:
Note that according to RFC 2461 [12], AdvDefaultLifetime is by default based on the value of MaxRtrAdvInterval. AdvDefaultLifetime is used in the Router Lifetime field of Router Advertisements. Given that this field is expressed in seconds, a small MaxRtrAdvInterval value can result in a zero value for this field. **To prevent this, routers SHOULD keep AdvDefaultLifetime in at least one second, even if the use of MaxRtrAdvInterval would result in a smaller value.**

Identifier: RQ_001_1341
RFC Clause: 8.1
Type: Mandatory
Applies to: Node

Requirement:
An IPv6 node MUST NOT support the Home Address destination option, type 2 routing header, or the Mobility Header unless it fully supports the requirements for either route optimization, mobile node, or home agent functionality.

RFC Text:
An IPv6 node MUST NOT support the Home Address destination option, type 2 routing header, or the Mobility Header unless it fully supports the requirements listed in the next sections for either route optimization, mobile node, or home agent functionality.

Identifier: RQ_001_1342
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
All correspondent nodes MUST be able to validate a Home Address option using an existing Binding Cache entry

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o **The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.**

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1343
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
All correspondent nodes MUST be able to insert a type 2 routing header into packets to be sent to a mobile node

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o **The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2**.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1344
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1345
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent Nodes SHOULD be able to interpret ICMP messages as described in RFC3775 section 9.3.4.

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1346
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent Nodes MUST be able to send Binding Error messages as described in RFC3775 Section 9.3.3.

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1347
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent Nodes MUST be able to process Mobility Headers as described in RFC3775 Section 9.2.

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1348
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent Nodes MUST be able to participate in a return routability procedure.

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1349
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent Nodes MUST be able to process Binding Update messages.

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1350
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent Nodes MUST be able to return a Binding Acknowledgement.

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1351
RFC Clause: 8.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent Nodes MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates (as described in RFC3775 Section 9.1and Section 9.6).

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1352
RFC Clause: 8.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
Correspondent Nodes SHOULD allow route optimization to be administratively enabled or disabled.

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

Identifier: RQ_001_1353
RFC Clause: 8.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
In a Correspondent Node implementation where route optimization can be administratively enabled or disabled, the default should be enabled.

RFC Text:
The following requirements apply to all correspondent nodes that support route optimization:

o The node MUST be able to validate a Home Address option using an existing Binding Cache entry, as described in Section 9.3.1.

o The node MUST be able to insert a type 2 routing header into packets to be sent to a mobile node, as described in Section 9.3.2.

o Unless the correspondent node is also acting as a mobile node, it MUST ignore type 2 routing headers and silently discard all packets that it has received with such headers.

o The node SHOULD be able to interpret ICMP messages as described in Section 9.3.4.

o The node MUST be able to send Binding Error messages as described in Section 9.3.3.

o The node MUST be able to process Mobility Headers as described in Section 9.2.

o The node MUST be able to participate in a return routability procedure (Section 9.4).

o The node MUST be able to process Binding Update messages (Section 9.5).

o The node MUST be able to return a Binding Acknowledgement (Section 9.5.4).

o The node MUST be able to maintain a Binding Cache of the bindings received in accepted Binding Updates, as described in Section 9.1and Section 9.6.

o The node SHOULD allow route optimization to be administratively enabled or disabled. **The default SHOULD be enabled.**

Identifier: RQ_001_1354
RFC Clause: 8.3
Type: Recommendation
Applies to: Router

Requirement:
Every IPv6 router SHOULD be able to send an Advertisement Interval option in each of its Router Advertisements

RFC Text:
All IPv6 routers, even those not serving as a home agent for Mobile IPv6, have an effect on how well mobile nodes can communicate:

o **Every IPv6 router SHOULD be able to send an Advertisement Interval option (Section 7.3) in each of its Router Advertisements [12], to aid movement detection by mobile nodes (as in Section 11.5.1).** The use of this option in Router Advertisements SHOULD be configurable.

o Every IPv6 router SHOULD be able to support sending unsolicited multicast Router Advertisements at the faster rate described in Section 7.5. If the router supports a faster rate, the used rate MUST be configurable.

o Each router SHOULD include at least one prefix with the Router Address (R) bit set and with its full IP address in its Router Advertisements (as described in Section 7.2).

o Routers supporting filtering packets with routing headers SHOULD support different rules for type 0 and type 2 routing headers (see Section 6.4) so that filtering of source routed packets (type 0) will not necessarily limit Mobile IPv6 traffic which is delivered via type 2 routing headers.

Identifier: RQ_001_1355
RFC Clause: 8.3
Type: Recommendation
Applies to: Router

Requirement:
The use of an Advertisement Interval option in Router Advertisements SHOULD be configurable in every IPv6 router

RFC Text:
All IPv6 routers, even those not serving as a home agent for Mobile IPv6, have an effect on how well mobile nodes can communicate:

o Every IPv6 router SHOULD be able to send an Advertisement Interval option (Section 7.3) in each of its Router Advertisements [12], to aid movement detection by mobile nodes (as in Section 11.5.1). **The use of this option in Router Advertisements SHOULD be configurable.**

o Every IPv6 router SHOULD be able to support sending unsolicited multicast Router Advertisements at the faster rate described in Section 7.5. If the router supports a faster rate, the used rate MUST be configurable.

o Each router SHOULD include at least one prefix with the Router Address (R) bit set and with its full IP address in its Router Advertisements (as described in Section 7.2).

o Routers supporting filtering packets with routing headers SHOULD support different rules for type 0 and type 2 routing headers (see Section 6.4) so that filtering of source routed packets (type 0) will not necessarily limit Mobile IPv6 traffic which is delivered via type 2 routing headers.

Identifier: RQ_001_1356
RFC Clause: 8.3
Type: Recommendation
Applies to: Router

Requirement:
Every IPv6 router SHOULD be able to support sending unsolicited multicast Router Advertisements at the rate described in RFC3775 Section 7.5.

RFC Text:
All IPv6 routers, even those not serving as a home agent for Mobile IPv6, have an effect on how well mobile nodes can communicate:

o Every IPv6 router SHOULD be able to send an Advertisement Interval option (Section 7.3) in each of its Router Advertisements [12], to aid movement detection by mobile nodes (as in Section 11.5.1). The use of this option in Router Advertisements SHOULD be configurable.

o **Every IPv6 router SHOULD be able to support sending unsolicited multicast Router Advertisements at the faster rate described in Section 7.5.** If the router supports a faster rate, the used rate MUST be configurable.

o Each router SHOULD include at least one prefix with the Router Address (R) bit set and with its full IP address in its Router Advertisements (as described in Section 7.2).

o Routers supporting filtering packets with routing headers SHOULD support different rules for type 0 and type 2 routing headers (see Section 6.4) so that filtering of source routed packets (type 0) will not necessarily limit Mobile IPv6 traffic which is delivered via type 2 routing headers.

Identifier: RQ_001_1357
RFC Clause: 8.3
Type: Mandatory
Applies to: Router

Requirement:
In every IPv6 router able to support sending unsolicited multicast Router Advertisements at the faster rate described in RFC3775 Section 7.5, the used rate MUST be configurable.

RFC Text:
All IPv6 routers, even those not serving as a home agent for Mobile IPv6, have an effect on how well mobile nodes can communicate:

o Every IPv6 router SHOULD be able to send an Advertisement Interval option (Section 7.3) in each of its Router Advertisements [12], to aid movement detection by mobile nodes (as in Section 11.5.1). The use of this option in Router Advertisements SHOULD be configurable.

o Every IPv6 router SHOULD be able to support sending unsolicited multicast Router Advertisements at the faster rate described in Section 7.5. **If the router supports a faster rate, the used rate MUST be configurable.**

o Each router SHOULD include at least one prefix with the Router Address (R) bit set and with its full IP address in its Router Advertisements (as described in Section 7.2).

o Routers supporting filtering packets with routing headers SHOULD support different rules for type 0 and type 2 routing headers (see Section 6.4) so that filtering of source routed packets (type 0) will not necessarily limit Mobile IPv6 traffic which is delivered via type 2 routing headers.

Identifier: RQ_001_1358
RFC Clause: 8.3
Type: Recommendation
Applies to: Router

Requirement:
Each router SHOULD include at least one prefix with the Router Address (R) bit set and with its full IP address in its Router Advertisements.

RFC Text:
All IPv6 routers, even those not serving as a home agent for Mobile IPv6, have an effect on how well mobile nodes can communicate:

o Every IPv6 router SHOULD be able to send an Advertisement Interval option (Section 7.3) in each of its Router Advertisements [12], to aid movement detection by mobile nodes (as in Section 11.5.1). The use of this option in Router Advertisements SHOULD be configurable.

o Every IPv6 router SHOULD be able to support sending unsolicited multicast Router Advertisements at the faster rate described in Section 7.5. If the router supports a faster rate, the used rate MUST be configurable.

o Each router SHOULD include at least one prefix with the Router Address (R) bit set and with its full IP address in its Router Advertisements (as described in Section 7.2).

o Routers supporting filtering packets with routing headers SHOULD support different rules for type 0 and type 2 routing headers (see Section 6.4) so that filtering of source routed packets (type 0) will not necessarily limit Mobile IPv6 traffic which is delivered via type 2 routing headers.

Identifier: RQ_001_1359
RFC Clause: 8.3
Type: Recommendation
Applies to: Router

Requirement:
Routers supporting filtering packets with routing headers SHOULD support different rules for type 0 and type 2 routing headers so that filtering of source routed packets (type 0) will not necessarily limit Mobile IPv6 traffic which is delivered via type 2 routing headers.

RFC Text:
All IPv6 routers, even those not serving as a home agent for Mobile IPv6, have an effect on how well mobile nodes can communicate:

o Every IPv6 router SHOULD be able to send an Advertisement Interval option (Section 7.3) in each of its Router Advertisements [12], to aid movement detection by mobile nodes (as in Section 11.5.1). The use of this option in Router Advertisements SHOULD be configurable.

o Every IPv6 router SHOULD be able to support sending unsolicited multicast Router Advertisements at the faster rate described in Section 7.5. If the router supports a faster rate, the used rate MUST be configurable.

o Each router SHOULD include at least one prefix with the Router Address (R) bit set and with its full IP address in its Router Advertisements (as described in Section 7.2).

o Routers supporting filtering packets with routing headers SHOULD support different rules for type 0 and type 2 routing headers (see Section 6.4) so that filtering of source routed packets (type 0) will not necessarily limit Mobile IPv6 traffic which is delivered via type 2 routing headers.

Identifier: RQ_001_1411
RFC Clause: 9.3.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Packets containing a Home Address option MUST be dropped if the given home address is not a unicast routable address.

RFC Text:
Packets containing a Home Address option MUST be dropped if the given home address is not a unicast routable address.

Identifier: RQ_001_1412
RFC Clause: 9.3.1
Type: Optional
Applies to: Correspondent_Node

Requirement:
Mobile nodes can include a Home Address destination option in a packet if they believe the correspondent node has a Binding Cache entry for the home address of a mobile node.

RFC Text:
Mobile nodes can include a Home Address destination option in a packet if they believe the correspondent node has a Binding Cache entry for the home address of a mobile node. Packets containing a Home Address option MUST be dropped if there is no corresponding Binding Cache entry. A corresponding Binding Cache entry MUST have the same home address as appears in the Home Address destination option, and the currently registered care-of address MUST be equal to the source address of the packet. These tests MUST NOT be done for packets that contain a Home Address option and a Binding Update.

Identifier: RQ_001_1413
RFC Clause: 9.3.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Packets containing a Home Address option, but contain no Binding Update option, MUST be dropped if there is no corresponding Binding Cache entry and the correspondent node MUST send the Binding Error message. The Status field in this message should be set to 1 (unknown binding for Home Address destination option).

RFC Text:
Mobile nodes can include a Home Address destination option in a packet if they believe the correspondent node has a Binding Cache entry for the home address of a mobile node. **Packets containing a Home Address option MUST be dropped if there is no corresponding Binding Cache entry.** A corresponding Binding Cache entry MUST have the same home address as appears in the Home Address destination option, and the currently registered care-of address MUST be equal to the source address of the packet. **These tests MUST NOT be done for packets that contain a Home Address option and a Binding Update.**

If the packet is dropped due the above tests, the correspondent node MUST send the Binding Error message as described in Section 9.3.3. The Status field in this message should be set to 1 (unknown binding for Home Address destination option).

Identifier: RQ_001_1414
RFC Clause: 9.3.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Packets containing a Home Address option, but contain no Binding Update option, MUST be dropped if the corresponding Binding Cache entry DOES NOT have the same home address as appears in the Home Address destination option and the correspondent node MUST send the Binding Error message. The Status field in this message should be set to 1 (unknown binding for Home Address destination option).

RFC Text:
Mobile nodes can include a Home Address destination option in a packet if they believe the correspondent node has a Binding Cache entry for the home address of a mobile node. Packets containing a Home Address option MUST be dropped if there is no corresponding Binding Cache entry. **A corresponding Binding Cache entry MUST have the same home address as appears in the Home Address destination option**, and the currently registered care-of address MUST be equal to the source address of the packet. **These tests MUST NOT be done for packets that contain a Home Address option and a Binding Update.**

If the packet is dropped due the above tests, the correspondent node MUST send the Binding Error message as described in Section 9.3.3. The Status field in this message should be set to 1 (unknown binding for Home Address destination option).

Identifier: RQ_001_1415
RFC Clause: 9.3.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Packets containing a Home Address option, but contain no Binding Update option, MUST be dropped if the currently registered care-of address IS NOT equal to the source address of the packet and and the correspondent node MUST send the Binding Error message. The Status field in this message should be set to 1 (unknown binding for Home Address destination option).

RFC Text:
Mobile nodes can include a Home Address destination option in a packet if they believe the correspondent node has a Binding Cache entry for the home address of a mobile node. Packets containing a Home Address option MUST be dropped if there is no corresponding Binding Cache entry. A corresponding Binding Cache entry MUST have the same home address as appears in the Home Address destination option, and **the currently registered care-of address MUST be equal to the source address of the packet. These tests MUST NOT be done for packets that contain a Home Address option and a Binding Update.**

If the packet is dropped due the above tests, the correspondent node MUST send the Binding Error message as described in Section 9.3.3. The Status field in this message should be set to 1 (unknown binding for Home Address destination option).

Identifier: RQ_001_1417
RFC Clause: 9.3.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The correspondent node MUSTtransfer the Home Address field from the Home Address option into the IPv6 header and replacing the original value of the Source Address field there.

RFC Text:
The correspondent node MUST process the option in a manner consistent with exchanging the Home Address field from the Home Address option into the IPv6 header and replacing the original value of the Source Address field there. After all IPv6 options have been processed, it MUST be possible for upper layers to process the packet without the knowledge that it came originally from a care-of address or that a Home Address option was used.

Identifier: RQ_001_1418
RFC Clause: 9.3.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
After all IPv6 options have been processed in the correspondent node, it MUST be possible for upper layers to process the packet without the knowledge that it came originally from a care-of address or that a Home Address option was used.

RFC Text:
The correspondent node MUST process the option in a manner consistent with exchanging the Home Address field from the Home Address option into the IPv6 header and replacing the original value of the Source Address field there. **After all IPv6 options have been processed, it MUST be possible for upper layers to process the packet without the knowledge that it came originally from a care-of address or that a Home Address option was used.**

Identifier: RQ_001_1419
RFC Clause: 9.3.1
Type: Optional
Applies to: Correspondent_Node

Requirement:
The use of IPsec Authentication Header (AH) for the Home Address option is not required,

RFC Text:
The use of IPsec Authentication Header (AH) for the Home Address option is not required, except that if the IPv6 header of a packet is covered by AH, then the authentication MUST also cover the Home Address option; this coverage is achieved automatically by the definition of the Option Type code for the Home Address option, since it indicates that the data within the option cannot change en route to the packet's final destination, and thus the option is included in the AH computation. By requiring that any authentication of the IPv6 header also cover the Home Address option, the security of the Source Address field in the IPv6 header is not compromised by the presence of a Home Address option.

Identifier: RQ_001_1420
RFC Clause: 9.3.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the IPv6 header of a packet is covered by IPsec Authentication Header (AH), then the authentication MUST also cover the Home Address option.

RFC Text:
The use of IPsec Authentication Header (AH) for the Home Address option is not required, except that if the IPv6 header of a packet is covered by AH, then the authentication MUST also cover the Home Address option; this coverage is achieved automatically by the definition of the Option Type code for the Home Address option, since it indicates that the data within the option cannot change en route to the packet's final destination, and thus the option is included in the AH computation. By requiring that any authentication of the IPv6 header also cover the Home Address option, the security of the Source Address field in the IPv6 header is not compromised by the presence of a Home Address option.

Identifier: RQ_001_1421
RFC Clause: 9.3.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
When attempting to verify AH authentication data in a packet that contains a Home Address option, the receiving node MUST calculate the AH authentication data as if the following were true: The Home Address option contains the care-of address, and the source IPv6 address field of the IPv6 header contains the home address.

RFC Text:
When attempting to verify AH authentication data in a packet that contains a Home Address option, the receiving node MUST calculate the AH authentication data as if the following were true: The Home Address option contains the care-of address, and the source IPv6 address field of the IPv6 header contains the home address. This conforms with the calculation specified in Section 11.3.2.

Identifier: RQ_001_1422
RFC Clause: 9.3.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
Before sending any packet, the sending node SHOULD examine its Binding Cache for an entry for the destination address to which the packet is being sent.

RFC Text:
Before sending any packet, the sending node SHOULD examine its Binding Cache for an entry for the destination address to which the packet is being sent. If the sending node has a Binding Cache entry for this address, the sending node SHOULD use a type 2 routing header to route the packet to this mobile node (the destination node) by way of its care-of address. However, the sending node MUST not do this in the following cases:

o When sending an IPv6 Neighbor Discovery [12] packet.

o Where otherwise noted in Section 6.1.

Identifier: RQ_001_1423
RFC Clause: 9.3.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
If the sending node has a Binding Cache entry for the destination address to which the packet is being sent, the sending node SHOULD use a type 2 routing header to route the packet to this mobile node (the destination node) by way of its care-of address, except when sending an IPv6 Neighbor Discovery packet or as otherwise noted in RFC3775 Section 6.1.

RFC Text:
Before sending any packet, the sending node SHOULD examine its Binding Cache for an entry for the destination address to which the packet is being sent. **If the sending node has a Binding Cache entry for this address, the sending node SHOULD use a type 2 routing header to route the packet to this mobile node (the destination node) by way of its care-of address. However, the sending node MUST not do this in the following cases:**

o when prefix information changes.[12] packet.

o Where otherwise noted in Section 6.1.

Identifier: RQ_001_1424
RFC Clause: 9.3.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
When calculating authentication data in a packet that contains a type 2 routing header, the correspondent node MUST calculate the AH authentication data as if the following were true: The routing header contains the care-of address, the destination IPv6 address field of the IPv6 header contains the home address, and the Segments Left field is zero.

RFC Text:
When calculating authentication data in a packet that contains a type 2 routing header, the correspondent node MUST calculate the AH authentication data as if the following were true: The routing header contains the care-of address, the destination IPv6 address field of the IPv6 header contains the home address, and the Segments Left field is zero. The IPsec Security Policy Database lookup MUST based on the mobile node's home address.

Identifier: RQ_001_1425
RFC Clause: 9.3.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
When calculating authentication data in a packet that contains a type 2 routing header, the IPsec Security Policy Database lookup MUST be based on the mobile node's home address.

RFC Text:
When calculating authentication data in a packet that contains a type 2 routing header, the correspondent node MUST calculate the AH authentication data as if the following were true: The routing header contains the care-of address, the destination IPv6 address field of the IPv6 header contains the home address, and the Segments Left field is zero. **The IPsec Security Policy Database lookup MUST based on the mobile node's home address.**

Identifier: RQ_001_1426
RFC Clause: 9.3.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
A Binding Error message MUST NOT be sent if the Source Address field, of the offending packet, does not contain a unicast address.

RFC Text:

A Binding Error message is sent directly to the address that appeared in the IPv6 Source Address field of the offending packet. If the Source Address field does not contain a unicast address, the Binding Error message MUST NOT be sent.

Identifier: RQ_001_1427
RFC Clause: 9.3.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Error message, the Home Address field in the MUST be copied from the Home Address field in the Home Address destination option of the offending packet, or set to the unspecified address if no such option appeared in the packet.

RFC Text:
The Home Address field in the Binding Error message MUST be copied from the Home Address field in the Home Address destination option of the offending packet, or set to the unspecified address if no such option appeared in the packet.

Identifier: RQ_001_1428
RFC Clause: 9.3.3
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
Binding Error messages SHOULD be subject to rate limiting in the same manner as is done for ICMPv6 messages.

RFC Text:
Binding Error messages SHOULD be subject to rate limiting in the same manner as is done for ICMPv6 messages [14].

Identifier: RQ_001_1429
RFC Clause: 9.3.4
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
If the correspondent node receives persistent ICMP Destination Unreachable messages after sending packets to a mobile node based on an entry in its Binding Cache, the correspondent node SHOULD delete this Binding Cache entry.

RFC Text:
If the correspondent node receives persistent ICMP Destination Unreachable messages after sending packets to a mobile node based on an entry in its Binding Cache, the correspondent node SHOULD delete this Binding Cache entry.

Identifier: RQ_001_1430
RFC Clause: 9.4.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Any packet, received by the correspondent node and carrying a Home Test Init message which includes a Home Address destination option MUST be silently ignored.

RFC Text:
Upon receiving a Home Test Init message, the correspondent node verifies the following:

o The packet MUST NOT include a Home Address destination option.

Any packet carrying a Home Test Init message which fails to satisfy all of these tests MUST be silently ignored.

Identifier: RQ_001_1431
RFC Clause: 9.4.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Any packet, received by the correspondent node and carrying a Care-of Test Init message message which includes a Home Address destination option MUST be silently ignored.

RFC Text:
Upon receiving a Care-of Test Init message, the correspondent node verifies the following:

o The packet MUST NOT include a Home Address destination option.

Any packet carrying a Care-of Test Init message which fails to satisfy all of these tests MUST be silently ignored.

Identifier: RQ_001_1432
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Before accepting a Binding Update, the receiving node MUST validate that the Binding Update packet contains a unicast routable home address (either in the Home Address option or in the Source Address, if the Home Address option is not present) .

RFC Text:
Before accepting a Binding Update, the receiving node MUST validate the Binding Update according to the following tests:

o The packet MUST contain a unicast routable home address, either in the Home Address option or in the Source Address, if the Home Address option is not present.

o The Sequence Number field in the Binding Update is greater than the Sequence Number received in the previous valid Binding Update for this home address, if any.

Identifier: RQ_001_1432
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Before accepting a Binding Update, the receiving node MUST validate that the Binding Update packet contains a unicast routable home address (either in the Home Address option or in the Source Address, if the Home Address option is not present) .

RFC Text:
Before accepting a Binding Update, the receiving node MUST validate the Binding Update according to the following tests:

o The packet MUST contain a unicast routable home address, either in the Home Address option or in the Source Address, if the Home Address option is not present.

o The Sequence Number field in the Binding Update is greater than the Sequence Number received in the previous valid Binding Update for this home address, if any.

Identifier: RQ_001_1433
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the node receiving a Binding Update has no Binding Cache entry for the indicated home address, it MUST accept any Sequence Number value in a received Binding Update from this mobile node.

RFC Text:
If the receiving node has no Binding Cache entry for the indicated home address, it MUST accept any Sequence Number value in a received Binding Update from this mobile node.

Identifier: RQ_001_1434
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The node receiving a Binding Update SHALL perform the Sequence Number comparison using modulo 2**16.

RFC Text:
This Sequence Number comparison MUST be performed modulo 216,** i.e., the number is a free running counter represented modulo 65536. A Sequence Number in a received Binding Update is considered less than or equal to the last received number if its value lies in the range of the last received number and the preceding 32768 values, inclusive. For example, if the last received sequence number was 15, then messages with sequence numbers 0 through 15, as well as 32783 through 65535, would be considered less than or equal.

Identifier: RQ_001_1434
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The node receiving a Binding Update SHALL perform the Sequence Number comparison using modulo 2**16.

RFC Text:
This Sequence Number comparison MUST be performed modulo 216,** i.e., the number is a free running counter represented modulo 65536. A Sequence Number in a received Binding Update is considered less than or equal to the last received number if its value lies in the range of the last received number and the preceding 32768 values, inclusive. For example, if the last received sequence number was 15, then messages with sequence numbers 0 through 15, as well as 32783 through 65535, would be considered less than or equal.

Identifier: RQ_001_1435
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update where the Home Registration (H) bit is not set, a Nonce Indices mobility option MUST be present, and the Home and Care-of Nonce Index values in this option MUST be recent enough to be recognized by the correspondent node.

RFC Text:
When the Home Registration (H) bit is not set, the following are also required:

o A Nonce Indices mobility option MUST be present, and the Home and Care-of Nonce Index values in this option MUST be recent enough to be recognized by the correspondent node. (Care-of Nonce Index values are not inspected for requests to delete a binding.)

o The correspondent node MUST re-generate the home keygen token and the care-of keygen token from the information contained in the packet. It then generates the binding management key Kbm and uses it to verify the authenticator field in the Binding Update as specified in Section 6.1.7.

o The Binding Authorization Data mobility option MUST be present, and its contents MUST satisfy rules presented in Section 5.2.6. Note that a care-of address different from the Source Address MAY have been specified by including an Alternate Care-of Address mobility option in the Binding Update. When such a message is received and the return routability procedure is used as an authorization method, the correspondent node MUST verify the authenticator by using the address within the Alternate Care-of Address in the calculations.

o The Binding Authorization Data mobility option MUST be the last option and MUST NOT have trailing padding.

Identifier: RQ_001_1361
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST be able to maintain an entry in its Binding Cache for each mobile node for which it is serving as the home agent.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o **Every home agent MUST be able to maintain an entry in its Binding Cache for each mobile node for which it is serving as the home agent (Section 10.1 and Section 10.3.1).**

o Every home agent MUST be able to intercept packets (using proxy Neighbor Discovery [12]) addressed to a mobile node for which it is currently serving as the home agent, on that mobile node's home link, while the mobile node is away from home (Section 10.4.1).

o ...

Identifier: RQ_001_1362
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST be able to intercept packets (using proxy Neighbor Discovery) addressed to a mobile node for which it is currently serving as the home agent, on that mobile node's home link, while the mobile node is away from home.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o Every home agent MUST be able to maintain an entry in its Binding Cache for each mobile node for which it is serving as the home agent (Section 10.1 and Section 10.3.1).

o **Every home agent MUST be able to intercept packets (using proxy Neighbor Discovery) addressed to a mobile node for which it is currently serving as the home agent, on that mobile node's home link, while the mobile node is away from home (Section 10.4.1).**

o ...

Identifier: RQ_001_1363
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST be able to encapsulate the packets intercepted for a Mobile Node in order to tunnel them to the primary care-of address for the Mobile Node indicated in its binding in the home agent's Binding Cache (Section 10.4.2).

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent MUST be able to encapsulate such intercepted packets in order to tunnel them to the primary care-of address for the mobile node indicated in its binding in the home agent's Binding Cache (Section 10.4.2).

o Every home agent MUST support decapsulating reverse tunneled packets sent to it from a mobile node's home address. Every home agent MUST also check that the source address in the tunneled packets corresponds to the currently registered location of the mobile node (Section 10.4.5).

o ...

Identifier: RQ_001_1364
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST support decapsulating reverse tunneled packets sent to it from a mobile node's home address.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent MUST be able to encapsulate [15] such intercepted packets in order to tunnel them to the primary care-of address for the mobile node indicated in its binding in the home agent's Binding Cache (Section 10.4.2).

o Every home agent MUST support decapsulating [15] reverse tunneled packets sent to it from a mobile node's home address. Every home agent MUST also check that the source address in the tunneled packets corresponds to the currently registered location of the mobile node (Section 10.4.5).

o ...

Identifier: RQ_001_1365
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Home Agents MUST be able to process Mobility Headers.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o The node MUST be able to process Mobility Headers as described in Section 10.2.

o ...

Identifier: RQ_001_1366
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST be able to return a Binding Acknowledgement in response to a Binding Update.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent MUST be able to return a Binding Acknowledgement in response to a Binding Update (Section 10.3.1).

o ...

Identifier: RQ_001_1367
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST maintain a separate Home Agents List for each link on which it is serving as a home agent.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent MUST maintain a separate Home Agents List for each link on which it is serving as a home agent, as described in Section 10.1 and Section 10.5.1.

o ...

Identifier: RQ_001_1368
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST be able to accept packets addressed to the Mobile IPv6 Home-Agents anycast address for the subnet on which it is serving as a home agent.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent MUST be able to accept packets addressed to the Mobile IPv6 Home-Agents anycast address [16] for the subnet on which it is serving as a home agent, and MUST be able to participate in dynamic home agent address discovery (Section 10.5).

o ...

Identifier: RQ_001_1369
RFC Clause: 8.4
Type: Recommendation
Applies to: Home_Agent

Requirement:
Every home agent SHOULD support a configuration mechanism to allow a system administrator to manually set the value to be sent by this home agent in the Home Agent Preference field of the Home Agent Information Option in Router Advertisements that it sends.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent SHOULD support a configuration mechanism to allow a system administrator to manually set the value to be sent by this home agent in the Home Agent Preference field of the Home Agent Information Option in Router Advertisements that it sends (Section 7.4).

o ...

Identifier: RQ_001_1370
RFC Clause: 8.4
Type: Recommendation
Applies to: Home_Agent

Requirement:
Every home agent SHOULD be able to send ICMP Mobile Prefix Advertisements .

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent SHOULD support sending ICMP Mobile Prefix Advertisements (Section 6.8), and SHOULD respond to Mobile Prefix Solicitations (Section 6.7). If supported, this behavior MUST be configurable, so that home agents can be configured to avoid sending such Prefix Advertisements according to the needs of the network administration in the home domain.

o ...

Identifier: RQ_001_1371
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST support IPsec ESP for protection of packets belonging to the return routability procedure.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent MUST support IPsec ESP for protection of packets belonging to the return routability procedure (Section 10.4.6).

o ...

Identifier: RQ_001_1372
RFC Clause: 8.4
Type: Recommendation
Applies to: Home_Agent

Requirement:
Every home agent SHOULD support the multicast group membership control protocols.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent SHOULD support the multicast group membership control protocols as described in Section 10.4.3. If this support is provided, the home agent MUST be capable of using it to determine which multicast data packets to forward via the tunnel to the mobile node.

o ...

Identifier: RQ_001_1373
RFC Clause: 8.4
Type: Optional
Applies to: Home_Agent

Requirement:
Home agents MAY support stateful address autoconfiguration for mobile nodes.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Home agents MAY support stateful address autoconfiguration for mobile nodes as described in Section 10.4.4

Identifier: RQ_001_1374
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Al IPv6 nodes capable of functioning as mobile nodes MUST maintain a Binding Update List.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o **The node MUST maintain a Binding Update List (Section 11.1).**

o ...

Identifier: RQ_001_1375
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST support sending packets containing a Home Address option, and follow the required IPsec interaction.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o **The node MUST support sending packets containing a Home Address option (Section 11.3.1), and follow the required IPsec interaction (Section 11.3.2)**.

o ...

Identifier: RQ_001_1376
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST be able to perform IPv6 encapsulation and decapsulation.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST be able to perform IPv6 encapsulation and decapsulation [15].

o ...

Identifier: RQ_001_1377
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST be able to process type 2 routing header.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST be able to process type 2 routing header as defined in Section 6.4 and Section 11.3.3.

o ...

Identifier: RQ_001_1378
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST support receiving a Binding Error message.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST support receiving a Binding Error message (Section 11.3.6).

o ...

Identifier: RQ_001_1379
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST support receiving ICMP errors.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST support receiving ICMP errors (Section 11.3.5).

o ...

Identifier: RQ_001_1380
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST support movement detection.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST support movement detection, care-of address formation, and returning home (Section 11.5).

o ...

Identifier: RQ_001_1381
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST be able to process Mobility Headers.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST be able to process Mobility Headers as described in Section 11.2.

o ...

Identifier: RQ_001_1382
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST be able to receive and process Binding Acknowledgements.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST be able to receive and process Binding Acknowledgements, as specified in Section 11.7.3.

o ...

Identifier: RQ_001_1383
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST support receiving a Binding Refresh Request, by responding with a Binding Update.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST support receiving a Binding Refresh Request (Section 6.1.2), by responding with a Binding Update.

o ....

Identifier: RQ_001_1384
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST support receiving Mobile Prefix Advertisements and reconfiguring its home address based on the prefix information contained therein.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST support receiving Mobile Prefix Advertisements (Section 11.4.3) and reconfiguring its home address based on the prefix information contained therein.

o ...

Identifier: RQ_001_1385
RFC Clause: 8.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes SHOULD support use of the dynamic home agent address discovery mechanism.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node SHOULD support use of the dynamic home agent address discovery mechanism, as described in Section 11.4.1.

o ...

Identifier: RQ_001_1386
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST allow route optimization to be administratively enabled or disabled.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.

o ...

Identifier: RQ_001_1387
RFC Clause: 8.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
Although all mobile nodes allow route optimization to be administratively enabled or disabled, the default behaviour SHOULD be "enabled".

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o **The node MUST allow route optimization to be administratively enabled or disabled. The default SHOULD be enabled.**

o ...

Identifier: RQ_001_1388
RFC Clause: 8.5
Type: Optional
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MAY support the multicast address listener part of a multicast group membership protocol.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MAY support the multicast address listener part of a multicast group membership protocol as described in Section 11.3.4. If this support is provided, the mobile node MUST be able to receive tunneled multicast packets from the home agent.

o ...

Identifier: RQ_001_1389
RFC Clause: 8.5
Type: Optional
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MAY support stateful address autoconfiguration mechanisms such as DHCPv6 on the interface represented by the tunnel to the home agent.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MAY support stateful address autoconfiguration mechanisms such as DHCPv6 [29] on the interface represented by the tunnel to the home agent.

Identifier: RQ_001_1390
RFC Clause: 9.1
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
A separate Binding Cache SHOULD be maintained by each IPv6 node for each of its unicast routable addresses

RFC Text:
IPv6 nodes with route optimization support maintain a Binding Cache of bindings for other nodes. **A separate Binding Cache SHOULD be maintained by each IPv6 node for each of its unicast routable addresses**. The Binding Cache MAY be implemented in any manner consistent with the external behavior described in this document, for example by being combined with the node's Destination Cache as maintained by Neighbor Discovery [12]. When sending a packet, the Binding Cache is searched before the Neighbor Discovery conceptual Destination Cache [12].

Identifier: RQ_001_1391
RFC Clause: 9.1
Type: Optional
Applies to: Correspondent_Node

Requirement:
The Binding Cache MAY be implemented in any manner consistent with the external behavior described in this document.

RFC Text:
IPv6 nodes with route optimization support maintain a Binding Cache of bindings for other nodes. A separate Binding Cache SHOULD be maintained by each IPv6 node for each of its unicast routable addresses. **The Binding Cache MAY be implemented in any manner consistent with the external behavior described in this document,** for example by being combined with the node's Destination Cache as maintained by Neighbor Discovery [12]. When sending a packet, the Binding Cache is searched before the Neighbor Discovery conceptual Destination Cache [12].

Identifier: RQ_001_1392
RFC Clause: 9.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
When sending a packet, the Binding Cache SHALL BE searched before the Neighbor Discovery conceptual Destination Cache

RFC Text:
IPv6 nodes with route optimization support maintain a Binding Cache of bindings for other nodes. A separate Binding Cache SHOULD be maintained by each IPv6 node for each of its unicast routable addresses. The Binding Cache MAY be implemented in any manner consistent with the external behavior described in this document, for example by being combined with the node's Destination Cache as maintained by Neighbor Discovery [12]. **When sending a packet, the Binding Cache is searched before the Neighbor Discovery conceptual Destination Cache [12].**

Identifier: RQ_001_1393
RFC Clause: 9.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

Each Binding Cache entry SHALL contain the following fields:
o The home address of the mobile node for which this is the Binding Cache entry.
o The care-of address for the mobile node indicated by the home address field in this Binding Cache entry.
o A lifetime value, indicating the remaining lifetime for this Binding Cache entry.
o A flag indicating whether or not this Binding Cache entry is a home registration entry (applicable only on nodes which support home agent functionality).
o The maximum value of the Sequence Number field received in previous Binding Updates for this home address.
o Usage information for this Binding Cache entry.

RFC Text:

Each Binding Cache entry conceptually contains the following fields:
o The home address of the mobile node for which this is the Binding Cache entry. This field is used as the key for searching the Binding Cache for the destination address of a packet being sent.
o The care-of address for the mobile node indicated by the home address field in this Binding Cache entry.
o A lifetime value, indicating the remaining lifetime for this Binding Cache entry. The lifetime value is initialized from the Lifetime field in the Binding Update that created or last modified this Binding Cache entry.
o A flag indicating whether or not this Binding Cache entry is a home registration entry (applicable only on nodes which support home agent functionality).
o **The maximum value of the Sequence Number field received in previous Binding Updates for this home address. The Sequence Number field is 16 bits long. Sequence Number values MUST be compared modulo 2**16 as explained in Section 9.5.1.**
o Usage information for this Binding Cache entry. This is needed to implement the cache replacement policy in use in the Binding Cache. Recent use of a cache entry also serves as an indication that a Binding Refresh Request should be sent when the lifetime of this entry nears expiration.

Identifier: RQ_001_1394
RFC Clause: 9.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

For nodes which support home agent functionality, each Binding Cache entry SHALL include a flag indicating whether or not this Binding Cache entry is a home registration entry

RFC Text:

Each Binding Cache entry conceptually contains the following fields:
o ...

o **A flag indicating whether or not this Binding Cache entry is a home registration entry (applicable only on nodes which support home agent functionality).**
o ...

Identifier: RQ_001_1395
RFC Clause: 9.1
Type: Optional
Applies to: Correspondent_Node

Requirement:
Binding Cache entries not marked as home registrations MAY be replaced at any time by any reasonable local cache replacement policy

RFC Text:
Binding Cache entries not marked as home registrations MAY be replaced at any time by any reasonable local cache replacement policy but SHOULD NOT be unnecessarily deleted. The Binding Cache for any one of a node's IPv6 addresses may contain at most one entry for each mobile node home address. The contents of a node's Binding Cache MUST NOT be changed in response to a Home Address option in a received packet.

Identifier: RQ_001_1396
RFC Clause: 9.1
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
Binding Cache entries not marked as home registrations SHOULD NOT be unnecessarily deleted.

RFC Text:
Binding Cache entries not marked as home registrations MAY be replaced at any time by any reasonable local cache replacement policy but SHOULD NOT be unnecessarily deleted. The Binding Cache for any one of a node's IPv6 addresses may contain at most one entry for each mobile node home address. The contents of a node's Binding Cache MUST NOT be changed in response to a Home Address option in a received packet.

Identifier: RQ_001_1397
RFC Clause: 9.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The contents of a node's Binding Cache MUST NOT be changed in response to a Home Address option in a received packet.

RFC Text:
Binding Cache entries not marked as home registrations MAY be replaced at any time by any reasonable local cache replacement policy but SHOULD NOT be unnecessarily deleted. The Binding Cache for any one of a node's IPv6 addresses may contain at most one entry for each mobile node home address. **The contents of a node's Binding Cache MUST NOT be changed in response to a Home Address option in a received packet.**

Identifier: RQ_001_1398
RFC Clause: 9.2
Type: Mandatory
Applies to: Node

Requirement:
In Mobility Header processing the checksum MUST be verified as per RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1398
RFC Clause: 9.2
Type: Mandatory
Applies to: Router

Requirement:
In Mobility Header processing the checksum MUST be verified as per RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1398
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
In Mobility Header processing the checksum MUST be verified as per RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1398
RFC Clause: 9.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In Mobility Header processing the checksum MUST be verified as per RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1398
RFC Clause: 9.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In Mobility Header processing the checksum MUST be verified as per RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1398
RFC Clause: 9.2
Type: Mandatory
Applies to: Host

Requirement:
In Mobility Header processing the checksum MUST be verified as per RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1398
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In Mobility Header processing the checksum MUST be verified as per RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1399
RFC Clause: 9.2
Type: Mandatory
Applies to: Node

Requirement:
In Mobility Header processing, if the checksum verification fails, the node MUST silently discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1399
RFC Clause: 9.2
Type: Mandatory
Applies to: Router

Requirement:
In Mobility Header processing, if the checksum verification fails, the node MUST silently discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1399
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
In Mobility Header processing, if the checksum verification fails, the node MUST silently discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1399
RFC Clause: 9.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In Mobility Header processing, if the checksum verification fails, the node MUST silently discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1399
RFC Clause: 9.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In Mobility Header processing, if the checksum verification fails, the node MUST silently discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1399
RFC Clause: 9.2
Type: Mandatory
Applies to: Host

Requirement:
In Mobility Header processing, if the checksum verification fails, the node MUST silently discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1399
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In Mobility Header processing, if the checksum verification fails, the node MUST silently discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1400
RFC Clause: 9.2
Type: Mandatory
Applies to: Node

Requirement:
In Mobility Header processing, the MH Type field MUST have a known value.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1400
RFC Clause: 9.2
Type: Mandatory
Applies to: Router

Requirement:
In Mobility Header processing, the MH Type field MUST have a known value.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1400
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
In Mobility Header processing, the MH Type field MUST have a known value.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1400
RFC Clause: 9.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In Mobility Header processing, the MH Type field MUST have a known value.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1400
RFC Clause: 9.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In Mobility Header processing, the MH Type field MUST have a known value.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1400
RFC Clause: 9.2
Type: Mandatory
Applies to: Host

Requirement:
In Mobility Header processing, the MH Type field MUST have a known value.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1400
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In Mobility Header processing, the MH Type field MUST have a known value.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1401
RFC Clause: 9.2
Type: Mandatory
Applies to: Node

Requirement:
In Mobility Header processing, if the MH Type field does not have a known value, the node MUST discard the message and issue a Binding Error message with Status field set to 2 (unrecognized MH Type value).

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1401
RFC Clause: 9.2
Type: Mandatory
Applies to: Router

Requirement:
In Mobility Header processing, if the MH Type field does not have a known value, the node MUST discard the message and issue a Binding Error message with Status field set to 2 (unrecognized MH Type value).

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1401
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
In Mobility Header processing, if the MH Type field does not have a known value, the node MUST discard the message and issue a Binding Error message with Status field set to 2 (unrecognized MH Type value).

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1401
RFC Clause: 9.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In Mobility Header processing, if the MH Type field does not have a known value, the node MUST discard the message and issue a Binding Error message with Status field set to 2 (unrecognized MH Type value).

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1401
RFC Clause: 9.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In Mobility Header processing, if the MH Type field does not have a known value, the node MUST discard the message and issue a Binding Error message with Status field set to 2 (unrecognized MH Type value).

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1401
RFC Clause: 9.2
Type: Mandatory
Applies to: Host

Requirement:
In Mobility Header processing, if the MH Type field does not have a known value, the node MUST discard the message and issue a Binding Error message with Status field set to 2 (unrecognized MH Type value).

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1401
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In Mobility Header processing, if the MH Type field does not have a known value, the node MUST discard the message and issue a Binding Error message with Status field set to 2 (unrecognized MH Type value).

RFC Text:
Mobility Header processing MUST observe the following rules:

o The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message.

o The MH Type field MUST have a known value (Section 6.1.1). Otherwise, the node MUST discard the message and issue a Binding Error message as described in Section 9.3.3, with Status field set to 2 (unrecognized MH Type value).

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1403
RFC Clause: 9.2
Type: Mandatory
Applies to: Node

Requirement:
In Mobility Header processing, the Payload Proto field MUST be IPPROTO_NONE (59 decimal).

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1403
RFC Clause: 9.2
Type: Mandatory
Applies to: Router

Requirement:
In Mobility Header processing, the Payload Proto field MUST be IPPROTO_NONE (59 decimal).

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1403
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
In Mobility Header processing, the Payload Proto field MUST be IPPROTO_NONE (59 decimal).

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1403
RFC Clause: 9.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In Mobility Header processing, the Payload Proto field MUST be IPPROTO_NONE (59 decimal).

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1403
RFC Clause: 9.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In Mobility Header processing, the Payload Proto field MUST be IPPROTO_NONE (59 decimal).

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1403
RFC Clause: 9.2
Type: Mandatory
Applies to: Host

Requirement:
In Mobility Header processing, the Payload Proto field MUST be IPPROTO_NONE (59 decimal).

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1403
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In Mobility Header processing, the Payload Proto field MUST be IPPROTO_NONE (59 decimal).

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1404
RFC Clause: 9.2
Type: Mandatory
Applies to: Node

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1404
RFC Clause: 9.2
Type: Mandatory
Applies to: Router

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1404
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1404
RFC Clause: 9.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1404
RFC Clause: 9.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1404
RFC Clause: 9.2
Type: Mandatory
Applies to: Host

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1404
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1405
RFC Clause: 9.2
Type: Recommendation
Applies to: Node

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1405
RFC Clause: 9.2
Type: Recommendation
Applies to: Router

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1405
RFC Clause: 9.2
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1405
RFC Clause: 9.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1405
RFC Clause: 9.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1405
RFC Clause: 9.2
Type: Recommendation
Applies to: Host

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1405
RFC Clause: 9.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
In Mobility Header processing, if the Payload Proto field is not IPPROTO_NONE (59 decimal), the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. The Pointer field in the ICMP message SHOULD point at the Payload Proto field.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1406
RFC Clause: 9.2
Type: Recommendation
Applies to: Node

Requirement:
When sending an ICMP Parameter Problem message in response to a Mobility Header where the Payload Proto field is not IPPROTO_NONE, the Pointer field in the ICMP Parameter Problem message SHOULD point at the Payload Proto field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. **The Pointer field in the ICMP message SHOULD point at the Payload Proto field**.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1406
RFC Clause: 9.2
Type: Recommendation
Applies to: Router

Requirement:
When sending an ICMP Parameter Problem message in response to a Mobility Header where the Payload Proto field is not IPPROTO_NONE, the Pointer field in the ICMP Parameter Problem message SHOULD point at the Payload Proto field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. **The Pointer field in the ICMP message SHOULD point at the Payload Proto field**.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1406
RFC Clause: 9.2
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
When sending an ICMP Parameter Problem message in response to a Mobility Header where the Payload Proto field is not IPPROTO_NONE, the Pointer field in the ICMP Parameter Problem message SHOULD point at the Payload Proto field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. **The Pointer field in the ICMP message SHOULD point at the Payload Proto field**.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1406
RFC Clause: 9.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
When sending an ICMP Parameter Problem message in response to a Mobility Header where the Payload Proto field is not IPPROTO_NONE, the Pointer field in the ICMP Parameter Problem message SHOULD point at the Payload Proto field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. **The Pointer field in the ICMP message SHOULD point at the Payload Proto field**.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1406
RFC Clause: 9.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
When sending an ICMP Parameter Problem message in response to a Mobility Header where the Payload Proto field is not IPPROTO_NONE, the Pointer field in the ICMP Parameter Problem message SHOULD point at the Payload Proto field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. **The Pointer field in the ICMP message SHOULD point at the Payload Proto field**.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1406
RFC Clause: 9.2
Type: Recommendation
Applies to: Host

Requirement:
When sending an ICMP Parameter Problem message in response to a Mobility Header where the Payload Proto field is not IPPROTO_NONE, the Pointer field in the ICMP Parameter Problem message SHOULD point at the Payload Proto field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. **The Pointer field in the ICMP message SHOULD point at the Payload Proto field**.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1406
RFC Clause: 9.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When sending an ICMP Parameter Problem message in response to a Mobility Header where the Payload Proto field is not IPPROTO_NONE, the Pointer field in the ICMP Parameter Problem message SHOULD point at the Payload Proto field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Payload Proto field MUST be IPPROTO_NONE (59 decimal). Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. Thus no Binding Cache information is used in sending the ICMP message. **The Pointer field in the ICMP message SHOULD point at the Payload Proto field**.

o ...

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1407
RFC Clause: 9.2
Type: Mandatory
Applies to: Node

Requirement:
The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1407
RFC Clause: 9.2
Type: Mandatory
Applies to: Router

Requirement:
The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1407
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1407
RFC Clause: 9.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1407
RFC Clause: 9.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1407
RFC Clause: 9.2
Type: Mandatory
Applies to: Host

Requirement:
The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1407
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in RFC3775 Section 6.1.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1408
RFC Clause: 9.2
Type: Mandatory
Applies to: Node

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1408
RFC Clause: 9.2
Type: Mandatory
Applies to: Router

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1408
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobility_aware_Router

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1408
RFC Clause: 9.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1408
RFC Clause: 9.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1408
RFC Clause: 9.2
Type: Mandatory
Applies to: Host

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1408
RFC Clause: 9.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node MUST discard the message.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1409
RFC Clause: 9.2
Type: Recommendation
Applies to: Node

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1409
RFC Clause: 9.2
Type: Recommendation
Applies to: Router

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1409
RFC Clause: 9.2
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1409
RFC Clause: 9.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1409
RFC Clause: 9.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1409
RFC Clause: 9.2
Type: Recommendation
Applies to: Host

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1409
RFC Clause: 9.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Header Len field in the Mobility Header is less than the length specified for this particular type of message in RFC3775 Section 6.1, the node SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1410
RFC Clause: 9.2
Type: Recommendation
Applies to: Node

Requirement:
When an ICMP Parameter Problem, Code 0, message is sent in response to a Mobility Header where the Header Len field in the Mobility Header is less than the length specified for this particular type of message, the Pointer field in the ICMP message SHOULD point at the Header Len field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1410
RFC Clause: 9.2
Type: Recommendation
Applies to: Router

Requirement:
When an ICMP Parameter Problem, Code 0, message is sent in response to a Mobility Header where the Header Len field in the Mobility Header is less than the length specified for this particular type of message, the Pointer field in the ICMP message SHOULD point at the Header Len field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1410
RFC Clause: 9.2
Type: Recommendation
Applies to: Mobility_aware_Router

Requirement:
When an ICMP Parameter Problem, Code 0, message is sent in response to a Mobility Header where the Header Len field in the Mobility Header is less than the length specified for this particular type of message, the Pointer field in the ICMP message SHOULD point at the Header Len field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1410
RFC Clause: 9.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
When an ICMP Parameter Problem, Code 0, message is sent in response to a Mobility Header where the Header Len field in the Mobility Header is less than the length specified for this particular type of message, the Pointer field in the ICMP message SHOULD point at the Header Len field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1410
RFC Clause: 9.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
When an ICMP Parameter Problem, Code 0, message is sent in response to a Mobility Header where the Header Len field in the Mobility Header is less than the length specified for this particular type of message, the Pointer field in the ICMP message SHOULD point at the Header Len field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1410
RFC Clause: 9.2
Type: Recommendation
Applies to: Host

Requirement:
When an ICMP Parameter Problem, Code 0, message is sent in response to a Mobility Header where the Header Len field in the Mobility Header is less than the length specified for this particular type of message, the Pointer field in the ICMP message SHOULD point at the Header Len field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1410
RFC Clause: 9.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When an ICMP Parameter Problem, Code 0, message is sent in response to a Mobility Header where the Header Len field in the Mobility Header is less than the length specified for this particular type of message, the Pointer field in the ICMP message SHOULD point at the Header Len field.

RFC Text:
Mobility Header processing MUST observe the following rules:

o ...

o The Header Len field in the Mobility Header MUST NOT be less than the length specified for this particular type of message in Section 6.1. Otherwise, the node MUST discard the message and SHOULD send ICMP Parameter Problem, Code 0, directly to the Source Address of the packet as specified in RFC 2463 [14]. (The Binding Cache information is again not used.) The Pointer field in the ICMP message SHOULD point at the Header Len field.

Subsequent checks depend on the particular Mobility Header.

Identifier: RQ_001_1436
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update where the Home Registration (H) bit is not set, the correspondent node MUST re-generate the home keygen token and the care-of keygen token from the information contained in the packet. It then generates the binding management key Kbm and uses it to verify the authenticator field in the Binding Update as specified in Section 6.1.7.

RFC Text:
When the Home Registration (H) bit is not set, the following are also required:

o A Nonce Indices mobility option MUST be present, and the Home and Care-of Nonce Index values in this option MUST be recent enough to be recognized by the correspondent node. (Care-of Nonce Index values are not inspected for requests to delete a binding.)

o **The correspondent node MUST re-generate the home keygen token and the care-of keygen token from the information contained in the packet. It then generates the binding management key Kbm and uses it to verify the authenticator field in the Binding Update as specified in Section 6.1.7**.

o The Binding Authorization Data mobility option MUST be present, and its contents MUST satisfy rules presented in Section 5.2.6. Note that a care-of address different from the Source Address MAY have been specified by including an Alternate Care-of Address mobility option in the Binding Update. When such a message is received and the return routability procedure is used as an authorization method, the correspondent node MUST verify the authenticator by using the address within the Alternate Care-of Address in the calculations.

o The Binding Authorization Data mobility option MUST be the last option and MUST NOT have trailing padding.

Identifier: RQ_001_1437
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update where the Home Registration (H) bit is not set, the Binding Authorization Data mobility option MUST be present, and its contents MUST satisfy rules presented in Section 5.2.6.

RFC Text:
When the Home Registration (H) bit is not set, the following are also required:

o A Nonce Indices mobility option MUST be present, and the Home and Care-of Nonce Index values in this option MUST be recent enough to be recognized by the correspondent node. (Care-of Nonce Index values are not inspected for requests to delete a binding.)

o The correspondent node MUST re-generate the home keygen token and the care-of keygen token from the information contained in the packet. It then generates the binding management key Kbm and uses it to verify the authenticator field in the Binding Update as specified in Section 6.1.7.

o The Binding Authorization Data mobility option MUST be present, and its contents MUST satisfy rules presented in Section 5.2.6. Note that a care-of address different from the Source Address MAY have been specified by including an Alternate Care-of Address mobility option in the Binding Update. When such a message is received and the return routability procedure is used as an authorization method, the correspondent node MUST verify the authenticator by using the address within the Alternate Care-of Address in the calculations.

o The Binding Authorization Data mobility option MUST be the last option and MUST NOT have trailing padding.

Identifier: RQ_001_1438
RFC Clause: 9.5.1
Type: Optional
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update where the Home Registration (H) bit is not set and a care-of address different from the Source Address has been specified by including an Alternate Care-of Address mobility option in the Binding Update, then if such a message is received and the return routability procedure is used as an authorization method, the correspondent node MUST verify the authenticator by using the address within the Alternate Care-of Address in the calculations.

RFC Text:
When the Home Registration (H) bit is not set, the following are also required:

o A Nonce Indices mobility option MUST be present, and the Home and Care-of Nonce Index values in this option MUST be recent enough to be recognized by the correspondent node. (Care-of Nonce Index values are not inspected for requests to delete a binding.)

o The correspondent node MUST re-generate the home keygen token and the care-of keygen token from the information contained in the packet. It then generates the binding management key Kbm and uses it to verify the authenticator field in the Binding Update as specified in Section 6.1.7.

o The Binding Authorization Data mobility option MUST be present, and its contents MUST satisfy rules presented in Section 5.2.6. Note that a care-of address different from the Source Address MAY have been specified by including an Alternate Care-of Address mobility option in the Binding Update. When such a message is received and the return routability procedure is used as an authorization method, the correspondent node MUST verify the authenticator by using the address within the Alternate Care-of Address in the calculations.

o The Binding Authorization Data mobility option MUST be the last option and MUST NOT have trailing padding.

Identifier: RQ_001_1439
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update where the Home Registration (H) bit is not set, the Binding Authorization Data mobility option MUST be the last option.

RFC Text:
When the Home Registration (H) bit is not set, the following are also required:

o A Nonce Indices mobility option MUST be present, and the Home and Care-of Nonce Index values in this option MUST be recent enough to be recognized by the correspondent node. (Care-of Nonce Index values are not inspected for requests to delete a binding.)

o The correspondent node MUST re-generate the home keygen token and the care-of keygen token from the information contained in the packet. It then generates the binding management key Kbm and uses it to verify the authenticator field in the Binding Update as specified in Section 6.1.7.

o The Binding Authorization Data mobility option MUST be present, and its contents MUST satisfy rules presented in Section 5.2.6. Note that a care-of address different from the Source Address MAY have been specified by including an Alternate Care-of Address mobility option in the Binding Update. When such a message is received and the return routability procedure is used as an authorization method, the correspondent node MUST verify the authenticator by using the address within the Alternate Care-of Address in the calculations.

o The Binding Authorization Data mobility option MUST be the last option and MUST NOT have trailing padding.

Identifier: RQ_001_1440
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update where the Home Registration (H) bit is not set, the Binding Authorization Data mobility option MUST NOT have trailing padding.

RFC Text:
When the Home Registration (H) bit is not set, the following are also required:

o A Nonce Indices mobility option MUST be present, and the Home and Care-of Nonce Index values in this option MUST be recent enough to be recognized by the correspondent node. (Care-of Nonce Index values are not inspected for requests to delete a binding.)

o The correspondent node MUST re-generate the home keygen token and the care-of keygen token from the information contained in the packet. It then generates the binding management key Kbm and uses it to verify the authenticator field in the Binding Update as specified in Section 6.1.7.

o The Binding Authorization Data mobility option MUST be present, and its contents MUST satisfy rules presented in Section 5.2.6. Note that a care-of address different from the Source Address MAY have been specified by including an Alternate Care-of Address mobility option in the Binding Update. When such a message is received and the return routability procedure is used as an authorization method, the correspondent node MUST verify the authenticator by using the address within the Alternate Care-of Address in the calculations.

o The Binding Authorization Data mobility option MUST be the last option and MUST NOT have trailing padding.

Identifier: RQ_001_1441
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update where the Home Registration (H) bit is set, the Nonce Indices mobility option MUST NOT be present.

RFC Text:
If the Home Registration (H) bit is set, the Nonce Indices mobility option MUST NOT be present.

Identifier: RQ_001_1442
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update containing a sequence number which is not greater than the sequence number from the last valid Binding Update for this home address, then the receiving node MUST send back a Binding Acknowledgement with status code 135, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement.

RFC Text:
If the mobile node sends a sequence number which is not greater than the sequence number from the last valid Binding Update for this home address, then the receiving node MUST send back a Binding Acknowledgement with status code 135, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement.

Identifier: RQ_001_1442
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If a node receives a Binding Update containing a sequence number which is not greater than the sequence number from the last valid Binding Update for this home address, then the receiving node MUST send back a Binding Acknowledgement with status code 135, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement.

RFC Text:
If the mobile node sends a sequence number which is not greater than the sequence number from the last valid Binding Update for this home address, then the receiving node MUST send back a Binding Acknowledgement with status code 135, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement.

Identifier: RQ_001_1443
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update where a binding already exists for the given home address and the home registration flag has a different value than the Home Registration (H) bit in the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 139 (registration type change disallowed).

RFC Text:
If a binding already exists for the given home address and the home registration flag has a different value than the Home Registration (H) bit in the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 139 (registration type change disallowed).
The home registration flag stored in the Binding Cache entry MUST NOT be changed.

Identifier: RQ_001_1443
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If a node receives a Binding Update where a binding already exists for the given home address and the home registration flag has a different value than the Home Registration (H) bit in the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 139 (registration type change disallowed).

RFC Text:
If a binding already exists for the given home address and the home registration flag has a different value than the Home Registration (H) bit in the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 139 (registration type change disallowed). The home registration flag stored in the Binding Cache entry MUST NOT be changed.

Identifier: RQ_001_1444
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node receives a Binding Update where a binding already exists for the given home address and the home registration flag has a different value than the Home Registration (H) bit in the Binding Update, the home registration flag stored in the Binding Cache entry MUST NOT be changed.

RFC Text:
If a binding already exists for the given home address and the home registration flag has a different value than the Home Registration (H) bit in the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 139 (registration type change disallowed). The home registration flag stored in the Binding Cache entry MUST NOT be changed.

Identifier: RQ_001_1444
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If a node receives a Binding Update where a binding already exists for the given home address and the home registration flag has a different value than the Home Registration (H) bit in the Binding Update, the home registration flag stored in the Binding Cache entry MUST NOT be changed.

RFC Text:
If a binding already exists for the given home address and the home registration flag has a different value than the Home Registration (H) bit in the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 139 (registration type change disallowed). The home registration flag stored in the Binding Cache entry MUST NOT be changed.

Identifier: RQ_001_1445
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the receiving node of a Binding Update, no longer recognizes the Home Nonce Index values from the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 136.

RFC Text:
If the receiving node no longer recognizes the Home Nonce Index value, Care-of Nonce Index value, or both values from the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 136, 137, or 138, respectively.

Identifier: RQ_001_1446
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the receiving node of a Binding Update, no longer recognizes the Care-of Nonce Index value, from the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 137.

RFC Text:
If the receiving node no longer recognizes the Home Nonce Index value, Care-of Nonce Index value, or both values from the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 136, 137, or 138, respectively.

Identifier: RQ_001_1447
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the receiving node of a Binding Update, no longer recognizes the Home Nonce Index value and Care-of Nonce Index value from the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 138.

RFC Text:
If the receiving node no longer recognizes the Home Nonce Index value, Care-of Nonce Index value, or both values from the Binding Update, then the receiving node MUST send back a Binding Acknowledgement with status code 136, 137, or 138, respectively.

Identifier: RQ_001_1448
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the receiving node is unable to validate a Binding Update, for any reason other than insufficiency of the Sequence Number, registration type change, or expired nonce index values, it must be MUST be silently discarded.

RFC Text:
Packets carrying Binding Updates that fail to satisfy all of these tests for any reason other than insufficiency of the Sequence Number, registration type change, or expired nonce index values, MUST be silently discarded.

Identifier: RQ_001_1448
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the receiving node is unable to validate a Binding Update, for any reason other than insufficiency of the Sequence Number, registration type change, or expired nonce index values, it must be MUST be silently discarded.

RFC Text:
Packets carrying Binding Updates that fail to satisfy all of these tests for any reason other than insufficiency of the Sequence Number, registration type change, or expired nonce index values, MUST be silently discarded.

Identifier: RQ_001_1449
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

If the Correspondant node validates a Binding Update where:

- the Lifetime specified in the Binding Update is zero or the specified care-of address matches the home address for the binding
- the Binding Update includes a valid home nonce index
- and the Home Registration (H) bit is set in the Binding Update,

then this is a request to delete the cached binding for the home address and the Binding Update is processed according to the procedure specified in Section 10.3.2.

RFC Text:

If the Binding Update is valid according to the tests above, then the Binding Update is processed further as follows:

o The Sequence Number value received from a mobile node in a Binding Update is stored by the receiving node in its Binding Cache entry for the given home address.

o If the Lifetime specified in the Binding Update is nonzero and the specified care-of address is not equal to the home address for the binding, then this is a request to cache a binding for the home address. If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.1; otherwise, it is processed according to the procedure specified in Section 9.5.2.

o **If the Lifetime specified in the Binding Update is zero or the specified care-of address matches the home address for the binding, then this is a request to delete the cached binding for the home address.** In this case, **the Binding Update MUST include a valid home nonce index**, and the care-of nonce index MUST be ignored by the correspondent node. The generation of the binding management key depends then exclusively on the home keygen token (Section 5.2.5). **If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.2;** otherwise, it is processed according to the procedure specified in Section 9.5.3.

Identifier: RQ_001_1450
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

If the Correspondant node validates a Binding Update where:

- the Lifetime specified in the Binding Update is zero or the specified care-of address matches the home address for the binding
- the Binding Update includes a valid home nonce index

then this is a request to delete the cached binding for the home address and the care-of nonce index MUST be ignored by the correspondent node.

The generation of the binding management key depends then exclusively on the home keygen token (Section 5.2.5).

RFC Text:

If the Binding Update is valid according to the tests above, **then the Binding Update is processed further as follows**:

o The Sequence Number value received from a mobile node in a Binding Update is stored by the receiving node in its Binding Cache entry for the given home address.

o If the Lifetime specified in the Binding Update is nonzero and the specified care-of address is not equal to the home address for the binding, then this is a request to cache a binding for the home address. If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.1; otherwise, it is processed according to the procedure specified in Section 9.5.2.

o **If the Lifetime specified in the Binding Update is zero** or the specified care-of address matches the home address for the binding, then this is a request to delete the cached binding for the home address. In this case, the Binding Update MUST include a valid home nonce index, and **the care-of nonce index MUST be ignored by the correspondent node. The generation of the binding management key depends then exclusively on the home keygen token (Section 5.2.5).** If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.2; otherwise, it is processed according to the procedure specified in Section 9.5.3.

Identifier: RQ_001_1451
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

If the Correspondant node validates a Binding Update where:

- the Lifetime specified in the Binding Update is zero or the specified care-of address matches the home address for the binding
- the Binding Update includes a valid home nonce index
- and the Home Registration (H) bit is not set in the Binding Update,

then this is a request to delete a cached binding and the Binding Update is processed according to the procedure specified in Section 9.5.3

RFC Text:

If the Binding Update is valid according to the tests above**, then the Binding Update is processed further as follows**:

o The Sequence Number value received from a mobile node in a Binding Update is stored by the receiving node in its Binding Cache entry for the given home address.

o If the Lifetime specified in the Binding Update is nonzero and the specified care-of address is not equal to the home address for the binding, then this is a request to cache a binding for the home address. If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.1; otherwise, it is processed according to the procedure specified in Section 9.5.2.

o **If the Lifetime specified in the Binding Update is zero or the specified care-of address matches the home address for the binding, then this is a request to delete the cached binding for the home address. In this case, the Binding Update MUST include a valid home nonce index, and the care-of nonce index MUST be ignored by the correspondent node. The generation of the binding management key depends then exclusively on the home keygen token (Section 5.2.5). If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.2; otherwise, it is processed according to the procedure specified in Section 9.5.3.**

Identifier: RQ_001_1452
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Correspondant node validates a Binding Update where:

- the Lifetime specified in the Binding Update is nonzero
- the specified care-of address is not equal to the home address for the binding
- the Home Registration (H) bit is set in the Binding Update

then this is a request to cache a binding for the home address and is processed according to the procedure specified in Section 10.3.1.

RFC Text:
If the Binding Update is valid according to the tests above, then the Binding Update is processed further as follows:

o The Sequence Number value received from a mobile node in a Binding Update is stored by the receiving node in its Binding Cache entry for the given home address.

o **If the Lifetime specified in the Binding Update is nonzero and the specified care-of address is not equal to the home address for the binding, then this is a request to cache a binding for the home address. If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.**1; otherwise, it is processed according to the procedure specified in Section 9.5.2.

o If the Lifetime specified in the Binding Update is zero or the specified care-of address matches the home address for the binding, then this is a request to delete the cached binding for the home address. In this case, the Binding Update MUST include a valid home nonce index, and the care-of nonce index MUST be ignored by the correspondent node. The generation of the binding management key depends then exclusively on the home keygen token (Section 5.2.5). If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.2; otherwise, it is processed according to the procedure specified in Section 9.5.3.

Identifier: RQ_001_1453
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Update, if the Alternate Care-of Address option is present, the specified care-of address MUST be the care-of address specified in the the Alternate Care-of Address option.

RFC Text:
The specified care-of address MUST be determined as follows:

o If the Alternate Care-of Address option is present, the care-of address is the address in that option.

o Otherwise, the care-of address is the Source Address field in the packet's IPv6 header.

Identifier: RQ_001_1453
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Binding Update, if the Alternate Care-of Address option is present, the specified care-of address MUST be the care-of address specified in the the Alternate Care-of Address option.

RFC Text:
The specified care-of address MUST be determined as follows:

o If the Alternate Care-of Address option is present, the care-of address is the address in that option.

o Otherwise, the care-of address is the Source Address field in the packet's IPv6 header.

Identifier: RQ_001_1454
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Update, if the Alternate Care-of Address option is not present, the care-of address MUST be the Source Address field in the packet's IPv6 header.

RFC Text:
The specified care-of address MUST be determined as follows:

o If the Alternate Care-of Address option is present, the care-of address is the address in that option.

o Otherwise, the care-of address is the Source Address field in the packet's IPv6 header.:

Identifier: RQ_001_1454
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Binding Update, if the Alternate Care-of Address option is not present, the care-of address MUST be the Source Address field in the packet's IPv6 header.

RFC Text:
The specified care-of address MUST be determined as follows:

o If the Alternate Care-of Address option is present, the care-of address is the address in that option.

o Otherwise, the care-of address is the Source Address field in the packet's IPv6 header.:

Identifier: RQ_001_1455
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Update, if the Home Address destination option is present, the home address for the binding MUST the home address is the address in that option.

RFC Text:
The home address for the binding MUST be determined as follows:

o If the Home Address destination option is present, the home address is the address in that option.

o Otherwise, the home address is the Source Address field in the packet's IPv6 header.

Identifier: RQ_001_1455
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Binding Update, if the Home Address destination option is present, the home address for the binding MUST the home address is the address in that option.

RFC Text:
The home address for the binding MUST be determined as follows:

o If the Home Address destination option is present, the home address is the address in that option.

o Otherwise, the home address is the Source Address field in the packet's IPv6 header.

Identifier: RQ_001_1456
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
In the Binding Update, if the Home Address destination option is not present, the home address for the binding MUST be the Source Address field in the packet's IPv6 header.

RFC Text:
The home address for the binding MUST be determined as follows:

o If the Home Address destination option is present, the home address is the address in that option.

o Otherwise, the home address is the Source Address field in the packet's IPv6 header.

Identifier: RQ_001_1456
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Binding Update, if the Home Address destination option is not present, the home address for the binding MUST be the Source Address field in the packet's IPv6 header.

RFC Text:
The home address for the binding MUST be determined as follows:

o If the Home Address destination option is present, the home address is the address in that option.

o Otherwise, the home address is the Source Address field in the packet's IPv6 header.

Identifier: RQ_001_1457
RFC Clause: 9.5.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
On receipt of a valid Binding Update that requests a node to cache a binding, for which the Home Registration (H) bit is not set in the Binding Update, the receiving node SHOULD, if such an entry does not already exists, create a new entry in its Binding Cache for this home address.

RFC Text:
This section describes the processing of a valid Binding Update that requests a node to cache a binding, for which the Home Registration (H) bit is not set in the Binding Update.

In this case, the receiving node SHOULD create a new entry in its Binding Cache for this home address, or update its existing Binding Cache entry for this home address, if such an entry already exists. The lifetime for the Binding Cache entry is initialized from the Lifetime field specified in the Binding Update, although this lifetime MAY be reduced by the node caching the binding; the lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update. Any Binding Cache entry MUST be deleted after the expiration of its lifetime.

Identifier: RQ_001_1458
RFC Clause: 9.5.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
On receipt of a valid Binding Update that requests a node to cache a binding, for which the Home Registration (H) bit is not set in the Binding Update, the receiving node SHOULD, if such an entry already exists, update its existing Binding Cache entry for this home address.

RFC Text:
This section describes the processing of a valid Binding Update that requests a node to cache a binding, for which the Home Registration (H) bit is not set in the Binding Update.

In this case, the receiving node SHOULD create a new entry in its Binding Cache for this home address, or **update its existing Binding Cache entry for this home address, if such an entry already exists**. The lifetime for the Binding Cache entry is initialized from the Lifetime field specified in the Binding Update, although this lifetime MAY be reduced by the node caching the binding; the lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update. Any Binding Cache entry MUST be deleted after the expiration of its lifetime.

Identifier: RQ_001_1459
RFC Clause: 9.5.2
Type: Optional
Applies to: Correspondent_Node

Requirement:
The lifetime for the Binding Cache entry MAY be reduced by the node caching the binding;

RFC Text:
This section describes the processing of a valid Binding Update that requests a node to cache a binding, for which the Home Registration (H) bit is not set in the Binding Update.

In this case, the receiving node SHOULD create a new entry in its Binding Cache for this home address, or update its existing Binding Cache entry for this home address, if such an entry already exists. The lifetime for the Binding Cache entry is initialized from the Lifetime field specified in the Binding Update, although **this lifetime MAY be reduced by the node caching the binding**; the lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update. Any Binding Cache entry MUST be deleted after the expiration of its lifetime.

Identifier: RQ_001_1460
RFC Clause: 9.5.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update.

RFC Text:
This section describes the processing of a valid Binding Update that requests a node to cache a binding, for which the Home Registration (H) bit is not set in the Binding Update.

In this case, the receiving node SHOULD create a new entry in its Binding Cache for this home address, or update its existing Binding Cache entry for this home address, if such an entry already exists. The lifetime for the Binding Cache entry is initialized from the Lifetime field specified in the Binding Update, although this lifetime MAY be reduced by the node caching the binding; **the lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update.** Any Binding Cache entry MUST be deleted after the expiration of its lifetime.

Identifier: RQ_001_1461
RFC Clause: 9.5.2
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Any Binding Cache entry MUST be deleted after the expiration of its lifetime.

RFC Text:
This section describes the processing of a valid Binding Update that requests a node to cache a binding, for which the Home Registration (H) bit is not set in the Binding Update.

In this case, the receiving node SHOULD create a new entry in its Binding Cache for this home address, or update its existing Binding Cache entry for this home address, if such an entry already exists. The lifetime for the Binding Cache entry is initialized from the Lifetime field specified in the Binding Update, although this lifetime MAY be reduced by the node caching the binding; the lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update. **Any Binding Cache entry MUST be deleted after the expiration of its lifetime.**

Identifier: RQ_001_1462
RFC Clause: 9.5.2
Type: Optional
Applies to: Correspondent_Node

Requirement:
The correspondent node MAY refuse to accept a new Binding Cache entry if it does not have sufficient resources.

RFC Text:
The correspondent node MAY refuse to accept a new Binding Cache entry if it does not have sufficient resources. A new entry MAY also be refused if the correspondent node believes its resources are utilized more efficiently in some other purpose, such as serving another mobile node with higher amount of traffic. In both cases the correspondent node SHOULD return a Binding Acknowledgement with status value 130.

Identifier: RQ_001_1463
RFC Clause: 9.5.2
Type: Optional
Applies to: Correspondent_Node

Requirement:
The correspondent node MAY refuse to accept a new Binding Cache entry if the correspondent node believes its resources are utilized more efficiently in some other purpose, such as serving another mobile node with higher amount of traffic.

RFC Text:
The correspondent node MAY refuse to accept a new Binding Cache entry if it does not have sufficient resources. **A new entry MAY also be refused if the correspondent node believes its resources are utilized more efficiently in some other purpose, such as serving another mobile node with higher amount of traffic.** In both cases the correspondent node SHOULD return a Binding Acknowledgement with status value 130.

Identifier: RQ_001_1464
RFC Clause: 9.5.2
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
If the correspondent node refuses to accept a new Binding Cache entry, if it does not have sufficient resources or it believes its resources are utilized more efficiently in some other purpose, it SHOULD return a Binding Acknowledgement with status value 130.

RFC Text:
The correspondent node MAY refuse to accept a new Binding Cache entry if it does not have sufficient resources. A new entry MAY also be refused if the correspondent node believes its resources are utilized more efficiently in some other purpose, such as serving another mobile node with higher amount of traffic. **In both cases the correspondent node SHOULD return a Binding Acknowledgement with status value 130.**

Identifier: RQ_001_1465
RFC Clause: 9.5.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
On receipt of a valid Binding Update that requests a node to delete a binding when the Home Registration (H) bit is not set in the Binding Update, any existing binding for the given home address MUST be deleted.

RFC Text:
This section describes the processing of a valid Binding Update that requests a node to delete a binding when the Home Registration (H) bit is not set in the Binding Update.

Any existing binding for the given home address MUST be deleted. A Binding Cache entry for the home address MUST NOT be created in response to receiving the Binding Update.

Identifier: RQ_001_1466
RFC Clause: 9.5.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
On receipt of a valid Binding Update that requests a node to delete a binding when the Home Registration (H) bit is not set in the Binding Update, a Binding Cache entry for the home address MUST NOT be created in response to receiving the Binding Update.

RFC Text:
This section describes the processing of a valid Binding Update that requests a node to delete a binding when the Home Registration (H) bit is not set in the Binding Update.

Any existing binding for the given home address MUST be deleted. **A Binding Cache entry for the home address MUST NOT be created in response to receiving the Binding Update.**

Identifier: RQ_001_1467
RFC Clause: 9.5.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Binding Cache entry was created by use of return routability nonces, the correspondent node MUST ensure that the same nonces are not used again with the particular home and care-of address.

RFC Text:
If the Binding Cache entry was created by use of return routability nonces, the correspondent node MUST ensure that the same nonces are not used again with the particular home and care-of address.
If both nonces are still valid, the correspondent node has to remember the particular combination of nonce indexes, addresses, and sequence number as illegal until at least one of the nonces has become too old.

Identifier: RQ_001_1468
RFC Clause: 9.5.3
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If both nonces are still valid, the correspondent node has to remember the particular combination of nonce indexes, addresses, and sequence number as illegal until at least one of the nonces has become too old.

RFC Text:
If the Binding Cache entry was created by use of return routability nonces, the correspondent node MUST ensure that the same nonces are not used again with the particular home and care-of address. **If both nonces are still valid, the correspondent node has to remember the particular combination of nonce indexes, addresses, and sequence number as illegal until at least one of the nonces has become too old.**

Identifier: RQ_001_1469
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a received Binding Update message is not valid (according to RFC3775 section 9.2 and 9.5.1) the Node MUST NOT send a Binding Acknowledgement.

RFC Text:
A Binding Acknowledgement may be sent to indicate receipt of a Binding Update as follows:

o If the Binding Update was discarded as described in Section 9.2 or Section 9.5.1, a Binding Acknowledgement MUST NOT be sent. Otherwise the treatment depends on the following rules.

o If the Acknowledge (A) bit set is set in the Binding Update, a Binding Acknowledgement MUST be sent. Otherwise, the treatment depends on the below rule.

o If the node rejects the Binding Update due to an expired nonce index, sequence number being out of window (Section 9.5.1), or insufficiency of resources (Section 9.5.2), a Binding Acknowledgement MUST be sent. If the node accepts the Binding Update, the Binding Acknowledgement SHOULD NOT be sent.

Identifier: RQ_001_1470
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a received Binding Update message has the Acknowledge (A) bit set is set a Binding Acknowledgement MUST be sent.

RFC Text:
A Binding Acknowledgement may be sent to indicate receipt of a Binding Update as follows:

o If the Binding Update was discarded as described in Section 9.2 or Section 9.5.1, a Binding Acknowledgement MUST NOT be sent. Otherwise the treatment depends on the following rules.

o **If the Acknowledge (A) bit set is set in the Binding Update, a Binding Acknowledgement MUST be sent.** Otherwise, the treatment depends on the below rule.

o If the node rejects the Binding Update due to an expired nonce index, sequence number being out of window (Section 9.5.1), or insufficiency of resources (Section 9.5.2), a Binding Acknowledgement MUST be sent. If the node accepts the Binding Update, the Binding Acknowledgement SHOULD NOT be sent.

Identifier: RQ_001_1471
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If a node rejects the Binding Update due to an expired nonce index, sequence number being out of window, or insufficiency of resources, a Binding Acknowledgement MUST be sent.

RFC Text:
A Binding Acknowledgement may be sent to indicate receipt of a Binding Update as follows:

o If the Binding Update was discarded as described in Section 9.2 or Section 9.5.1, a Binding Acknowledgement MUST NOT be sent. Otherwise the treatment depends on the following rules.

o If the Acknowledge (A) bit set is set in the Binding Update, a Binding Acknowledgement MUST be sent. Otherwise, the treatment depends on the below rule.

o If the node rejects the Binding Update due to an expired nonce index, sequence number being out of window (Section 9.5.1), or insufficiency of resources (Section 9.5.2), a Binding Acknowledgement MUST be sent. If the node accepts the Binding Update, the Binding Acknowledgement SHOULD NOT be sent.

Identifier: RQ_001_1472
RFC Clause: 9.5.4
Type: Recommendation
Applies to: Correspondent_Node

Requirement:
If a node accepts the Binding Update, and the Acknowledge (A) bit is NOT set in the Binding Update, the Binding Acknowledgement SHOULD NOT be sent.

RFC Text:
A Binding Acknowledgement may be sent to indicate receipt of a Binding Update as follows:

o If the Binding Update was discarded as described in Section 9.2 or Section 9.5.1, a Binding Acknowledgement MUST NOT be sent. Otherwise the treatment depends on the following rules.

o If the Acknowledge (A) bit set is set in the Binding Update, a Binding Acknowledgement MUST be sent. Otherwise, the treatment depends on the below rule.

o If the node rejects the Binding Update due to an expired nonce index, sequence number being out of window (Section 9.5.1), or insufficiency of resources (Section 9.5.2), a Binding Acknowledgement MUST be sent. **If the node accepts the Binding Update, the Binding Acknowledgement SHOULD NOT be sent.**

Identifier: RQ_001_1473
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the node accepts the Binding Update and creates or updates an entry for this binding, the Status field in the Binding Acknowledgement MUST be set to a value less than 128.

RFC Text:
If the node accepts the Binding Update and creates or updates an entry for this binding, the Status field in the Binding Acknowledgement MUST be set to a value less than 128. Otherwise, the Status field MUST be set to a value greater than or equal to 128. Values for the Status field are described in Section 6.1.8 and in the IANA registry of assigned numbers [19].

Identifier: RQ_001_1474
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the node DOES NOT accept the Binding Update, the Status field in the Binding Acknowledgement MUST be set to a value greater than or equal to 128.

RFC Text:
If the node accepts the Binding Update and creates or updates an entry for this binding, the Status field in the Binding Acknowledgement MUST be set to a value less than 128. Otherwise, the Status field MUST be set to a value greater than or equal to 128. Values for the Status field are described in Section 6.1.8 and in the IANA registry of assigned numbers [19].

Identifier: RQ_001_1475
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Status field in the Binding Acknowledgement contains the value 136 (expired home nonce index), 137 (expired care-of nonce index), or 138 (expired nonces) then the message MUST NOT include the Binding Authorization Data mobility option.

RFC Text:
If the Status field in the Binding Acknowledgement contains the value 136 (expired home nonce index), 137 (expired care-of nonce index), or 138 (expired nonces) then the message MUST NOT include the Binding Authorization Data mobility option. Otherwise, the Binding Authorization Data mobility option MUST be included, and MUST meet the specific authentication requirements for Binding Acknowledgements as defined in Section 5.2.

Identifier: RQ_001_1476
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Status field in the Binding Acknowledgement DOES NOTcontain the value 136 (expired home nonce index), 137 (expired care-of nonce index), or 138 (expired nonces) then the Binding Authorization Data mobility option MUST be included,

RFC Text:
If the Status field in the Binding Acknowledgement contains the value 136 (expired home nonce index), 137 (expired care-of nonce index), or 138 (expired nonces) then the message MUST NOT include the Binding Authorization Data mobility option. Otherwise, the Binding Authorization Data mobility option MUST be included, and MUST meet the specific authentication requirements for Binding Acknowledgements as defined in Section 5.2.

Identifier: RQ_001_1477
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Status field in the Binding Acknowledgement DOES NOTcontain the value 136 (expired home nonce index), 137 (expired care-of nonce index), or 138 (expired nonces) then the Binding Authorization Data mobility option MUST meet the specific authentication requirements for Binding Acknowledgements as defined in Section 5.2.

RFC Text:
If the Status field in the Binding Acknowledgement contains the value 136 (expired home nonce index), 137 (expired care-of nonce index), or 138 (expired nonces) then the message MUST NOT include the Binding Authorization Data mobility option. Otherwise, the Binding Authorization Data mobility option MUST be included, and MUST meet the specific authentication requirements for Binding Acknowledgements as defined in Section 5.2.

Identifier: RQ_001_1478
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Source Address field of the IPv6 header that carried the Binding Update does not contain a unicast address, the Binding Acknowledgement MUST NOT be sent.

RFC Text:
If the Source Address field of the IPv6 header that carried the Binding Update does not contain a unicast address, the Binding Acknowledgement MUST NOT be sent and the Binding Update packet MUST be silently discarded. Otherwise, the acknowledgement MUST be sent to the Source Address. Unlike the treatment of regular packets, this addressing procedure does not use information from the Binding Cache. However, a routing header is needed in some cases. If the Source Address is the home address of the mobile node, i.e., the Binding Update did not contain a Home Address destination option, then the Binding Acknowledgement MUST be sent to that address and the routing header MUST NOT be used. Otherwise, the Binding Acknowledgement MUST be sent using a type 2 routing header which contains the mobile node's home address.

Identifier: RQ_001_1479
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Source Address field of the IPv6 header that carried the Binding Update does not contain a unicast address, the Binding Update packet MUST be silently discarded.

RFC Text:
If the Source Address field of the IPv6 header that carried the Binding Update does not contain a unicast address, the Binding Acknowledgement MUST NOT be sent and the Binding Update packet MUST be silently discarded. Otherwise, the acknowledgement MUST be sent to the Source Address. Unlike the treatment of regular packets, this addressing procedure does not use information from the Binding Cache. However, a routing header is needed in some cases. If the Source Address is the home address of the mobile node, i.e., the Binding Update did not contain a Home Address destination option, then the Binding Acknowledgement MUST be sent to that address and the routing header MUST NOT be used. Otherwise, the Binding Acknowledgement MUST be sent using a type 2 routing header which contains the mobile node's home address.

Identifier: RQ_001_1480
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Source Address field of the IPv6 header that carried the Binding Update does contain a unicast address, the Binding Acknowledgement MUST be sent to the Source Address.

RFC Text:
If the Source Address field of the IPv6 header that carried the Binding Update does not contain a unicast address, the Binding Acknowledgement MUST NOT be sent and the Binding Update packet MUST be silently discarded. **Otherwise, the acknowledgement MUST be sent to the Source Address.** Unlike the treatment of regular packets, this addressing procedure does not use information from the Binding Cache. However, a routing header is needed in some cases. If the Source Address is the home address of the mobile node, i.e., the Binding Update did not contain a Home Address destination option, then the Binding Acknowledgement MUST be sent to that address and the routing header MUST NOT be used. Otherwise, the Binding Acknowledgement MUST be sent using a type 2 routing header which contains the mobile node's home address.

Identifier: RQ_001_1481
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

If the Source Address field of the IPv6 header that carried the Binding Update is the home address of the mobile node then the Binding Acknowledgement MUST be sent to that address and the routing header MUST NOT be used.

RFC Text:

If the Source Address field of the IPv6 header that carried the Binding Update does not contain a unicast address, the Binding Acknowledgement MUST NOT be sent and the Binding Update packet MUST be silently discarded. Otherwise, the acknowledgement MUST be sent to the Source Address. Unlike the treatment of regular packets, this addressing procedure does not use information from the Binding Cache. However, a routing header is needed in some cases. **If the Source Address is the home address of the mobile node, i.e., the Binding Update did not contain a Home Address destination option, then the Binding Acknowledgement MUST be sent to that address and the routing header MUST NOT be used.** Otherwise, the Binding Acknowledgement MUST be sent using a type 2 routing header which contains the mobile node's home address.

Identifier: RQ_001_1482
RFC Clause: 9.5.4
Type: Mandatory
Applies to: Correspondent_Node

Requirement:

If the Source Address field of the IPv6 header that carried the Binding Update is NOT the home address of the mobile node then the Binding Acknowledgement MUST be sent using a type 2 routing header which contains the mobile node's home address.

RFC Text:

If the Source Address field of the IPv6 header that carried the Binding Update does not contain a unicast address, the Binding Acknowledgement MUST NOT be sent and the Binding Update packet MUST be silently discarded. Otherwise, the acknowledgement MUST be sent to the Source Address. Unlike the treatment of regular packets, this addressing procedure does not use information from the Binding Cache. However, a routing header is needed in some cases. If the Source Address is the home address of the mobile node, i.e., the Binding Update did not contain a Home Address destination option, then the Binding Acknowledgement MUST be sent to that address and the routing header MUST NOT be used. **Otherwise, the Binding Acknowledgement MUST be sent using a type 2 routing header which contains the mobile node's home address.**

Identifier: RQ_001_1483
RFC Clause: 9.5.5
Type: Optional
Applies to: Correspondent_Node

Requirement:

If the sender knows that the Binding Cache entry is still in active use, it MAY send a Binding Refresh Request message to the mobile node in an attempt to avoid the overhead and latency due to deleting and recreating the Binding Cache entry. This message is always sent to the home address of the mobile node

RFC Text:

If the sender knows that the Binding Cache entry is still in active use, it MAY send a Binding Refresh Request message to the mobile node in an attempt to avoid this overhead and latency due to deleting and recreating the Binding Cache entry. This message is always sent to the home address of the mobile node

Identifier: RQ_001_1484
RFC Clause: 9.5.5
Type: Optional
Applies to: Correspondent_Node

Requirement:
The correspondent node MAY retransmit Binding Refresh Request messages as long as the rate limitation is applied.

RFC Text:
The correspondent node MAY retransmit Binding Refresh Request messages as long as the rate limitation is applied. The correspondent node MUST stop retransmitting when it receives a Binding Update.

Identifier: RQ_001_1485
RFC Clause: 9.5.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The correspondent node MUST stop retransmitting Binding Refresh Request messages when it receives a Binding Update.

RFC Text:
The correspondent node MAY retransmit Binding Refresh Request messages as long as the rate limitation is applied. **The correspondent node MUST stop retransmitting when it receives a Binding Update.**

Identifier: RQ_001_1486
RFC Clause: 9.6
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Any entry in a node's Binding Cache MUST be deleted after the expiration of the Lifetime specified in the Binding Update from which the entry was created or last updated.

RFC Text:
Conceptually, a node maintains a separate timer for each entry in its Binding Cache. When creating or updating a Binding Cache entry in response to a received and accepted Binding Update, the node sets the timer for this entry to the specified Lifetime period. **Any entry in a node's Binding Cache MUST be deleted after the expiration of the Lifetime specified in the Binding Update from which the entry was created or last updated.**

Identifier: RQ_001_1486
RFC Clause: 9.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
Any entry in a node's Binding Cache MUST be deleted after the expiration of the Lifetime specified in the Binding Update from which the entry was created or last updated.

RFC Text:
Conceptually, a node maintains a separate timer for each entry in its Binding Cache. When creating or updating a Binding Cache entry in response to a received and accepted Binding Update, the node sets the timer for this entry to the specified Lifetime period. **Any entry in a node's Binding Cache MUST be deleted after the expiration of the Lifetime specified in the Binding Update from which the entry was created or last updated.**

Identifier: RQ_001_1488
RFC Clause: 10.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Each home agent MUST maintain a Binding Cache.

RFC Text:
Each home agent MUST maintain a Binding Cache and Home Agents List.

Identifier: RQ_001_1489
RFC Clause: 10.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Each home agent MUST maintain a Home Agents List.

RFC Text:
Each home agent MUST maintain a Binding Cache and **Home Agents List.**

Identifier: RQ_001_1490
RFC Clause: 10.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Global addresses for the router in a Home Agents List entry MUST be deleted once the prefix associated with that address is no longer valid.

RFC Text:
Each home agent maintains a separate Home Agents List for each link on which it is serving as a home agent. A new entry is created or an existing entry is updated in response to receipt of a valid Router Advertisement in which the Home Agent (H) bit is set. Each Home Agents List entry conceptually contains the following fields:

- The link-local IP address of a home agent on the link. This address is learned through the Source Address of the Router Advertisements [12] received from the router.

- One or more global IP addresses for this home agent. Global addresses are learned through Prefix Information options with the Router Address (R) bit set and received in Router Advertisements from this link-local address. **Global addresses for the router in a Home Agents List entry MUST be deleted once the prefix associated with that address is no longer valid [12].**

- The remaining lifetime of this Home Agents List entry. If a Home Agent Information Option is present in a Router Advertisement received from a home agent, the lifetime of the Home Agents List entry representing that home agent is initialized from the Home Agent Lifetime field in the option (if present); otherwise, the lifetime is initialized from the Router Lifetime field in the received Router Advertisement. If Home Agents List entry lifetime reaches zero, the entry MUST be deleted from the Home Agents List.

- The preference for this home agent; higher values indicate a more preferable home agent. The preference value is taken from the Home Agent Preference field in the received Router Advertisement, if the Router Advertisement contains a Home Agent Information Option and is otherwise set to the default value of 0. A home agent uses this preference in ordering the Home Agents List when it sends an ICMP Home Agent Address Discovery message.

Identifier: RQ_001_1491
RFC Clause: 10.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
. If Home Agents List entry lifetime reaches zero, the entry MUST be deleted from the Home Agents List.

RFC Text:
Each home agent maintains a separate Home Agents List for each link on which it is serving as a home agent. A new entry is created or an existing entry is updated in response to receipt of a valid Router Advertisement in which the Home Agent (H) bit is set. Each Home Agents List entry conceptually contains the following fields:

- o The link-local IP address of a home agent on the link. This address is learned through the Source Address of the Router Advertisements [12] received from the router.

- o One or more global IP addresses for this home agent. Global addresses are learned through Prefix Information options with the Router Address (R) bit set and received in Router Advertisements from this link-local address. Global addresses for the router in a Home Agents List entry MUST be deleted once the prefix associated with that address is no longer valid [12].

- o The remaining lifetime of this Home Agents List entry. If a Home Agent Information Option is present in a Router Advertisement received from a home agent, the lifetime of the Home Agents List entry representing that home agent is initialized from the Home Agent Lifetime field in the option (if present); otherwise, the lifetime is initialized from the Router Lifetime field in the received Router Advertisement. **If Home Agents List entry lifetime reaches zero, the entry MUST be deleted from the Home Agents List.**

- o The preference for this home agent; higher values indicate a more preferable home agent. The preference value is taken from the Home Agent Preference field in the received Router Advertisement, if the Router Advertisement contains a Home Agent Information Option and is otherwise set to the default value of 0. A home agent uses this preference in ordering the Home Agents List when it sends an ICMP Home Agent Address Discovery message.

Identifier: RQ_001_1492
RFC Clause: 10.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
All IPv6 Home Agents MUST observe the rules described in RFC3775 Section 9.2 when processing Mobility Headers.

RFC Text:
All IPv6 home agents MUST observe the rules described in Section 9.2 when processing Mobility Headers.

Identifier: RQ_001_1493
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In processing the Binding Update, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent MUST reject the Binding Update.

RFC Text:
To begin processing the Binding Update, the home agent MUST perform the following sequence of tests:

- **If the node implements only correspondent node functionality, or has not been configured to act as a home agent, then the node MUST reject the Binding Update. The node MUST also return a Binding Acknowledgement to the mobile node, in which the Status field is set to 131 (home registration not supported).**

- **Else, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (not home subnet).**

- **Else, if the home agent chooses to reject the Binding Update for any other reason (e.g., insufficient resources to serve another mobile node as a home agent), then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to an appropriate value to indicate the reason for the rejection.**

- **A Home Address destination option MUST be present in the message. It MUST be validated as described in Section 9.3.1 with the following additional rule. The Binding Cache entry existence test MUST NOT be done for IPsec packets when the Home Address option contains an address for which the receiving node could act as a home agent.**

Identifier: RQ_001_1494
RFC Clause: 10.3.1
Type: Recommendation
Applies to: Home_Agent

Requirement:

In processing the Binding Update, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (not home subnet).

RFC Text:

To begin processing the Binding Update, the home agent MUST perform the following sequence of tests:

- If the node implements only correspondent node functionality, or has not been configured to act as a home agent, then the node MUST reject the Binding Update. The node MUST also return a Binding Acknowledgement to the mobile node, in which the Status field is set to 131 (home registration not supported).

- **Else, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent** MUST reject the Binding Update and **SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (not home subnet).**

- Else, if the home agent chooses to reject the Binding Update for any other reason (e.g., insufficient resources to serve another mobile node as a home agent), then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to an appropriate value to indicate the reason for the rejection.

- A Home Address destination option MUST be present in the message. It MUST be validated as described in Section 9.3.1 with the following additional rule. The Binding Cache entry existence test MUST NOT be done for IPsec packets when the Home Address option contains an address for which the receiving node could act as a home agent.

Identifier: RQ_001_1495
RFC Clause: 10.3.1
Type: Recommendation
Applies to: Home_Agent

Requirement:

In processing the Binding Update, if the home agent chooses to reject the Binding Update for any unspecified reason (e.g., insufficient resources to serve another mobile node as a home agent), then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to an appropriate value to indicate the reason for the rejection.

RFC Text:

To begin processing the Binding Update, the home agent MUST perform the following sequence of tests:

- If the node implements only correspondent node functionality, or has not been configured to act as a home agent, then the node MUST reject the Binding Update. The node MUST also return a Binding Acknowledgement to the mobile node, in which the Status field is set to 131 (home registration not supported).

- Else, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (not home subnet).

- **Else, if the home agent chooses to reject the Binding Update for any other reason (e.g., insufficient resources to serve another mobile node as a home agent), then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to an appropriate value to indicate the reason for the rejection.**

- A Home Address destination option MUST be present in the message. It MUST be validated as described in Section 9.3.1 with the following additional rule. The Binding Cache entry existence test MUST NOT be done for IPsec packets when the Home Address option contains an address for which the receiving node could act as a home agent.

Identifier: RQ_001_1496
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Node

Requirement:
If the node rejects a Binding Update because it implements only correspondent node functionality, or has not been configured to act as a home agent, then the node MUST also return a Binding Acknowledgement to the mobile node, in which the Status field is set to 131 (home registration not supported).

RFC Text:
To begin processing the Binding Update, the home agent MUST perform the following sequence of tests:

- **If the node implements only correspondent node functionality, or has not been configured to act as a home agent, then the node MUST reject the Binding Update. The node MUST also return a Binding Acknowledgement to the mobile node, in which the Status field is set to 131 (home registration not supported).**

- Else, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (not home subnet).

- Else, if the home agent chooses to reject the Binding Update for any other reason (e.g., insufficient resources to serve another mobile node as a home agent), then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to an appropriate value to indicate the reason for the rejection.

- A Home Address destination option MUST be present in the message. It MUST be validated as described in Section 9.3.1 with the following additional rule. The Binding Cache entry existence test MUST NOT be done for IPsec packets when the Home Address option contains an address for which the receiving node could act as a home agent.

Identifier: RQ_001_1497
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If home agent accepts the Binding Update, it MUST then create a new entry in its Binding Cache for this mobile node if no such entry exists.

RFC Text:
If home agent accepts the Binding Update, it MUST then create a new entry in its Binding Cache for this mobile node or update its existing Binding Cache entry, if such an entry already exists. The Home Address field as received in the Home Address option provides the home address of the mobile node.

Identifier: RQ_001_1498
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When a Home Agent is updating its Binding Cache following the acceptation of a Binding Update, the Home Agent MUST mark the Binding Cache entry as a home registration to indicate that it is serving as a home agent for this binding.

RFC Text:
The home agent MUST mark this Binding Cache entry as a home registration to indicate that the node is serving as a home agent for this binding. Binding Cache entries marked as a home registration MUST be excluded from the normal cache replacement policy used for the Binding Cache (Section 9.6) and MUST NOT be removed from the Binding Cache until the expiration of the Lifetime period.

Identifier: RQ_001_1499
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
A Home agent's Binding Cache entries, marked as a home registration MUST be excluded from the normal cache replacement policy used for the Binding Cache.

RFC Text:
The home agent MUST mark this Binding Cache entry as a home registration to indicate that the node is serving as a home agent for this binding. **Binding Cache entries marked as a home registration MUST be excluded from the normal cache replacement policy used for the Binding Cache (Section 9.6)** and MUST NOT be removed from the Binding Cache until the expiration of the Lifetime period.

Identifier: RQ_001_1500
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
A Home agent's Binding Cache entries, marked as a home registration MUST NOT be removed from the Binding Cache until the expiration of the Lifetime period.

RFC Text:
The home agent MUST mark this Binding Cache entry as a home registration to indicate that the node is serving as a home agent for this binding. **Binding Cache entries marked as a home registration** MUST be excluded from the normal cache replacement policy used for the Binding Cache (Section 9.6) and **MUST NOT be removed from the Binding Cache until the expiration of the Lifetime period.**

Identifier: RQ_001_1501
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Unless this home agent already has a binding for the given home address, the home agent MUST perform Duplicate Address Detection on the mobile node's home link before returning the Binding Acknowledgement.

RFC Text:
Unless this home agent already has a binding for the given home address, the home agent MUST perform Duplicate Address Detection [13] on the mobile node's home link before returning the Binding Acknowledgement. This ensures that no other node on the home link was using the mobile node's home address when the Binding Update arrived. If this Duplicate Address Detection fails for the given home address or an associated link local address, then the home agent MUST reject the complete Binding Update and MUST return a Binding Acknowledgement to the mobile node, in which the Status field is set to 134 (Duplicate Address Detection failed). When the home agent sends a successful Binding Acknowledgement to the mobile node, the home agent assures to the mobile node that its address(es) will be kept unique by the home agent for as long as the lifetime was granted for the binding.

Identifier: RQ_001_1502
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the home agent's Duplicate Address Detection fails for the given home address or an associated link local address, then the home agent MUST reject the complete Binding Update.

RFC Text:
Unless this home agent already has a binding for the given home address, the home agent MUST perform Duplicate Address Detection [13] on the mobile node's home link before returning the Binding Acknowledgement. This ensures that no other node on the home link was using the mobile node's home address when the Binding Update arrived. **If this Duplicate Address Detection fails for the given home address or an associated link local address, then the home agent MUST reject the complete Binding Update** and MUST return a Binding Acknowledgement to the mobile node, in which the Status field is set to 134 (Duplicate Address Detection failed). When the home agent sends a successful Binding Acknowledgement to the mobile node, the home agent assures to the mobile node that its address(es) will be kept unique by the home agent for as long as the lifetime was granted for the binding.

Identifier: RQ_001_1503
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the home agent's Duplicate Address Detection fails for the given home address or an associated link local address, then the home agent MUST return a Binding Acknowledgement to the mobile node, in which the Status field is set to 134 (Duplicate Address Detection failed).

RFC Text:
Unless this home agent already has a binding for the given home address, the home agent MUST perform Duplicate Address Detection [13] on the mobile node's home link before returning the Binding Acknowledgement. This ensures that no other node on the home link was using the mobile node's home address when the Binding Update arrived. **If this Duplicate Address Detection fails for the given home address or an associated link local address, then the home agent** MUST reject the complete Binding Update and **MUST return a Binding Acknowledgement to the mobile node, in which the Status field is set to 134 (Duplicate Address Detection failed).** When the home agent sends a successful Binding Acknowledgement to the mobile node, the home agent assures to the mobile node that its address(es) will be kept unique by the home agent for as long as the lifetime was granted for the binding.

Identifier: RQ_001_1504
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The lifetime for the Binding Cache entry at the home agent MUST NOT be greater than the Lifetime value specified in the Binding Update.

RFC Text:
The lifetime of the Binding Cache entry depends on a number of factors:

- **The lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update.**

- The lifetime for the Binding Cache entry MUST NOT be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address specified with the Binding Update. The remaining valid lifetime for this prefix is determined by the home agent based on its own Prefix List entry [12].

  The remaining preferred lifetime SHOULD NOT have any impact on the lifetime for the binding cache entry.

  The home agent MUST remove a binding when the valid lifetime of the prefix associated with it expires.

- The home agent MAY further decrease the specified lifetime for the binding, for example based on a local policy. The resulting lifetime is stored by the home agent in the Binding Cache entry, and this Binding Cache entry MUST be deleted by the home agent after the expiration of this lifetime.

Identifier: RQ_001_1505
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The lifetime for the Binding Cache entry, at the home agent, MUST NOT be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address specified with the Binding Update.

RFC Text:
The lifetime of the Binding Cache entry depends on a number of factors:

- **The lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update.**

- **The lifetime for the Binding Cache entry MUST NOT be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address specified with the Binding Update. Th**e remaining valid lifetime for this prefix is determined by the home agent based on its own Prefix List entry [12].

  The remaining preferred lifetime SHOULD NOT have any impact on the lifetime for the binding cache entry.

  The home agent MUST remove a binding when the valid lifetime of the prefix associated with it expires.

- The home agent MAY further decrease the specified lifetime for the binding, for example based on a local policy. The resulting lifetime is stored by the home agent in the Binding Cache entry, and this Binding Cache entry MUST be deleted by the home agent after the expiration of this lifetime.

Identifier: RQ_001_1506
RFC Clause: 10.3.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
The remaining preferred lifetime for the Binding Cache entry, at the home agent, SHOULD NOT have any impact on the lifetime for the binding cache entry.

RFC Text:
The lifetime of the Binding Cache entry depends on a number of factors:

o The lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update.

o The lifetime for the Binding Cache entry MUST NOT be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address specified with the Binding Update. The remaining valid lifetime for this prefix is determined by the home agent based on its own Prefix List entry [12].

The remaining preferred lifetime SHOULD NOT have any impact on the lifetime for the binding cache entry.

The home agent MUST remove a binding when the valid lifetime of the prefix associated with it expires.

o The home agent MAY further decrease the specified lifetime for the binding, for example based on a local policy. The resulting lifetime is stored by the home agent in the Binding Cache entry, and this Binding Cache entry MUST be deleted by the home agent after the expiration of this lifetime.

Identifier: RQ_001_1507
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST remove a binding when the valid lifetime of the prefix associated with it expires

RFC Text:
The lifetime of the Binding Cache entry depends on a number of factors:

o The lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update.

o The lifetime for the Binding Cache entry MUST NOT be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address specified with the Binding Update. The remaining valid lifetime for this prefix is determined by the home agent based on its own Prefix List entry [12].

The remaining preferred lifetime SHOULD NOT have any impact on the lifetime for the binding cache entry.

The home agent MUST remove a binding when the valid lifetime of the prefix associated with it expires.

o The home agent MAY further decrease the specified lifetime for the binding, for example based on a local policy. The resulting lifetime is stored by the home agent in the Binding Cache entry, and this Binding Cache entry MUST be deleted by the home agent after the expiration of this lifetime.

Identifier: RQ_001_1508
RFC Clause: 10.3.1
Type: Optional
Applies to: Home_Agent

Requirement:
The home agent MAY further decrease the specified lifetime for the binding.

RFC Text:
The lifetime of the Binding Cache entry depends on a number of factors:

- The lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update.

- The lifetime for the Binding Cache entry MUST NOT be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address specified with the Binding Update. The remaining valid lifetime for this prefix is determined by the home agent based on its own Prefix List entry [12].

  The remaining preferred lifetime SHOULD NOT have any impact on the lifetime for the binding cache entry.

  The home agent MUST remove a binding when the valid lifetime of the prefix associated with it expires.

- **The home agent MAY further decrease the specified lifetime for the binding, for example based on a local policy.** The resulting lifetime is stored by the home agent in the Binding Cache entry, and this Binding Cache entry MUST be deleted by the home agent after the expiration of this lifetime.

Identifier: RQ_001_1509
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the home agent further decreases the specified lifetime for the binding, , the resulting lifetime is stored by the home agent in the Binding Cache entry, and this Binding Cache entry MUST be deleted by the home agent after the expiration of this lifetime.

RFC Text:
The lifetime of the Binding Cache entry depends on a number of factors:

- The lifetime for the Binding Cache entry MUST NOT be greater than the Lifetime value specified in the Binding Update.

- The lifetime for the Binding Cache entry MUST NOT be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address specified with the Binding Update. The remaining valid lifetime for this prefix is determined by the home agent based on its own Prefix List entry [12].

  The remaining preferred lifetime SHOULD NOT have any impact on the lifetime for the binding cache entry.

  The home agent MUST remove a binding when the valid lifetime of the prefix associated with it expires.

- The home agent MAY further decrease the specified lifetime for the binding, for example based on a local policy. **The resulting lifetime is stored by the home agent in the Binding Cache entry, and this Binding Cache entry MUST be deleted by the home agent after the expiration of this lifetime.**

Identifier: RQ_001_1510
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In response to a Binding Update message,the home agent MUST return a Binding Acknowledgement to the mobile node.

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.

* The IPsec security associations between the mobile node and the home agent have been established dynamically.

* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Identifier: RQ_001_1511
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When, after accepting a Binding Update, the Home Agent returns a Binding Acknowledgement to the mobile node, the Status field of the Binding Acknowledgement MUST be set to a value indicating success (0 or 1).

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

- **The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used otherwise.** For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

- The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

  * The Key Management Mobility Capability (K) bit was set in the Binding Update.

  * The IPsec security associations between the mobile node and the home agent have been established dynamically.

  * The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

  Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

  K = 0

  Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

  K = 1

  Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

  Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

- The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

- The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

- If the home agent stores the Binding Cache entry in nonvolatile storage, then the Binding Refresh Advice mobility option MUST be omitted. Otherwise, the home agent MAY include this option to suggest that the mobile node refreshes its binding before the actual lifetime of the binding ends.

If the Binding Refresh Advice mobility option is present, the
Refresh Interval field in the option MUST be set to a value less
than the Lifetime value being returned in the Binding
Acknowledgement. This indicates that the mobile node SHOULD
attempt to refresh its home registration at the indicated shorter
interval. The home agent MUST still retain the registration for
the Lifetime period, even if the mobile node does not refresh its
registration within the Refresh period.

Identifier: RQ_001_1512
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When, after accepting a Binding Update, the Home Agent returns a Binding Acknowledgement to the mobile node, if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime, the Status field MUST be set to the value 1 (accepted but prefix discovery necessary).

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

- **The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used otherwise.** For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

- The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

  * The Key Management Mobility Capability (K) bit was set in the Binding Update.

  * The IPsec security associations between the mobile node and the home agent have been established dynamically.

  * The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

- The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

- The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

- If the home agent stores the Binding Cache entry in nonvolatile storage, then the Binding Refresh Advice mobility option MUST be omitted. Otherwise, the home agent MAY include this option to suggest that the mobile node refreshes its binding before the actual lifetime of the binding ends.

If the Binding Refresh Advice mobility option is present, the
Refresh Interval field in the option MUST be set to a value less
than the Lifetime value being returned in the Binding
Acknowledgement. This indicates that the mobile node SHOULD
attempt to refresh its home registration at the indicated shorter
interval. The home agent MUST still retain the registration for
the Lifetime period, even if the mobile node does not refresh its
registration within the Refresh period.

Identifier: RQ_001_1513
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

When the home agent returns a Binding Acknowledgement to the mobile node, the Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.
* The IPsec security associations between the mobile node and the home agent have been established dynamically.
* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

RFC Text:

Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

*** The Key Management Mobility Capability (K) bit was set in the Binding Update.**

*** The IPsec security associations between the mobile node and the home agent have been established dynamically.**

*** The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.**

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

o The Sequence Number field MUST be copied from the Sequence Number
  given in the Binding Update.

o The Lifetime field MUST be set to the remaining lifetime for the
  binding as set by the home agent in its home registration Binding
  Cache entry for the mobile node, as described above.

o If the home agent stores the Binding Cache entry in nonvolatile
  storage, then the Binding Refresh Advice mobility option MUST be
  omitted. Otherwise, the home agent MAY include this option to
  suggest that the mobile node refreshes its binding before the
  actual lifetime of the binding ends.

  If the Binding Refresh Advice mobility option is present, the
  Refresh Interval field in the option MUST be set to a value less
  than the Lifetime value being returned in the Binding
  Acknowledgement. This indicates that the mobile node SHOULD
  attempt to refresh its home registration at the indicated shorter
  interval. The home agent MUST still retain the registration for
  the Lifetime period, even if the mobile node does not refresh its
  registration within the Refresh period.

Identifier: RQ_001_1514
RFC Clause: 10.3.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
If, when the home agent returns a Binding Acknowledgement to the mobile node, the Key Management Mobility Capability (K) bit is set to 0 (K=0) the home agent SHOULD discard key management connections, if any, to the old care-ofaddress.

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.

* The IPsec security associations between the mobile node and the home agent have been established dynamically.

* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

o The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

o The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

o If the home agent stores the Binding Cache entry in nonvolatile
  storage, then the Binding Refresh Advice mobility option MUST be
  omitted. Otherwise, the home agent MAY include this option to
  suggest that the mobile node refreshes its binding before the
  actual lifetime of the binding ends.

  If the Binding Refresh Advice mobility option is present, the
  Refresh Interval field in the option MUST be set to a value less
  than the Lifetime value being returned in the Binding
  Acknowledgement. This indicates that the mobile node SHOULD
  attempt to refresh its home registration at the indicated shorter
  interval. The home agent MUST still retain the registration for
  the Lifetime period, even if the mobile node does not refresh its
  registration within the Refresh period.

Identifier: RQ_001_1515
RFC Clause: 10.3.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
If, when the home agent returns a Binding Acknowledgement to the mobile node, the Key Management Mobility Capability (K) bit is set to 1 (K=1) the home agent SHOULD move the peer endpoint of the key management protocol connection, if any, to the new care-of address.

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.

* The IPsec security associations between the mobile node and the home agent have been established dynamically.

* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

o The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

o The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

o If the home agent stores the Binding Cache entry in nonvolatile
  storage, then the Binding Refresh Advice mobility option MUST be
  omitted. Otherwise, the home agent MAY include this option to
  suggest that the mobile node refreshes its binding before the
  actual lifetime of the binding ends.

  If the Binding Refresh Advice mobility option is present, the
  Refresh Interval field in the option MUST be set to a value less
  than the Lifetime value being returned in the Binding
  Acknowledgement. This indicates that the mobile node SHOULD
  attempt to refresh its home registration at the indicated shorter
  interval. The home agent MUST still retain the registration for
  the Lifetime period, even if the mobile node does not refresh its
  registration within the Refresh period.

Identifier: RQ_001_1516
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When the home agent returns a Binding Acknowledgement to the mobile node, the Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.

* The IPsec security associations between the mobile node and the home agent have been established dynamically.

* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

o The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

o The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

o If the home agent stores the Binding Cache entry in nonvolatile
  storage, then the Binding Refresh Advice mobility option MUST be
  omitted. Otherwise, the home agent MAY include this option to
  suggest that the mobile node refreshes its binding before the
  actual lifetime of the binding ends.

  If the Binding Refresh Advice mobility option is present, the
  Refresh Interval field in the option MUST be set to a value less
  than the Lifetime value being returned in the Binding
  Acknowledgement. This indicates that the mobile node SHOULD
  attempt to refresh its home registration at the indicated shorter
  interval. The home agent MUST still retain the registration for
  the Lifetime period, even if the mobile node does not refresh its
  registration within the Refresh period.

Identifier: RQ_001_1517
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When the home agent returns a Binding Acknowledgement to the mobile node, the Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node.

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.

* The IPsec security associations between the mobile node and the home agent have been established dynamically.

* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

o The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

o The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

o If the home agent stores the Binding Cache entry in nonvolatile
  storage, then the Binding Refresh Advice mobility option MUST be
  omitted. Otherwise, the home agent MAY include this option to
  suggest that the mobile node refreshes its binding before the
  actual lifetime of the binding ends.

  If the Binding Refresh Advice mobility option is present, the
  Refresh Interval field in the option MUST be set to a value less
  than the Lifetime value being returned in the Binding
  Acknowledgement. This indicates that the mobile node SHOULD
  attempt to refresh its home registration at the indicated shorter
  interval. The home agent MUST still retain the registration for
  the Lifetime period, even if the mobile node does not refresh its
  registration within the Refresh period.

Identifier: RQ_001_1518
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When the home agent returns a Binding Acknowledgement to the mobile node, if the home agent stores the Binding Cache entry in nonvolatile storage, then the Binding Refresh Advice mobility option MUST be omitted.

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.

* The IPsec security associations between the mobile node and the home agent have been established dynamically.

* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

o The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

o The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

o If the home agent stores the Binding Cache entry in nonvolatile storage, then the Binding Refresh Advice mobility option MUST be omitted. Otherwise, the home agent MAY include this option to suggest that the mobile node refreshes its binding before the actual lifetime of the binding ends.

If the Binding Refresh Advice mobility option is present, the Refresh Interval field in the option MUST be set to a value less than the Lifetime value being returned in the Binding Acknowledgement. This indicates that the mobile node SHOULD attempt to refresh its home registration at the indicated shorter interval. The home agent MUST still retain the registration for the Lifetime period, even if the mobile node does not refresh its registration within the Refresh period.

Identifier: RQ_001_1519
RFC Clause: 10.3.1
Type: Optional
Applies to: Home_Agent

Requirement:
When the home agent returns a Binding Acknowledgement to the mobile node, if the home agent does not store the Binding Cache entry in nonvolatile storage, then the Binding Refresh Advice mobility option MAY be included.

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.

* The IPsec security associations between the mobile node and the home agent have been established dynamically.

* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

o The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

o The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

- **If the home agent stores the Binding Cache entry in nonvolatile storage, then the Binding Refresh Advice mobility option MUST be omitted. Otherwise, the home agent MAY include this option to suggest that the mobile node refreshes its binding before the actual lifetime of the binding ends.**

  If the Binding Refresh Advice mobility option is present, the Refresh Interval field in the option MUST be set to a value less than the Lifetime value being returned in the Binding Acknowledgement. This indicates that the mobile node SHOULD attempt to refresh its home registration at the indicated shorter interval. The home agent MUST still retain the registration for the Lifetime period, even if the mobile node does not refresh its registration within the Refresh period.

Identifier: RQ_001_1520
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When the home agent returns a Binding Acknowledgement to the mobile node, if the Binding Refresh Advice mobility option is present, the Refresh Interval field in the option MUST be set to a value less than the Lifetime value being returned in the Binding Acknowledgement.

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

- The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

  otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

- The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

  * The Key Management Mobility Capability (K) bit was set in the Binding Update.

  * The IPsec security associations between the mobile node and the home agent have been established dynamically.

  * The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

  Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

  K = 0

  Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

  K = 1

  Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

  Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

- The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

- The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

o If the home agent stores the Binding Cache entry in nonvolatile
storage, then the Binding Refresh Advice mobility option MUST be
omitted. Otherwise, the home agent MAY include this option to
suggest that the mobile node refreshes its binding before the
actual lifetime of the binding ends.

If the Binding Refresh Advice mobility option is present, the Refresh Interval field in the option MUST be set to a value less than the Lifetime value being returned in the Binding Acknowledgement. This indicates that the mobile node SHOULD attempt to refresh its home registration at the indicated shorter interval. The home agent MUST still retain the registration for the Lifetime period, even if the mobile node does not refresh its registration within the Refresh period.

Identifier: RQ_001_1521
RFC Clause: 10.3.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
When the home agent returns a Binding Acknowledgement to the mobile node, if the Binding Refresh Advice mobility option is present, the Refresh Interval field in the option is set to a value less than the Lifetime value being returned in the Binding Acknowledgement indicating that the mobile node SHOULDattempt to refresh its home registration at the indicated shorter interval.

RFC Text:
Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.

* The IPsec security associations between the mobile node and the home agent have been established dynamically.

* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

o The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

o The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

o If the home agent stores the Binding Cache entry in nonvolatile
storage, then the Binding Refresh Advice mobility option MUST be
omitted. Otherwise, the home agent MAY include this option to
suggest that the mobile node refreshes its binding before the
actual lifetime of the binding ends.

If the Binding Refresh Advice mobility option is present, the
Refresh Interval field in the option MUST be set to a value less
than the Lifetime value being returned in the Binding
Acknowledgement. **This indicates that the mobile node SHOULD
attempt to refresh its home registration at the indicated shorter
interval. The home agent MUST still retain the registration for
the Lifetime period, even if the mobile node does not refresh its
registration within the Refresh period.**

Identifier: RQ_001_1522
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

When the home agent returns a Binding Acknowledgement to the mobile node, the home agent MUST retain the mobile node's registration for the Lifetime period, even if the mobile node does not refresh its registration within the Refresh period.

RFC Text:

Regardless of the setting of the Acknowledge (A) bit in the Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node constructed as follows:

o The Status field MUST be set to a value indicating success. The value 1 (accepted but prefix discovery necessary) MUST be used if the subnet prefix of the specified home address is deprecated, or becomes deprecated during the lifetime of the binding, or becomes invalid at the end of the lifetime. The value 0 MUST be used

otherwise. For the purposes of comparing the binding and prefix lifetimes, the prefix lifetimes are first converted into units of four seconds by ignoring the two least significant bits.

o The Key Management Mobility Capability (K) bit is set if the following conditions are all fulfilled, and cleared otherwise:

* The Key Management Mobility Capability (K) bit was set in the Binding Update.

* The IPsec security associations between the mobile node and the home agent have been established dynamically.

* The home agent has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves.

Depending on the final value of the bit in the Binding Acknowledgement, the home agent SHOULD perform the following actions:

K = 0

Discard key management connections, if any, to the old care-of address. If the mobile node did not have a binding before sending this Binding Update, discard the connections to the home address.

K = 1

Move the peer endpoint of the key management protocol connection, if any, to the new care-of address. For an IKE phase 1 connection, this means that any IKE packets sent to the peer are sent to this address, and packets from this address with the original ISAKMP cookies are accepted.

Note that RFC 2408 [8] Section 2.5.3 gives specific rules that ISAKMP cookies must satisfy: they must depend on specific parties and can only be generated by the entity itself. Then it recommends a particular way to do this, namely a hash of IP addresses. With the K bit set to 1, the recommended implementation technique does not work directly. To satisfy the two rules, the specific parties must be treated as the original IP addresses, not the ones in use at the specific moment.

o The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

o The Lifetime field MUST be set to the remaining lifetime for the binding as set by the home agent in its home registration Binding Cache entry for the mobile node, as described above.

o If the home agent stores the Binding Cache entry in nonvolatile
storage, then the Binding Refresh Advice mobility option MUST be
omitted. Otherwise, the home agent MAY include this option to
suggest that the mobile node refreshes its binding before the
actual lifetime of the binding ends.

If the Binding Refresh Advice mobility option is present, the
Refresh Interval field in the option MUST be set to a value less
than the Lifetime value being returned in the Binding
Acknowledgement. This indicates that the mobile node SHOULD
attempt to refresh its home registration at the indicated shorter
interval. **The home agent MUST still retain the registration for
the Lifetime period, even if the mobile node does not refresh its
registration within the Refresh period.**

Identifier: RQ_001_1523
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST follow the procedure defined in RFC3775 Section 10.4.1 to intercept packets on the mobile node's home link addressed to the mobile node, while the home agent is serving as the home agent for this mobile node.

RFC Text:
In addition, the home agent MUST follow the procedure defined in Section 10.4.1 to intercept packets on the mobile node's home link addressed to the mobile node, while the home agent is serving as the home agent for this mobile node. The home agent MUST also be prepared to accept reverse tunneled packets from the new care-of address of the mobile node, as described in Section 10.4.5. Finally, the home agent MUST also propagate new home network prefixes, as described in Section 10.6.

Identifier: RQ_001_1524
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST be prepared to accept reverse tunneled packets from the new care-of address of the mobile node, as described in Section 10.4.5.

RFC Text:
In addition, the home agent MUST follow the procedure defined in Section 10.4.1 to intercept packets on the mobile node's home link addressed to the mobile node, while the home agent is serving as the home agent for this mobile node. **The home agent MUST also be prepared to accept reverse tunneled packets from the new care-of address of the mobile node, as described in Section 10.4.5.** Finally, the home agent MUST also propagate new home network prefixes, as described in Section 10.6.

Identifier: RQ_001_1525
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST also propagate new home network prefixes, as described in Section 10.6.

RFC Text:
In addition, the home agent MUST follow the procedure defined in Section 10.4.1 to intercept packets on the mobile node's home link addressed to the mobile node, while the home agent is serving as the home agent for this mobile node. The home agent MUST also be prepared to accept reverse tunneled packets from the new care-of address of the mobile node, as described in Section 10.4.5. **Finally, the home agent MUST also propagate new home network prefixes, as described in Section 10.6.**

Identifier: RQ_001_1526
RFC Clause: 10.3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
On receipt of a Binding Update, the Home Agent MUST check its Binding Cache for the existence of an entry marked as a home registration for the Mobile Mode that sent the Binding Update. If there is no such entry, then the Home Agent MUST reject the Binding Update.

RFC Text:
To begin processing the Binding Update, the home agent MUST perform the following test:

o If the receiving node has no entry marked as a home registration in its Binding Cache for this mobile node, then this node MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 133 (not home agent for this mobile node).

Identifier: RQ_001_1527
RFC Clause: 10.3.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
On receipt of a Binding Update, the Home Agent MUST check its Binding Cache for the existence of an entry marked as a home registration for the Mobile Mode that sent the Binding Update. If there is no such entry, then the Home Agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 133 (not home agent for this mobile node).

RFC Text:
To begin processing the Binding Update, the home agent MUST perform the following test:

o **If the receiving node has no entry marked as a home registration in its Binding Cache for this mobile node, then this node** MUST reject the Binding Update and **SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 133 (not home agent for this mobile node).**

Identifier: RQ_001_1528
RFC Clause: 10.3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the home agent accepts the Primary Care-of Address De-Registration Binding Update, then it MUST delete any existing entry in its Binding Cache for this mobile node.

RFC Text:
If the home agent does not reject the Binding Update as described above, then it MUST delete any existing entry in its Binding Cache for this mobile node. Then, the home agent MUST return a Binding Acknowledgement to the mobile node, constructed as follows:

o The Status field MUST be set to a value 0, indicating success.

o The Key Management Mobility Capability (K) bit is set or cleared and actions based on its value are performed as described in the previous section. The mobile node's home address is used as its new care-of address for the purposes of moving the key management connection to a new endpoint.

o The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

o The Lifetime field MUST be set to zero.

o The Binding Refresh Advice mobility option MUST be omitted.

Identifier: RQ_001_1529
RFC Clause: 10.3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
On acceptance of the Primary Care-of Address De-Registration Binding Update, the home agent MUST return a Binding Acknowledgement to the mobile node.

RFC Text:
If the home agent does not reject the Binding Update as described above, then it MUST delete any existing entry in its Binding Cache for this mobile node. Then, the home agent MUST return a Binding Acknowledgement to the mobile node, constructed as follows:

- The Status field MUST be set to a value 0, indicating success.
- The Key Management Mobility Capability (K) bit is set or cleared and actions based on its value are performed as described in the previous section. The mobile node's home address is used as its new care-of address for the purposes of moving the key management connection to a new endpoint.
- The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.
- The Lifetime field MUST be set to zero.
- The Binding Refresh Advice mobility option MUST be omitted.

Identifier: RQ_001_1530
RFC Clause: 10.3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Binding Acknowledgement sent by the the home agent in response to a Primary Care-of Address De-Registration Binding Update, the Status field MUST be set to a value 0, indicating success.

RFC Text:
If the home agent does not reject the Binding Update as described above, then it MUST delete any existing entry in its Binding Cache for this mobile node. Then, the home agent MUST return a Binding Acknowledgement to the mobile node, constructed as follows:

- **The Status field MUST be set to a value 0, indicating success.**
- The Key Management Mobility Capability (K) bit is set or cleared and actions based on its value are performed as described in the previous section. The mobile node's home address is used as its new care-of address for the purposes of moving the key management connection to a new endpoint.
- The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.
- The Lifetime field MUST be set to zero.
- The Binding Refresh Advice mobility option MUST be omitted.

Identifier: RQ_001_1531
RFC Clause: 10.3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Binding Acknowledgement sent by the the home agent in response to a Primary Care-of Address De-Registration Binding Update, the Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.

RFC Text:
If the home agent does not reject the Binding Update as described above, then it MUST delete any existing entry in its Binding Cache for this mobile node. Then, the home agent MUST return a Binding Acknowledgement to the mobile node, constructed as follows:

- The Status field MUST be set to a value 0, indicating success.
- The Key Management Mobility Capability (K) bit is set or cleared and actions based on its value are performed as described in the previous section. The mobile node's home address is used as its new care-of address for the purposes of moving the key management connection to a new endpoint.
- **The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update**.
- The Lifetime field MUST be set to zero.
- The Binding Refresh Advice mobility option MUST be omitted.

Identifier: RQ_001_1532
RFC Clause: 10.3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Binding Acknowledgement sent by the the home agent in response to a Primary Care-of Address De-Registration Binding Update, the Lifetime field MUST be set to zero.

RFC Text:
If the home agent does not reject the Binding Update as described above, then it MUST delete any existing entry in its Binding Cache for this mobile node. Then, the home agent MUST return a Binding Acknowledgement to the mobile node, constructed as follows:

- The Status field MUST be set to a value 0, indicating success.
- The Key Management Mobility Capability (K) bit is set or cleared and actions based on its value are performed as described in the previous section. The mobile node's home address is used as its new care-of address for the purposes of moving the key management connection to a new endpoint.
- The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.
- **The Lifetime field MUST be set to zer**o.
- The Binding Refresh Advice mobility option MUST be omitted.

Identifier: RQ_001_1533
RFC Clause: 10.3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
In the Binding Acknowledgement sent by the the home agent in response to a Primary Care-of Address De-Registration Binding Update, the Binding Refresh Advice mobility option MUST be omitted.

RFC Text:
If the home agent does not reject the Binding Update as described above, then it MUST delete any existing entry in its Binding Cache for this mobile node. Then, the home agent MUST return a Binding Acknowledgement to the mobile node, constructed as follows:

- The Status field MUST be set to a value 0, indicating success.
- The Key Management Mobility Capability (K) bit is set or cleared and actions based on its value are performed as described in the previous section. The mobile node's home address is used as its new care-of address for the purposes of moving the key management connection to a new endpoint.
- The Sequence Number field MUST be copied from the Sequence Number given in the Binding Update.
- The Lifetime field MUST be set to zero.
- **The Binding Refresh Advice mobility option MUST be omitte**d.

Identifier: RQ_001_1534
RFC Clause: 10.3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
On acceptance of the Primary Care-of Address De-Registration Binding Update, the home agent MUST stop intercepting packets on the mobile node's home link that are addressed to the mobile node (Section 10.4.1).

RFC Text:
In addition, the home agent MUST stop intercepting packets on the mobile node's home link that are addressed to the mobile node (Section 10.4.1).

Identifier: RQ_001_1535
RFC Clause: 10.3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
When the Status field in the Binding Acknowledgement is greater than or equal to 128 and the Source Address of the Binding Update is on the home link, the home agent MUST send it to the mobile node's link layer address (retrieved either from the Binding Update or through Neighbor Solicitation).

RFC Text:
The rules for selecting the Destination IP address (and, if required, routing header construction) for the Binding Acknowledgement to the mobile node are the same as in the previous section. **When the Status field in the Binding Acknowledgement is greater than or equal to 128 and the Source Address of the Binding Update is on the home link, the home agent MUST send it to the mobile node's link layer address (retrieved either from the Binding Update or through Neighbor Solicitation).**

Identifier: RQ_001_1536
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent for mobile node MUST attempt to intercept packets on the mobile node's home link that are addressed to the mobile node.

RFC Text:
While a node is serving as the home agent for mobile node it MUST attempt to intercept packets on the mobile node's home link that are addressed to the mobile node.

Identifier: RQ_001_1537
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When a node begins serving as the home agent it MUST multicast onto the home link a Neighbor Advertisement message on behalf of the mobile node.

RFC Text:
In order to do this, when a node begins serving as the home agent it MUST multicast onto the home link a Neighbor Advertisement message [12] on behalf of the mobile node. For the home address specified in the Binding Update, the home agent sends a Neighbor Advertisement message [12] to the all-nodes multicast address on the home link to advertise the home agent's own link-layer address for this IP address on behalf of the mobile node. If the Link-Layer Address Compatibility (L) flag has been specified in the Binding Update, the home agent MUST do the same for the link-local address of the mobile node.

Identifier: RQ_001_1538
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the Link-Layer Address Compatibility (L) flag has been specified in the Binding Update, the home agent MUST multicast a Neighbor Advertisement message, to the all-nodes multicast address on the home link to advertise the link-local address of the mobile node.

RFC Text:
In order to do this, when a node begins serving as the home agent it MUST multicast onto the home link a Neighbor Advertisement message [12] on behalf of the mobile node. For the home address specified in the Binding Update, the home agent sends a Neighbor Advertisement message [12] to the all-nodes multicast address on the home link to advertise the home agent's own link-layer address for this IP address on behalf of the mobile node. **If the Link-Layer Address Compatibility (L) flag has been specified in the Binding Update, the home agent MUST do the same for the link-local address of the mobile node.**

Identifier: RQ_001_1539
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.

RFC Text:
All fields in each Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node if it was sending this Neighbor Advertisement [12] while at home, with the following exceptions:

- **The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.**
- The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.
- The Router (R) bit in the Advertisement MUST be set to zero.
- The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation.
- The Override Flag (O) in the Advertisement MUST be set, indicating that the Advertisement SHOULD override any existing Neighbor Cache entry at any node receiving it.
- The Source Address in the IPv6 header MUST be set to the home agent's IP address on the interface used to send the advertisement.

Identifier: RQ_001_1540
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.

RFC Text:
All fields in each Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node if it was sending this Neighbor Advertisement [12] while at home, with the following exceptions:

- The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.
- **The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.**
- The Router (R) bit in the Advertisement MUST be set to zero.
- The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation.
- The Override Flag (O) in the Advertisement MUST be set, indicating that the Advertisement SHOULD override any existing Neighbor Cache entry at any node receiving it.
- The Source Address in the IPv6 header MUST be set to the home agent's IP address on the interface used to send the advertisement.

Identifier: RQ_001_1541
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Router (R) bit in the Advertisement MUST be set to zero.

RFC Text:
All fields in each Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node if it was sending this Neighbor Advertisement [12] while at home, with the following exceptions:

- o The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.
- o The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.
- o **The Router (R) bit in the Advertisement MUST be set to zero**.
- o The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation.
- o The Override Flag (O) in the Advertisement MUST be set, indicating that the Advertisement SHOULD override any existing Neighbor Cache entry at any node receiving it.
- o The Source Address in the IPv6 header MUST be set to the home agent's IP address on the interface used to send the advertisement.

Identifier: RQ_001_1542
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Solicited Flag (S) in the Advertisement MUST NOT be set.

RFC Text:
All fields in each Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node if it was sending this Neighbor Advertisement [12] while at home, with the following exceptions:

- o The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.
- o The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.
- o The Router (R) bit in the Advertisement MUST be set to zero.
- **o The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation.**
- o The Override Flag (O) in the Advertisement MUST be set, indicating that the Advertisement SHOULD override any existing Neighbor Cache entry at any node receiving it.
- o The Source Address in the IPv6 header MUST be set to the home agent's IP address on the interface used to send the advertisement.

Identifier: RQ_001_1543
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Override Flag (O) in the Advertisement MUST be set.

RFC Text:
All fields in each Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node if it was sending this Neighbor Advertisement [12] while at home, with the following exceptions:

- o The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.
- o The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.
- o The Router (R) bit in the Advertisement MUST be set to zero.
- o The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation.
- **o The Override Flag (O) in the Advertisement MUST be set, indicating that the Advertisement SHOULD override any existing Neighbor Cache entry at any node receiving it.**
- o The Source Address in the IPv6 header MUST be set to the home agent's IP address on the interface used to send the advertisement.

Identifier: RQ_001_1544
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The Source Address in the IPv6 header MUST be set to the home agent's IP address on the interface used to send the advertisement.

RFC Text:
All fields in each Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node if it was sending this Neighbor Advertisement [12] while at home, with the following exceptions:

- o The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.
- o The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.
- o The Router (R) bit in the Advertisement MUST be set to zero.
- o The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation.
- o The Override Flag (O) in the Advertisement MUST be set, indicating that the Advertisement SHOULD override any existing Neighbor Cache entry at any node receiving it.
- **o The Source Address in the IPv6 header MUST be set to the home agent's IP address on the interface used to send the advertisement.**

Identifier: RQ_001_1545
RFC Clause: 10.4.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
Other fields in the Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node if it was sending this Neighbor Advertisement [12] while at home.

RFC Text:
All fields in each Neighbor Advertisement message SHOULD be set in the same way they would be set by the mobile node if it was sending this Neighbor Advertisement [12] while at home, with the following exceptions:

- The Target Address in the Neighbor Advertisement MUST be set to the specific IP address for the mobile node.
- The Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address.
- The Router (R) bit in the Advertisement MUST be set to zero.
- The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation.
- The Override Flag (O) in the Advertisement MUST be set, indicating that the Advertisement SHOULD override any existing Neighbor Cache entry at any node receiving it.
- The Source Address in the IPv6 header MUST be set to the home agent's IP address on the interface used to send the advertisement.

Identifier: RQ_001_1546
RFC Clause: 10.4.1
Type: Optional
Applies to: Home_Agent

Requirement:
The home agent MAY retransmit this Neighbor Advertisement message up to MAX_NEIGHBOR_ADVERTISEMENT times to increase its reliability

RFC Text:
Any node on the home link that receives one of the Neighbor Advertisement messages (described above) will update its Neighbor Cache to associate the mobile node's address with the home agent's link layer address, causing it to transmit any future packets normally destined to the mobile node to the mobile node's home agent. Since multicasting on the local link (such as Ethernet) is typically not guaranteed to be reliable, **the home agent MAY retransmit this Neighbor Advertisement message up to MAX_NEIGHBOR_ADVERTISEMENT (see [12]) times to increase its reliability.** It is still possible that some nodes on the home link will not receive any of the Neighbor Advertisements, but these nodes will eventually be able to detect the link-layer address change for the mobile node's address through use of Neighbor Unreachability Detection [12].

Identifier: RQ_001_1547
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When a node is serving as a Home Agent for a Mobile Node, it MUST act as a proxy for this Mobile Node and reply to any received Neighbor Solicitations for it.

RFC Text:
While a node is serving as a home agent for some mobile node, the home agent uses IPv6 Neighbor Discovery [12] to intercept unicast packets on the home link addressed to the mobile node. **In order to intercept packets in this way, the home agent MUST act as a proxy for this mobile node and reply to any received Neighbor Solicitations for it.** When a home agent receives a Neighbor Solicitation, it MUST check if the Target Address specified in the message matches the address of any mobile node for which it has a Binding Cache entry marked as a home registration.

Identifier: RQ_001_1548
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When a home agent receives a Neighbor Solicitation, it MUST check if the Target Address specified in the message matches the address of any mobile node for which it has a Binding Cache entry marked as a home registration and if a match is recognised, the home agent MUST act as a proxy for this mobile node and reply to any received Neighbor Solicitations for it.

RFC Text:
While a node is serving as a home agent for some mobile node, the home agent uses IPv6 Neighbor Discovery [12] to intercept unicast packets on the home link addressed to the mobile node. In order to intercept packets in this way, the home agent MUST act as a proxy for this mobile node and reply to any received Neighbor Solicitations for it. **When a home agent receives a Neighbor Solicitation, it MUST check if the Target Address specified in the message matches the address of any mobile node for which it has a Binding Cache entry marked as a home registration.**

Identifier: RQ_001_1549
RFC Clause: 10.4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
When receiving a Neighbor Solicitation aimed at a Mobile Node it is serving, the Home Agent MUST reply with a Neighbor Advertisement giving its own link-layer address as the link-layer address for the specified Target Address. In addition, the Router (R) bit in the Advertisement MUST be set to zero.

RFC Text:
If such an entry exists in the home agent's Binding Cache, the home agent MUST reply to the Neighbor Solicitation with a Neighbor Advertisement giving the home agent's own link-layer address as the link-layer address for the specified Target Address. In addition, the Router (R) bit in the Advertisement MUST be set to zero. Acting as a proxy in this way allows other nodes on the mobile node's home link to resolve the mobile node's address and for the home agent to defend these addresses on the home link for Duplicate Address Detection [12].

Identifier: RQ_001_1550
RFC Clause: 10.4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
While the mobile node is away from home, the home agent SHALL intercept any packets on the home link addressed to the mobile node's home address, as described in Section 10.4.1.

RFC Text:
While the mobile node is away from home, the home agent intercepts any packets on the home link addressed to the mobile node's home address, as described in Section 10.4.1. In order to forward each intercepted packet to the mobile node, the home agent MUST tunnel the packet to the mobile node using IPv6 encapsulation [15]. When a home agent encapsulates an intercepted packet for forwarding to the mobile node, the home agent sets the Source Address in the new tunnel IP header to the home agent's own IP address and sets the Destination Address in the tunnel IP header to the mobile node's primary care-of address. When received by the mobile node, normal processing of the tunnel header [15] will result in decapsulation and processing of the original packet by the mobile node.

Identifier: RQ_001_1551
RFC Clause: 10.4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST tunnel the intercepted packet to the mobile node using IPv6 encapsulation, with the Source Address in the new tunnel IP header set to the home agent's own IP address and the Destination Address in the tunnel IP header set to the mobile node's primary care-of address.

RFC Text:
While the mobile node is away from home, the home agent intercepts any packets on the home link addressed to the mobile node's home address, as described in Section 10.4.1. In order to forward each intercepted packet to the mobile node, the home agent MUST tunnel the packet to the mobile node using IPv6 encapsulation [15]. When a home agent encapsulates an intercepted packet for forwarding to the mobile node, the home agent sets the Source Address in the new tunnel IP header to the home agent's own IP address and sets the Destination Address in the tunnel IP header to the mobile node's primary care-of address. When received by the mobile node, normal processing of the tunnel header [15] will result in decapsulation and processing of the original packet by the mobile node.

Identifier: RQ_001_1552
RFC Clause: 10.4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
Packets addressed to the mobile node's link-local address MUST NOT be tunneled to the mobile node and MUST be discarded

RFC Text:
However, packets addressed to the mobile node's link-local address MUST NOT be tunneled to the mobile node. Instead, these packets MUST be discarded and the home agent SHOULD return an ICMP Destination Unreachable, Code 3, message to the packet's Source Address (unless this Source Address is a multicast address). Packets addressed to the mobile node's site-local address SHOULD NOT be tunneled to the mobile node by default.

Identifier: RQ_001_1553
RFC Clause: 10.4.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
On receipt of Packets addressed to the mobile node's link-local address the home agent SHOULD return an ICMP Destination Unreachable, Code 3, message to the packet's Source Address (unless this Source Address is a multicast address).

RFC Text:
However, packets addressed to the mobile node's link-local address MUST NOT be tunneled to the mobile node. Instead, these packets MUST be discarded and the home agent SHOULD return an ICMP Destination Unreachable, Code 3, message to the packet's Source Address (unless this Source Address is a multicast address). Packets addressed to the mobile node's site-local address SHOULD NOT be tunneled to the mobile node by default.

Identifier: RQ_001_1554
RFC Clause: 10.4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
Packets addressed to the mobile node's site-local address SHOULD NOT be tunneled to the mobile node by default.

RFC Text:
However, packets addressed to the mobile node's link-local address MUST NOT be tunneled to the mobile node. Instead, these packets MUST be discarded and the home agent SHOULD return an ICMP Destination Unreachable, Code 3, message to the packet's Source Address (unless this Source Address is a multicast address). **Packets addressed to the mobile node's site-local address SHOULD NOT be tunneled to the mobile node by default.**

Identifier: RQ_001_1555
RFC Clause: 10.4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
Multicast packets addressed to a multicast address with link-local scope to which the mobile node is subscribed, MUST NOT be tunneled to the mobile node.

RFC Text:
Interception and tunneling of the following multicast addressed packets on the home network are only done if the home agent supports multicast group membership control messages from the mobile node as described in the next section. Tunneling of multicast packets to a mobile node follows similar limitations to those defined above for unicast packets addressed to the mobile node's link-local and site- local addresses. Multicast packets addressed to a multicast address with link-local scope [3], to which the mobile node is subscribed, MUST NOT be tunneled to the mobile node. These packets SHOULD be silently discarded (after delivering to other local multicast recipients). Multicast packets addressed to a multicast address with a scope larger than link-local, but smaller than global (e.g., site- local and organization-local [3], to which the mobile node is subscribed, SHOULD NOT be tunneled to the mobile node. Multicast packets addressed with a global scope, to which the mobile node has successfully subscribed, MUST be tunneled to the mobile node.

Identifier: RQ_001_1556
RFC Clause: 10.4.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
Multicast packets addressed to a multicast address with link-local scope or a scope larger than link-local, but smaller than global (e.g., site- local and organization-local, to which the mobile node is subscribed,SHOULD be silently discarded (after delivering to other local multicast recipients).

RFC Text:
Interception and tunneling of the following multicast addressed packets on the home network are only done if the home agent supports multicast group membership control messages from the mobile node as described in the next section. **Tunneling of multicast packets to a mobile node follows similar limitations to those defined above for unicast packets addressed to the mobile node's link-local and site- local addresses. Multicast packets addressed to a multicast address with link-local scope [3], to which the mobile node is subscribed**, MUST NOT be tunneled to the mobile node. **These packets SHOULD be silently discarded (after delivering to other local multicast recipients).** Multicast packets addressed to a multicast address with a scope larger than link-local, but smaller than global (e.g., site- local and organization-local [3], to which the mobile node is subscribed, SHOULD NOT be tunneled to the mobile node. Multicast packets addressed with a global scope, to which the mobile node has successfully subscribed, MUST be tunneled to the mobile node.

Identifier: RQ_001_1557
RFC Clause: 10.4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
Multicast packets addressed with a global scope, to which the mobile node has subscribed, MUST be tunneled to the mobile node.

RFC Text:
Interception and tunneling of the following multicast addressed packets on the home network are only done if the home agent supports multicast group membership control messages from the mobile node as described in the next section. Tunneling of multicast packets to a mobile node follows similar limitations to those defined above for unicast packets addressed to the mobile node's link-local and site- local addresses. Multicast packets addressed to a multicast address with link-local scope [3], to which the mobile node is subscribed, MUST NOT be tunneled to the mobile node. These packets SHOULD be silently discarded (after delivering to other local multicast recipients). Multicast packets addressed to a multicast address with a scope larger than link-local, but smaller than global (e.g., site- local and organization-local [3], to which the mobile node is subscribed, SHOULD NOT be tunneled to the mobile node. **Multicast packets addressed with a global scope, to which the mobile node has successfully subscribed, MUST be tunneled to the mobile node.**

Identifier: RQ_001_1558
RFC Clause: 10.4.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
Multicast packets addressed to a multicast address with a scope larger than link-local, but smaller than global (e.g., site- local and organization-local, to which the mobile node is subscribed, SHOULD NOT be tunneled to the mobile node.

RFC Text:
Interception and tunneling of the following multicast addressed packets on the home network are only done if the home agent supports multicast group membership control messages from the mobile node as described in the next section. Tunneling of multicast packets to a mobile node follows similar limitations to those defined above for unicast packets addressed to the mobile node's link-local and site- local addresses. Multicast packets addressed to a multicast address with link-local scope [3], to which the mobile node is subscribed, MUST NOT be tunneled to the mobile node. These packets SHOULD be silently discarded (after delivering to other local multicast recipients). **Multicast packets addressed to a multicast address with a scope larger than link-local, but smaller than global (e.g., site- local and organization-local [3], to which the mobile node is subscribed, SHOULD NOT be tunneled to the mobile node.** Multicast packets addressed with a global scope, to which the mobile node has successfully subscribed, MUST be tunneled to the mobile node.

Identifier: RQ_001_1559
RFC Clause: 10.4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
Before tunneling a packet to the mobile node, the home agent MUST perform any IPsec processing as indicated by the security policy data base.

RFC Text:
Before tunneling a packet to the mobile node, the home agent MUST perform any IPsec processing as indicated by the security policy data base.

Identifier: RQ_001_1560
RFC Clause: 10.4.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
If multicast data packet forwarding support is not provided, multicast group membership control messages are silently ignored.

RFC Text:
This section is a prerequisite for the multicast data packet forwarding, described in the previous section. If this support is not provided, multicast group membership control messages are silently ignored.

Identifier: RQ_001_1561
RFC Clause: 10.4.3
Type: Recommendation
Applies to: Home_Agent

Requirement:
the home agent SHOULD be capable of receiving tunneled multicast group membership control information from the mobile node in order to determine which groups the mobile node has subscribed to.

RFC Text:
In order to forward multicast data packets from the home network to all the proper mobile nodes, the home agent SHOULD be capable of receiving tunneled multicast group membership control information from the mobile node in order to determine which groups the mobile node has subscribed to. These multicast group membership messages are Listener Report messages specified in MLD [17] or in other protocols such as [37].

Identifier: RQ_001_1562
RFC Clause: 10.4.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
To obtain the mobile node's current multicast group membership the home agent must periodically transmit MLD Query messages through the tunnel to the mobile node.

RFC Text:
To obtain the mobile node's current multicast group membership the home agent must periodically transmit MLD Query messages through the tunnel to the mobile node. These MLD periodic transmissions will ensure the home agent has an accurate record of the groups in which the mobile node is interested despite packet losses of the mobile node's MLD group membership messages.

Identifier: RQ_001_1563
RFC Clause: 10.4.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
To avoid ambiguity on the home agent, due to mobile nodes which may choose identical link-local source addresses for their MLD function, it is necessary for the home agent to identify which mobile node was actually the issuer of a particular MLD message.

RFC Text:
Note that at this time, even though a link-local source is used on MLD packets, no functionality depends on these addresses being unique, nor do they elicit direct responses. All MLD messages are sent to multicast destinations. **To avoid ambiguity on the home agent, due to mobile nodes which may choose identical link-local source addresses for their MLD function, it is necessary for the home agent to identify which mobile node was actually the issuer of a particular MLD message.** This may be accomplished by noting which tunnel such an MLD arrived by, which IPsec SA was used, or by other distinguishing means.

Identifier: RQ_001_1564
RFC Clause: 10.4.3
Type: Optional
Applies to: Home_Agent

Requirement:
the home agent MAY identify which mobile node was actually the issuer of a particular MLD message by noting which tunnel such an MLD arrived by, which IPsec SA was used, or by other distinguishing means.

RFC Text:
Note that at this time, even though a link-local source is used on MLD packets, no functionality depends on these addresses being unique, nor do they elicit direct responses. All MLD messages are sent to multicast destinations. To avoid ambiguity on the home agent, due to mobile nodes which may choose identical link-local source addresses for their MLD function, it is necessary for the home agent to identify which mobile node was actually the issuer of a particular MLD message. **This may be accomplished by noting which tunnel such an MLD arrived by, which IPsec SA was used, or by other distinguishing means.**

Identifier: RQ_001_1565
RFC Clause: 10.4.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
If stateful address autoconfiguration mechanisms support is not provided, then the M and O bits must remain cleared on the Mobile Prefix Advertisement Messages.

RFC Text:
This section describes how home agents support the use of stateful address autoconfiguration mechanisms such as DHCPv6 [29] from the mobile nodes. If this support is not provided, then the M and O bits must remain cleared on the Mobile Prefix Advertisement Messages. Any mobile node which sends DHCPv6 messages to the home agent without this support will not receive a response.

Identifier: RQ_001_1566
RFC Clause: 10.4.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
The arriving tunnel or IPsec SA of DHCPv6 link-scope messages from the mobile node must be noted by the home agent so that DHCPv6 responses may be sent back to the appropriate mobile node.

RFC Text:
If DHCPv6 is used, packets are sent with link-local source addresses either to a link-scope multicast address or a link-local address. Mobile nodes desiring to locate a DHCPv6 service may reverse tunnel standard DHCPv6 packets to the home agent. Since these link-scope packets cannot be forwarded onto the home network, it is necessary for the home agent to either implement a DHCPv6 relay agent or a DHCPv6 server function itself. **The arriving tunnel or IPsec SA of DHCPv6 link-scope messages from the mobile node must be noted so that DHCPv6 responses may be sent back to the appropriate mobile node.** DHCPv6 messages sent to the mobile node with a link-local destination must be tunneled within the same tunnel header used for other packet flows.

Identifier: RQ_001_1567
RFC Clause: 10.4.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
DHCPv6 messages sent to the mobile node with a link-local destination must be tunneled within the same tunnel header used for other packet flows

RFC Text:
If DHCPv6 is used, packets are sent with link-local source addresses either to a link-scope multicast address or a link-local address. Mobile nodes desiring to locate a DHCPv6 service may reverse tunnel standard DHCPv6 packets to the home agent. Since these link-scope packets cannot be forwarded onto the home network, it is necessary for the home agent to either implement a DHCPv6 relay agent or a DHCPv6 server function itself. The arriving tunnel or IPsec SA of DHCPv6 link-scope messages from the mobile node must be noted so that DHCPv6 responses may be sent back to the appropriate mobile node. **DHCPv6 messages sent to the mobile node with a link-local destination must be tunneled within the same tunnel header used for other packet flows**.

Identifier: RQ_001_1568
RFC Clause: 10.4.5
Type: Mandatory
Applies to: Home_Agent

Requirement:
Home agents MUST support reverse tunneling.

RFC Text:
Unless a binding has been established between the mobile node and a correspondent node, traffic from the mobile node to the correspondent node goes through a reverse tunnel. **Home agents MUST support reverse tunneling as follows:**

- **The tunneled traffic arrives to the home agent's address using IPv6 encapsulation [15].**

- Depending on the security policies used by the home agent, reverse tunneled packets MAY be discarded unless accompanied by a valid ESP header. The support for authenticated reverse tunneling allows the home agent to protect the home network and correspondent nodes from malicious nodes masquerading as a mobile node.

- Otherwise, when a home agent decapsulates a tunneled packet from the mobile node, the home agent MUST verify that the Source Address in the tunnel IP header is the mobile node's primary care-of address. Otherwise, any node in the Internet could send traffic through the home agent and escape ingress filtering limitations. This simple check forces the attacker to know the current location of the real mobile node and be able to defeat ingress filtering. This check is not necessary if the reverse-tunneled packet is protected by ESP in tunnel mode.

Identifier: RQ_001_1569
RFC Clause: 10.4.5
Type: Optional
Applies to: Home_Agent

Requirement:
Home Agent MAY discard reverse tunneled packets unless accompanied by a valid ESP header.

RFC Text:
Unless a binding has been established between the mobile node and a correspondent node, traffic from the mobile node to the correspondent node goes through a reverse tunnel. Home agents MUST support reverse tunneling as follows:

- The tunneled traffic arrives to the home agent's address using IPv6 encapsulation [15].

- **Depending on the security policies used by the home agent, reverse tunneled packets MAY be discarded unless accompanied by a valid ESP header.** The support for authenticated reverse tunneling allows the home agent to protect the home network and correspondent nodes from malicious nodes masquerading as a mobile node.

- Otherwise, when a home agent decapsulates a tunneled packet from the mobile node, the home agent MUST verify that the Source Address in the tunnel IP header is the mobile node's primary care-of address. Otherwise, any node in the Internet could send traffic through the home agent and escape ingress filtering limitations. This simple check forces the attacker to know the current location of the real mobile node and be able to defeat ingress filtering. This check is not necessary if the reverse-tunneled packet is protected by ESP in tunnel mode.

Identifier: RQ_001_1570
RFC Clause: 10.4.5
Type: Mandatory
Applies to: Home_Agent

Requirement:
Unless the reverse-tunneled packet is protected by ESP in tunnel mode, the home agent MUST verify that the Source Address in the tunnel IP header is the mobile node's primary care-of address.

RFC Text:
Unless a binding has been established between the mobile node and a correspondent node, traffic from the mobile node to the correspondent node goes through a reverse tunnel. Home agents MUST support reverse tunneling as follows:

o The tunneled traffic arrives to the home agent's address using IPv6 encapsulation [15].

o Depending on the security policies used by the home agent, reverse tunneled packets MAY be discarded unless accompanied by a valid ESP header. The support for authenticated reverse tunneling allows the home agent to protect the home network and correspondent nodes from malicious nodes masquerading as a mobile node.

o Otherwise, when a home agent decapsulates a tunneled packet from the mobile node, the home agent MUST verify that the Source Address in the tunnel IP header is the mobile node's primary care-of address. Otherwise, any node in the Internet could send traffic through the home agent and escape ingress filtering limitations. This simple check forces the attacker to know the current location of the real mobile node and be able to defeat ingress filtering. **This check is not necessary if the reverse-tunneled packet is protected by ESP in tunnel mode.**

Identifier: RQ_001_1571
RFC Clause: 10.4.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST support tunnel mode IPsec ESP for the protection of packets belonging to the return routability procedure.

RFC Text:
The return routability procedure, described in Section 5.2.5, assumes that the confidentiality of the Home Test Init and Home Test messages is protected as they are tunneled between the home agent and the mobile node. Therefore, **the home agent MUST support tunnel mode IPsec ESP for the protection of packets belonging to the return routability procedure.** Support for a non-null encryption transform and authentication algorithm MUST be available. It is not necessary to distinguish between different kinds of packets during the return routability procedure.

Identifier: RQ_001_1572
RFC Clause: 10.4.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST provide support for a non-null encryption transform and authentication algorithm.

RFC Text:
The return routability procedure, described in Section 5.2.5, assumes that the confidentiality of the Home Test Init and Home Test messages is protected as they are tunneled between the home agent and the mobile node. Therefore, the home agent MUST support tunnel mode IPsec ESP for the protection of packets belonging to the return routability procedure. **Support for a non-null encryption transform and authentication algorithm MUST be available.** It is not necessary to distinguish between different kinds of packets during the return routability procedure.

Identifier: RQ_001_1573
RFC Clause: 10.4.6
Type: Mandatory
Applies to: Home_Agent

Requirement:
When the care-of address for the mobile node changes as a result of an accepted Binding Update, special treatment is needed for the next packets sent using these security associations. The home agent MUST set the new care-of address as the destination address of these packets, as if the outer header destination address in the security association had changed .

RFC Text:
Security associations are needed to provide this protection. **When the care-of address for the mobile node changes as a result of an accepted Binding Update, special treatment is needed for the next packets sent using these security associations. The home agent MUST set the new care-of address as the destination address of these packets, as if the outer header destination address in the security association had changed** [21].

Identifier: RQ_001_1574
RFC Clause: 10.4.6
Type: Recommendation
Applies to: Home_Agent

Requirement:
The Return Routability Packets protection SHOULD be used with all mobile nodes.

RFC Text:
The above protection SHOULD be used with all mobile nodes. The use is controlled by configuration of the IPsec security policy database both at the mobile node and at the home agent.

Identifier: RQ_001_1575
RFC Clause: 10.4.6
Type: Mandatory
Applies to: Home_Agent

Requirement:

When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent.

RFC Text:

As described earlier, the Binding Update and Binding Acknowledgement messages require protection between the home agent and the mobile node. The Mobility Header protocol carries both these messages as well as the return routability messages. From the point of view of the security policy database these messages are indistinguishable. **When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent.** This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters the tunnel. This makes use of per-interface security policy database entries [4] specific to the tunnel interface (the node's attachment to the tunnel [11]).

Identifier: RQ_001_1576
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists).

RFC Text:
On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- **If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists).** Skip all the following steps.

- Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].

- Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; otherwise, the default preference of 0 MUST be used.

- Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.

- If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.

- Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.

- If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.

- If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

Identifier: RQ_001_1577
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is set, extract the Source Address from the IP header of the Router Advertisement.

RFC Text:
On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- o If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists). Skip all the following steps.
- o **Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].**
- o Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; otherwise, the default preference of 0 MUST be used.
- o Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.
- o If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.
- o Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.
- o If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.
- o If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

Identifier: RQ_001_1578
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is set and if the Router Advertisement contains a Home Agent Information Option, then the home agent preference is taken from the Home Agent Preference field in the option.

RFC Text:
On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists). Skip all the following steps.
- **Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].**
- **Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option;** otherwise, the default preference of 0 MUST be used.
- Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.
- If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.
- Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.
- If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.
- If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

Identifier: RQ_001_1579
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is set and if the Router Advertisement does not contain a Home Agent Information Option, then the home agent preference of 0 MUST be used.

RFC Text:
On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists). Skip all the following steps.
- **Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].**
- Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; **otherwise, the default preference of 0 MUST be used.**
- Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.
- If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.
- Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.
- If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.
- If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

Identifier: RQ_001_1580
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is set and if the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option.

RFC Text:

On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists). Skip all the following steps.
- **Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].**
- Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; otherwise, the default preference of 0 MUST be used.
- **Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option;** otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.
- If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.
- Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.
- If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.
- If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

Identifier: RQ_001_1581
RFC Clause: 10.5.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is set and if the Router Advertisement does not contain a Home Agent Information Option, then the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.

RFC Text:
On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists). Skip all the following steps.
- **Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].**
- Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; otherwise, the default preference of 0 MUST be used.
- **Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.**
- If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.
- Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.
- If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.
- If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

Identifier: RQ_001_1582
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is set and if the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.

RFC Text:

On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists). Skip all the following steps.
- **Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].**
- Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; otherwise, the default preference of 0 MUST be used.
- Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.
- **If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.**
- Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.
- If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.
- If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

Identifier: RQ_001_1583
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is set and if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined from the Home Agent Information Option.

RFC Text:
On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- o If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists). Skip all the following steps.
- o **Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].**
- o Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; otherwise, the default preference of 0 MUST be used.
- o Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.
- o If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.
- **o Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.**
- o If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.
- o If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

Identifier: RQ_001_1584
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is set and if the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined from the Home Agent Information Option.

RFC Text:

On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- o If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists). Skip all the following steps.
- o **Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].**
- o Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; otherwise, the default preference of 0 MUST be used.
- o Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.
- o If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.
- o Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.
- **o If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.**
- o If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

Identifier: RQ_001_1585
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

On receipt of a valid Router Advertisement, the home agent performs the following, in addition to any steps already required of it by Neighbor Discovery. If the Home Agent (H) bit in the Router Advertisement is set and if the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.

RFC Text:

On receipt of a valid Router Advertisement, as defined in the processing algorithm specified for Neighbor Discovery [12], the home agent performs the following steps in addition to any steps already required of it by Neighbor Discovery:

- o If the Home Agent (H) bit in the Router Advertisement is not set, delete the sending node's entry in the current Home Agents List (if one exists). Skip all the following steps.
- o **Otherwise, extract the Source Address from the IP header of the Router Advertisement. This is the link-local IP address on this link of the home agent sending this Advertisement [12].**
- o Determine the preference for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the preference is taken from the Home Agent Preference field in the option; otherwise, the default preference of 0 MUST be used.
- o Determine the lifetime for this home agent. If the Router Advertisement contains a Home Agent Information Option, then the lifetime is taken from the Home Agent Lifetime field in the option; otherwise, the lifetime specified by the Router Lifetime field in the Router Advertisement SHOULD be used.
- o If the link-local address of the home agent sending this Advertisement is already present in this home agent's Home Agents List and the received home agent lifetime value is zero, immediately delete this entry in the Home Agents List.
- o Otherwise, if the link-local address of the home agent sending this Advertisement is already present in the receiving home agent's Home Agents List, reset its lifetime and preference to the values determined above.
- o If the link-local address of the home agent sending this Advertisement is not already present in the Home Agents List maintained by the receiving home agent, and the lifetime for the sending home agent is non-zero, create a new entry in the list, and initialize its lifetime and preference to the values determined above.
- **o If the Home Agents List entry for the link-local address of the home agent sending this Advertisement was not deleted as described above, determine any global address(es) of the home agent based on each Prefix Information option received in this Advertisement in which the Router Address (R) bit is set (Section 7.2). Add all such global addresses to the list of global addresses in this Home Agents List entry.**

Identifier: RQ_001_1586
RFC Clause: 10.5.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
A home agent SHOULD maintain an entry in its Home Agents List for each valid home agent address until that entry's lifetime expires.

RFC Text:
A home agent SHOULD maintain an entry in its Home Agents List for each valid home agent address until that entry's lifetime expires, after which time the entry MUST be deleted.

Identifier: RQ_001_1587
RFC Clause: 10.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
A home agent MUST delete a entrys in its Home Agents List for valid home agent address when that entry's lifetime expires.

RFC Text:
A home agent SHOULD maintain an entry in its Home Agents List for each valid home agent address until that entry's lifetime expires, after which time the entry MUST be deleted.

Identifier: RQ_001_1588
RFC Clause: 10.5.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
A home agent receiving a Home Agent Address Discovery Request message that serves this subnet SHOULD return an ICMP Home Agent Address Discovery Reply message to the mobile node with the Source Address of the Reply packet set to one of the global unicast addresses of the home agent.

RFC Text:
As described in Section 11.4.1, a mobile node attempts dynamic home agent address discovery by sending an ICMP Home Agent Address Discovery Request message to the Mobile IPv6 Home-Agents anycast address [16] for its home IP subnet prefix. **A home agent receiving a Home Agent Address Discovery Request message that serves this subnet SHOULD return an ICMP Home Agent Address Discovery Reply message to the mobile node with the Source Address of the Reply packet set to one of the global unicast addresses of the home agent.** The Home Agent Addresses field in the Reply message is constructed as follows:

- The Home Agent Addresses field SHOULD contain all global IP addresses for each home agent currently listed in this home agent's own Home Agents List (Section 10.1).
- The IP addresses in the Home Agent Addresses field SHOULD be listed in order of decreasing preference values, based either on the respective advertised preference from a Home Agent Information option or on the default preference of 0 if no preference is advertised (or on the configured home agent preference for this home agent itself).
- Among home agents with equal preference, their IP addresses in the Home Agent Addresses field SHOULD be listed in an order randomized with respect to other home agents with equal preference every time a Home Agent Address Discovery Reply message is returned by this home agent.
- If more than one global IP address is associated with a home agent, these addresses SHOULD be listed in a randomized order.

Johnson, et al. Standard Track [Page 101]

RFC 3775 Mobility Support in IPv6 June 2004

- The home agent SHOULD reduce the number of home agent IP addresses so that the packet fits within the minimum IPv6 MTU [11]. The home agent addresses selected for inclusion in the packet SHOULD be those from the complete list with the highest preference. This limitation avoids the danger of the Reply message packet being fragmented (or rejected by an intermediate router with an ICMP Packet Too Big message [14]).

Identifier: RQ_001_1589
RFC Clause: 10.5.1
Type: Recommendation
Applies to: Home_Agent

Requirement:

When a home agent receiving a Home Agent Address Discovery Request message that serves this subnet, returns an ICMP Home Agent Address Discovery Reply message to the mobile node. The Home Agent Addresses field in the Reply message SHOULD be constructed as follows:

o The Home Agent Addresses field SHOULD contain all global IP addresses for each home agent currently listed in this home agent's own Home Agents List (Section 10.1).

o The IP addresses in the Home Agent Addresses field SHOULD be listed in order of decreasing preference values, based either on the respective advertised preference from a Home Agent Information option or on the default preference of 0 if no preference is advertised (or on the configured home agent preference for this home agent itself).

o Among home agents with equal preference, their IP addresses in the Home Agent Addresses field SHOULD be listed in an order randomized
with respect to other home agents with equal preference every time a Home Agent Address Discovery Reply message is returned by this home agent.

o If more than one global IP address is associated with a home agent, these addresses SHOULD be listed in a randomized order.

o The home agent SHOULD reduce the number of home agent IP addresses so that the packet fits within the minimum IPv6 MTU [11]. The
home agent addresses selected for inclusion in the packet SHOULD be those from the complete list with the highest preference.

RFC Text:

As described in Section 11.4.1, a mobile node attempts dynamic home agent address discovery by sending an ICMP Home Agent Address Discovery Request message to the Mobile IPv6 Home-Agents anycast address [16] for its home IP subnet prefix. A home agent receiving a Home Agent Address Discovery Request message that serves this subnet SHOULD return an ICMP Home Agent Address Discovery Reply message to the mobile node with the Source Address of the Reply packet set to one of the global unicast addresses of the home agent. **The Home Agent Addresses field in the Reply message is constructed as follows:**

o The Home Agent Addresses field SHOULD contain all global IP addresses for each home agent currently listed in this home agent's own Home Agents List (Section 10.1).

o The IP addresses in the Home Agent Addresses field SHOULD be listed in order of decreasing preference values, based either on the respective advertised preference from a Home Agent Information option or on the default preference of 0 if no preference is advertised (or on the configured home agent preference for this home agent itself).

o Among home agents with equal preference, their IP addresses in the Home Agent Addresses field SHOULD be listed in an order randomized with respect to other home agents with equal preference every time a Home Agent Address Discovery Reply message is returned by this home agent.

o If more than one global IP address is associated with a home agent, these addresses SHOULD be listed in a randomized order.

o The home agent SHOULD reduce the number of home agent IP addresses so that the packet fits within the minimum IPv6 MTU [11]. The home agent addresses selected for inclusion in the packet SHOULD be those from the complete list with the highest preference. This limitation avoids the danger of the Reply message packet being fragmented (or rejected by an intermediate router with an ICMP Packet Too Big message [14]).

Identifier: RQ_001_1590
RFC Clause: 10.6.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
In order to ensure that the mobile nodes get the same information from different home agents, it is preferred that all of the home agents on the same link be configured in the same manner.

RFC Text:
If there are multiple home agents, differences in the advertisements sent by different home agents can lead to an inability to use a particular home address when changing to another home agent. **In order to ensure that the mobile nodes get the same information from different home agents, it is preferred that all of the home agents on the same link be configured in the same manner**.

Identifier: RQ_001_1591
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
A home agent serving a mobile node MUST schedule the delivery of the new prefix information to that mobile node when the state of the flags changes for the prefix of the mobile node's registered home address.

RFC Text:
A home agent serving a mobile node will schedule the delivery of the new prefix information to that mobile node when any of the following conditions occur:

MUST:

- **The state of the flags changes for the prefix of the mobile node's registered home address.**
- The valid or preferred lifetime is reconfigured or changes for any reason other than advancing real time.
- The mobile node requests the information with a Mobile Prefix Solicitation (see Section 11.4.2).

SHOULD:

- A new prefix is added to the home subnet interface(s) of the home agent.

MAY:

- The valid or preferred lifetime or the state of the flags changes for a prefix which is not used in any Binding Cache entry for this mobile node.

Identifier: RQ_001_1592
RFC Clause: 10.6.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
A home agent serving a mobile node SHOULD schedule the delivery of the new prefix information to that mobile node when a new prefix is added to the home subnet interface(s) of the home agent.

RFC Text:
A home agent serving a mobile node will schedule the delivery of the new prefix information to that mobile node when any of the following conditions occur:

MUST:

- The state of the flags changes for the prefix of the mobile node's registered home address.
- The valid or preferred lifetime is reconfigured or changes for any reason other than advancing real time.
- The mobile node requests the information with a Mobile Prefix Solicitation (see Section 11.4.2).

SHOULD:

- **A new prefix is added to the home subnet interface(s) of the home agent.**

MAY:

- The valid or preferred lifetime or the state of the flags changes for a prefix which is not used in any Binding Cache entry for this mobile node.

Identifier: RQ_001_1593
RFC Clause: 10.6.2
Type: Optional
Applies to: Home_Agent

Requirement:
A home agent serving a mobile node MAY schedule the delivery of the new prefix information to that mobile node when the valid or preferred lifetime or the state of the flags changes for a prefix which is not used in any Binding Cache entry for this mobile node.

RFC Text:
A home agent serving a mobile node will schedule the delivery of the new prefix information to that mobile node when any of the following conditions occur:

MUST:

- The state of the flags changes for the prefix of the mobile node's registered home address.
- The valid or preferred lifetime is reconfigured or changes for any reason other than advancing real time.
- The mobile node requests the information with a Mobile Prefix Solicitation (see Section 11.4.2).

SHOULD:

- A new prefix is added to the home subnet interface(s) of the home agent.

MAY:

- **The valid or preferred lifetime or the state of the flags changes for a prefix which is not used in any Binding Cache entry for this mobile node.**

Identifier: RQ_001_1594
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
If a mobile node sends a mobile prefix solicitation, the home agent sends prefix information to the mobile node right away.

RFC Text:
The home agent uses the following algorithm to determine when to send prefix information to the mobile node.

- **If a mobile node sends a solicitation, answer right away.**
- If no Mobile Prefix Advertisement has been sent to the mobile node in the last MaxMobPfxAdvInterval seconds (see Section 13), then ensure that a transmission is scheduled. The actual transmission time is randomized as described below.
- If a prefix matching the mobile node's home registration is added on the home subnet interface or if its information changes in any way that does not deprecate the mobile node's address, ensure that a transmission is scheduled. The actual transmission time is randomized as described below.
- If a home registration expires, cancel any scheduled advertisements to the mobile node.

Identifier: RQ_001_1595
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
If no Mobile Prefix Advertisement has been sent to the mobile node in the last MaxMobPfxAdvInterval seconds (see Section 13), then the home agent ensures that a transmission of prefix information is scheduled. The actual transmission time is randomized.

RFC Text:
The home agent uses the following algorithm to determine when to send prefix information to the mobile node.

- o If a mobile node sends a solicitation, answer right away.
- o **If no Mobile Prefix Advertisement has been sent to the mobile node in the last MaxMobPfxAdvInterval seconds (see Section 13), then ensure that a transmission is scheduled. The actual transmission time is randomized as described below.**
- o If a prefix matching the mobile node's home registration is added on the home subnet interface or if its information changes in any way that does not deprecate the mobile node's address, ensure that a transmission is scheduled. The actual transmission time is randomized as described below.
- o If a home registration expires, cancel any scheduled advertisements to the mobile node.

Identifier: RQ_001_1596
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
If a prefix matching the mobile node's home registration is added on the home subnet interface or if its information changes in any way that does not deprecate the mobile node's address, the home agent ensures that a transmission is scheduled. The actual transmission time is randomized.

RFC Text:
The home agent uses the following algorithm to determine when to send prefix information to the mobile node.

- o If a mobile node sends a solicitation, answer right away.
- o If no Mobile Prefix Advertisement has been sent to the mobile node in the last MaxMobPfxAdvInterval seconds (see Section 13), then ensure that a transmission is scheduled. The actual transmission time is randomized as described below.
- o **If a prefix matching the mobile node's home registration is added on the home subnet interface or if its information changes in any way that does not deprecate the mobile node's address, ensure that a transmission is scheduled. The actual transmission time is randomized as described below.**
- o If a home registration expires, cancel any scheduled advertisements to the mobile node.

Identifier: RQ_001_1597
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
If a home registration expires, the home agent cancels any scheduled advertisements to the mobile node.

RFC Text:
The home agent uses the following algorithm to determine when to send prefix information to the mobile node.

o If a mobile node sends a solicitation, answer right away.

o If no Mobile Prefix Advertisement has been sent to the mobile node in the last MaxMobPfxAdvInterval seconds (see Section 13), then ensure that a transmission is scheduled. The actual transmission time is randomized as described below.

o If a prefix matching the mobile node's home registration is added on the home subnet interface or if its information changes in any way that does not deprecate the mobile node's address, ensure that a transmission is scheduled. The actual transmission time is randomized as described below.

o If a home registration expires, cancel any scheduled advertisements to the mobile node.

Identifier: RQ_001_1598
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent randomises the transmission of prefix information by computing a fresh value for RAND_ADV_DELAY which offsets from the current time for the scheduled transmission.

First calculate the maximum delay for the scheduled Advertisement:
MaxScheduleDelay = min (MaxMobPfxAdvInterval, Preferred Lifetime),

where MaxMobPfxAdvInterval is as defined in Section 12. Then compute the final delay for the advertisement:
RAND_ADV_DELAY = MinMobPfxAdvInterval + (rand() % abs(MaxScheduleDelay - MinMobPfxAdvInterval))

Here rand() returns a random integer value in the range of 0 to the maximum possible integer value.

RFC Text:
Otherwise, the home agent computes a fresh value for RAND_ADV_DELAY which offsets from the current time for the scheduled transmission. First calculate the maximum delay for the scheduled Advertisement:

MaxScheduleDelay = min (MaxMobPfxAdvInterval, Preferred Lifetime),

where MaxMobPfxAdvInterval is as defined in Section 12. Then compute the final delay for the advertisement:

RAND_ADV_DELAY = MinMobPfxAdvInterval +
(rand() % abs(MaxScheduleDelay - MinMobPfxAdvInterval))

Here rand() returns a random integer value in the range of 0 to the maximum possible integer value. This computation is expected to alleviate bursts of advertisements when prefix information changes. In addition, a home agent MAY further reduce the rate of packet transmission by further delaying individual advertisements, when necessary to avoid overwhelming local network resources. The home agent SHOULD periodically continue to retransmit an unsolicited Advertisement to the mobile node, until it is acknowledged by the receipt of a Mobile Prefix Solicitation from the mobile node.

Identifier: RQ_001_1599
RFC Clause: 10.6.2
Type: Optional
Applies to: Home_Agent

Requirement:
The home agent MAY further reduce the rate of packet transmission by further delaying individual advertisements, when necessary to avoid overwhelming local network resources.

RFC Text:
Otherwise, the home agent computes a fresh value for RAND_ADV_DELAY which offsets from the current time for the scheduled transmission. First calculate the maximum delay for the scheduled Advertisement:

```
MaxScheduleDelay = min (MaxMobPfxAdvInterval, Preferred Lifetime),
```

where MaxMobPfxAdvInterval is as defined in Section 12. Then compute the final delay for the advertisement:

```
RAND_ADV_DELAY = MinMobPfxAdvInterval +
      (rand() % abs(MaxScheduleDelay - MinMobPfxAdvInterval))
```

Here rand() returns a random integer value in the range of 0 to the maximum possible integer value. This computation is expected to alleviate bursts of advertisements when prefix information changes. **In addition, a home agent MAY further reduce the rate of packet transmission by further delaying individual advertisements, when necessary to avoid overwhelming local network resources.** The home agent SHOULD periodically continue to retransmit an unsolicited Advertisement to the mobile node, until it is acknowledged by the receipt of a Mobile Prefix Solicitation from the mobile node.

Identifier: RQ_001_1600
RFC Clause: 10.6.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
When prefix information changes, the home agent SHOULD periodically continue to retransmit an unsolicited Advertisement to the mobile node, until it is acknowledged by the receipt of a Mobile Prefix Solicitation from the mobile node.

RFC Text:
Otherwise, the home agent computes a fresh value for RAND_ADV_DELAY which offsets from the current time for the scheduled transmission. First calculate the maximum delay for the scheduled Advertisement:

```
MaxScheduleDelay = min (MaxMobPfxAdvInterval, Preferred Lifetime),
```

where MaxMobPfxAdvInterval is as defined in Section 12. Then compute the final delay for the advertisement:

```
RAND_ADV_DELAY = MinMobPfxAdvInterval +
      (rand() % abs(MaxScheduleDelay - MinMobPfxAdvInterval))
```

Here rand() returns a random integer value in the range of 0 to the maximum possible integer value. This computation is expected to alleviate bursts of advertisements when prefix information changes. In addition, a home agent MAY further reduce the rate of packet transmission by further delaying individual advertisements, when necessary to avoid overwhelming local network resources. **The home agent SHOULD periodically continue to retransmit an unsolicited Advertisement to the mobile node, until it is acknowledged by the receipt of a Mobile Prefix Solicitation from the mobile node.**

Identifier: RQ_001_1601
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST wait PREFIX_ADV_TIMEOUT (see Section 12) before the first retransmission of prefix information and double the retransmission wait time for every succeeding retransmission until a maximum number of PREFIX_ADV_RETRIES attempts (see Section 12) has been tried.

RFC Text:
The home agent MUST wait PREFIX_ADV_TIMEOUT (see Section 12) before the first retransmission and double the retransmission wait time for every succeeding retransmission until a maximum number of PREFIX_ADV_RETRIES attempts (see Section 12) has been tried. If the mobile node's bindings expire before the matching Binding Update has been received, then the home agent MUST NOT attempt any more retransmissions, even if not all PREFIX_ADV_RETRIES have been retransmitted. In the meantime, if the mobile node sends another Binding Update without returning home, then the home agent SHOULD begin transmitting the unsolicited Advertisement again.

Identifier: RQ_001_1602
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
If the mobile node's bindings expire before the matching Binding Update has been received, then the home agent MUST NOT attempt any more Mobile Prefix Advertisement retransmissions, even if not all PREFIX_ADV_RETRIES have been retransmitted.

RFC Text:
The home agent MUST wait PREFIX_ADV_TIMEOUT (see Section 12) before the first retransmission and double the retransmission wait time for every succeeding retransmission until a maximum number of PREFIX_ADV_RETRIES attempts (see Section 12) has been tried. **If the mobile node's bindings expire before the matching Binding Update has been received, then the home agent MUST NOT attempt any more retransmissions, even if not all PREFIX_ADV_RETRIES have been retransmitted.** In the meantime, if the mobile node sends another Binding Update without returning home, then the home agent SHOULD begin transmitting the unsolicited Advertisement again.

Identifier: RQ_001_1603
RFC Clause: 10.6.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
If a Home Agent has stopped sending Mobile Prefix Advertisement due to expiration of the Mobile Node's bindings, and the mobile node sends a Binding Update without returning home, then the home agent SHOULD begin transmitting the unsolicited Advertisement again.

RFC Text:
The home agent MUST wait PREFIX_ADV_TIMEOUT (see Section 12) before the first retransmission and double the retransmission wait time for every succeeding retransmission until a maximum number of PREFIX_ADV_RETRIES attempts (see Section 12) has been tried. If the mobile node's bindings expire before the matching Binding Update has been received, then the home agent MUST NOT attempt any more retransmissions, even if not all PREFIX_ADV_RETRIES have been retransmitted. **In the meantime, if the mobile node sends another Binding Update without returning home, then the home agent SHOULD begin transmitting the unsolicited Advertisement again.**

Identifier: RQ_001_1604
RFC Clause: 10.6.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
If another Prefix Advertisement is sent to the mobile node, before the mobile node acknowledges a previous transmission, the home agent SHOULD combine any Prefix Information options in the unacknowledged Mobile Prefix Advertisement into a new Advertisement. The home agent then discards the old Advertisement.

RFC Text:
If some condition, as described above, occurs on the home link and causes another Prefix Advertisement to be sent to the mobile node, before the mobile node acknowledges a previous transmission, the home agent SHOULD combine any Prefix Information options in the unacknowledged Mobile Prefix Advertisement into a new Advertisement. The home agent then discards the old Advertisement.

Identifier: RQ_001_1605
RFC Clause: 10.6.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
If another Prefix Advertisement is sent to the mobile node, before the mobile node acknowledges a previous transmission, the home agent SHOULD discard the old Advertisement.

RFC Text:
If some condition, as described above, occurs on the home link and causes another Prefix Advertisement to be sent to the mobile node, before the mobile node acknowledges a previous transmission, the home agent SHOULD combine any Prefix Information options in the unacknowledged Mobile Prefix Advertisement into a new Advertisement**. The home agent then discards the old Advertisement.**

Identifier: RQ_001_1606
RFC Clause: 10.6.3
Type: Mandatory
Applies to: Home_Agent

Requirement:

When sending a Mobile Prefix Advertisement to the mobile node, the home agent MUST construct the packet as follows:

o The Source Address in the packet's IPv6 header MUST be set to the home agent's IP address to which the mobile node addressed its current home registration or its default global home agent address if no binding exists.

o If the advertisement was solicited, it MUST be destined to the source address of the solicitation. If it was triggered by prefix changes or renumbering, the advertisement's destination will be the mobile node's home address in the binding which triggered the rule.

o A type 2 routing header MUST be included with the mobile node's home address.

o IPsec headers MUST be supported

o The home agent MUST send the packet as it would any other unicast IPv6 packet that it originates.

o Set the Managed Address Configuration (M) flag if the corresponding flag has been set in any of the Router Advertisements from which the prefix information has been learned (including the ones sent by this home agent).

o Set the Other Stateful Configuration (O) flag if the corresponding flag has been set in any of the Router Advertisements from which the prefix information has been learned (including the ones sent by this home agent).

RFC Text:

When sending a Mobile Prefix Advertisement to the mobile node, the home agent MUST construct the packet as follows:

- **o The Source Address in the packet's IPv6 header MUST be set to the home agent's IP address to which the mobile node addressed its current home registration or its default global home agent address if no binding exists.**
- **o If the advertisement was solicited, it MUST be destined to the source address of the solicitation. If it was triggered by prefix changes or renumbering, the advertisement's destination will be the mobile node's home address in the binding which triggered the rule.**
- **o A type 2 routing header MUST be included with the mobile node's home address.**
- **o IPsec headers MUST be supported** and SHOULD be used.
- **o The home agent MUST send the packet as it would any other unicast IPv6 packet that it originates.**
- **o Set the Managed Address Configuration (M) flag if the corresponding flag has been set in any of the Router Advertisements from which the prefix information has been learned (including the ones sent by this home agent).**
- **o Set the Other Stateful Configuration (O) flag if the corresponding flag has been set in any of the Router Advertisements from which the prefix information has been learned (including the ones sent by this home agent).**

Identifier: RQ_001_1607
RFC Clause: 10.6.3
Type: Recommendation
Applies to: Home_Agent

Requirement:
When sending a Mobile Prefix Advertisement to the mobile node, the home agent SHOULD use IPsec headers.

RFC Text:
When sending a Mobile Prefix Advertisement to the mobile node, the home agent MUST construct the packet as follows:

- The Source Address in the packet's IPv6 header MUST be set to the home agent's IP address to which the mobile node addressed its current home registration or its default global home agent address if no binding exists.
- If the advertisement was solicited, it MUST be destined to the source address of the solicitation. If it was triggered by prefix changes or renumbering, the advertisement's destination will be the mobile node's home address in the binding which triggered the rule.
- A type 2 routing header MUST be included with the mobile node's home address.
- **IPsec header**s MUST be supported and **SHOULD be used.**
- The home agent MUST send the packet as it would any other unicast IPv6 packet that it originates.
- Set the Managed Address Configuration (M) flag if the corresponding flag has been set in any of the Router Advertisements from which the prefix information has been learned (including the ones sent by this home agent).
- Set the Other Stateful Configuration (O) flag if the corresponding flag has been set in any of the Router Advertisements from which the prefix information has been learned (including the ones sent by this home agent).

Identifier: RQ_001_1608
RFC Clause: 10.6.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
The lifetime returned by the home agent in a Binding Acknowledgement MUST not be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address.

RFC Text:
As described in Section 10.3.1, the lifetime returned by the home agent in a Binding Acknowledgement MUST not be greater than the remaining valid lifetime for the subnet prefix in the mobile node's home address. This limit on the binding lifetime serves to prohibit use of a mobile node's home address after it becomes invalid.

Identifier: RQ_001_1609
RFC Clause: 11.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Each mobile node MUST maintain a Binding Update List.

RFC Text:
Each mobile node MUST maintain a Binding Update List.

Identifier: RQ_001_1610
RFC Clause: 11.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Update List, all comparisons between Sequence Number values MUST be performed modulo 2**16.

RFC Text:
Each Binding Update List entry conceptually contains the following fields:

- The IP address of the node to which a Binding Update was sent.
- The home address for which that Binding Update was sent.
- The care-of address sent in that Binding Update. This value is necessary for the mobile node to determine if it has sent a Binding Update while giving its new care-of address to this destination after changing its care-of address.
- The initial value of the Lifetime field sent in that Binding Update.
- The remaining lifetime of that binding. This lifetime is initialized from the Lifetime value sent in the Binding Update and is decremented until it reaches zero, at which time this entry MUST be deleted from the Binding Update List.
- The maximum value of the Sequence Number field sent in previous Binding Updates to this destination. **The Sequence Number field is 16 bits long and all comparisons between Sequence Number values MUST be performed modulo 2**16** (see Section 9.5.1).
- The time at which a Binding Update was last sent to this destination, as needed to implement the rate limiting restriction for sending Binding Updates.
- The state of any retransmissions needed for this Binding Update. This state includes the time remaining until the next retransmission attempt for the Binding Update and the current state of the exponential back-off mechanism for retransmissions.
- A flag specifying whether or not future Binding Updates should be sent to this destination. The mobile node sets this flag in the Binding Update List entry when it receives an ICMP Parameter Problem, Code 1, error message in response to a return routability message or Binding Update sent to that destination, as described in Section 11.3.5.

Identifier: RQ_001_1611
RFC Clause: 11.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 mobile nodes MUST observe the rules described in Section 9.2 when processing Mobility Headers.

RFC Text:
All IPv6 mobile nodes MUST observe the rules described in Section 9.2 when processing Mobility Headers.

Identifier: RQ_001_1612
RFC Clause: 11.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address.

RFC Text:
While a mobile node is away from home, it continues to use its home address, as well as also using one or more care-of addresses. When sending a packet while away from home, a mobile node MAY choose among these in selecting the address that it will use as the source of the packet, as follows:

- Protocols layered over IP will generally treat the mobile node's home address as its IP address for most packets. **For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address.** Likewise, for packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address in this way. If a binding exists, the mobile node SHOULD send the packets directly to the correspondent node. Otherwise, if a binding does not exist, the mobile node MUST use reverse tunneling.

- The mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, not requiring the use of a Home Address option in the packet. This is particularly useful for short-term communication that may easily be retried if it fails. Using the mobile node's care-of address as the source for such queries will generally have a lower overhead than using the mobile node's home address, since no extra options need be used in either the query or its reply. Such packets can be routed normally, directly between their source and destination without relying on Mobile IPv6. If application running on the mobile node has no particular knowledge that the communication being sent fits within this general type of communication, however, the mobile node should not use its care-of address as the source of the packet in this way.

  The choice of the most efficient communications method is application specific, and outside the scope of this specification. The APIs necessary for controlling the choice are also out of scope.

- While not at its home link, the mobile node MUST NOT use the Home Address destination option when communicating with link-local or site-local peers, if the scope of the home address is larger than the scope of the peer's address.

  Similarly, the mobile node MUST NOT use the Home Address destination option for IPv6 Neighbor Discovery [12] packets.

Identifier: RQ_001_1613
RFC Clause: 11.3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
For packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address.

RFC Text:
While a mobile node is away from home, it continues to use its home address, as well as also using one or more care-of addresses. When sending a packet while away from home, a mobile node MAY choose among these in selecting the address that it will use as the source of the packet, as follows:

- Protocols layered over IP will generally treat the mobile node's home address as its IP address for most packets. For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address. Likewise, **for packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address in this way.** If a binding exists, the mobile node SHOULD send the packets directly to the correspondent node. Otherwise, if a binding does not exist, the mobile node MUST use reverse tunneling.

- The mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, not requiring the use of a Home Address option in the packet. This is particularly useful for short-term communication that may easily be retried if it fails. Using the mobile node's care-of address as the source for such queries will generally have a lower overhead than using the mobile node's home address, since no extra options need be used in either the query or its reply. Such packets can be routed normally, directly between their source and destination without relying on Mobile IPv6. If application running on the mobile node has no particular knowledge that the communication being sent fits within this general type of communication, however, the mobile node should not use its care-of address as the source of the packet in this way.

  The choice of the most efficient communications method is application specific, and outside the scope of this specification. The APIs necessary for controlling the choice are also out of scope.

- While not at its home link, the mobile node MUST NOT use the Home Address destination option when communicating with link-local or site-local peers, if the scope of the home address is larger than the scope of the peer's address.

  Similarly, the mobile node MUST NOT use the Home Address destination option for IPv6 Neighbor Discovery [12] packets.

Identifier: RQ_001_1614
RFC Clause: 11.3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If a binding exists between the Mobile Node and the Corresponding Node, the mobile node SHOULD send the packets directly to the correspondent node.

RFC Text:
While a mobile node is away from home, it continues to use its home address, as well as also using one or more care-of addresses. When sending a packet while away from home, a mobile node MAY choose among these in selecting the address that it will use as the source of the packet, as follows:

- Protocols layered over IP will generally treat the mobile node's home address as its IP address for most packets. For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address. Likewise, for packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address in this way. **If a binding exists, the mobile node SHOULD send the packets directly to the correspondent node.** Otherwise, if a binding does not exist, the mobile node MUST use reverse tunneling.

- The mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, not requiring the use of a Home Address option in the packet. This is particularly useful for short-term communication that may easily be retried if it fails. Using the mobile node's care-of address as the source for such queries will generally have a lower overhead than using the mobile node's home address, since no extra options need be used in either the query or its reply. Such packets can be routed normally, directly between their source and destination without relying on Mobile IPv6. If application running on the mobile node has no particular knowledge that the communication being sent fits within this general type of communication, however, the mobile node should not use its care-of address as the source of the packet in this way.

  The choice of the most efficient communications method is application specific, and outside the scope of this specification. The APIs necessary for controlling the choice are also out of scope.

- While not at its home link, the mobile node MUST NOT use the Home Address destination option when communicating with link-local or site-local peers, if the scope of the home address is larger than the scope of the peer's address.

  Similarly, the mobile node MUST NOT use the Home Address destination option for IPv6 Neighbor Discovery [12] packets.

Identifier: RQ_001_1615
RFC Clause: 11.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If there is no existing binding between the Mobile Node and the Correspondent Node, the Mobile Node node MUST use reverse tunneling to send packets to the correspondent node.

RFC Text:
While a mobile node is away from home, it continues to use its home address, as well as also using one or more care-of addresses. When sending a packet while away from home, a mobile node MAY choose among these in selecting the address that it will use as the source of the packet, as follows:

- Protocols layered over IP will generally treat the mobile node's home address as its IP address for most packets. For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address. Likewise, for packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address in this way. If a binding exists, the mobile node SHOULD send the packets directly to the correspondent node. **Otherwise, if a binding does not exist, the mobile node MUST use reverse tunneling.**

- The mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, not requiring the use of a Home Address option in the packet. This is particularly useful for short-term communication that may easily be retried if it fails. Using the mobile node's care-of address as the source for such queries will generally have a lower overhead than using the mobile node's home address, since no extra options need be used in either the query or its reply. Such packets can be routed normally, directly between their source and destination without relying on Mobile IPv6. If application running on the mobile node has no particular knowledge that the communication being sent fits within this general type of communication, however, the mobile node should not use its care-of address as the source of the packet in this way.

  The choice of the most efficient communications method is application specific, and outside the scope of this specification. The APIs necessary for controlling the choice are also out of scope.

- While not at its home link, the mobile node MUST NOT use the Home Address destination option when communicating with link-local or site-local peers, if the scope of the home address is larger than the scope of the peer's address.

  Similarly, the mobile node MUST NOT use the Home Address destination option for IPv6 Neighbor Discovery [12] packets.

Identifier: RQ_001_1616
RFC Clause: 11.3.1
Type: Optional
Applies to: Mobile_Node

Requirement:
The mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, not requiring the use of a Home Address option in the packet.

RFC Text:
While a mobile node is away from home, it continues to use its home address, as well as also using one or more care-of addresses. When sending a packet while away from home, a mobile node MAY choose among these in selecting the address that it will use as the source of the packet, as follows:

- Protocols layered over IP will generally treat the mobile node's home address as its IP address for most packets. For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address. Likewise, for packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address in this way. If a binding exists, the mobile node SHOULD send the packets directly to the correspondent node. Otherwise, if a binding does not exist, the mobile node MUST use reverse tunneling.

- **The mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, not requiring the use of a Home Address option in the packet.** This is particularly useful for short-term communication that may easily be retried if it fails. Using the mobile node's care-of address as the source for such queries will generally have a lower overhead than using the mobile node's home address, since no extra options need be used in either the query or its reply. Such packets can be routed normally, directly between their source and destination without relying on Mobile IPv6. If application running on the mobile node has no particular knowledge that the communication being sent fits within this general type of communication, however, the mobile node should not use its care-of address as the source of the packet in this way.

  The choice of the most efficient communications method is application specific, and outside the scope of this specification. The APIs necessary for controlling the choice are also out of scope.

- While not at its home link, the mobile node MUST NOT use the Home Address destination option when communicating with link-local or site-local peers, if the scope of the home address is larger than the scope of the peer's address.

  Similarly, the mobile node MUST NOT use the Home Address destination option for IPv6 Neighbor Discovery [12] packets.

Identifier: RQ_001_1617
RFC Clause: 11.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
While not at its home link, the mobile node MUST NOT use the Home Address destination option when communicating with link-local or site-local peers, if the scope of the home address is larger than the scope of the peer's address.

RFC Text:
While a mobile node is away from home, it continues to use its home address, as well as also using one or more care-of addresses. When sending a packet while away from home, a mobile node MAY choose among these in selecting the address that it will use as the source of the packet, as follows:

o Protocols layered over IP will generally treat the mobile node's home address as its IP address for most packets. For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address. Likewise, for packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address in this way. If a binding exists, the mobile node SHOULD send the packets directly to the correspondent node. Otherwise, if a binding does not exist, the mobile node MUST use reverse tunneling.

o The mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, not requiring the use of a Home Address option in the packet. This is particularly useful for short-term communication that may easily be retried if it fails. Using the mobile node's care-of address as the source for such queries will generally have a lower overhead than using the mobile node's home address, since no extra options need be used in either the query or its reply. Such packets can be routed normally, directly between their source and destination without relying on Mobile IPv6. If application running on the mobile node has no particular knowledge that the communication being sent fits within this general type of communication, however, the mobile node should not use its care-of address as the source of the packet in this way.

  The choice of the most efficient communications method is application specific, and outside the scope of this specification. The APIs necessary for controlling the choice are also out of scope.

o **While not at its home link, the mobile node MUST NOT use the Home Address destination option when communicating with link-local or site-local peers, if the scope of the home address is larger than the scope of the peer's address.**

  Similarly, the mobile node MUST NOT use the Home Address destination option for IPv6 Neighbor Discovery [12] packets.

Identifier: RQ_001_1618
RFC Clause: 11.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The mobile node MUST NOT use the Home Address destination option for IPv6 Neighbor Discovery packets.

RFC Text:
While a mobile node is away from home, it continues to use its home address, as well as also using one or more care-of addresses. When sending a packet while away from home, a mobile node MAY choose among these in selecting the address that it will use as the source of the packet, as follows:

- Protocols layered over IP will generally treat the mobile node's home address as its IP address for most packets. For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address. Likewise, for packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address in this way. If a binding exists, the mobile node SHOULD send the packets directly to the correspondent node. Otherwise, if a binding does not exist, the mobile node MUST use reverse tunneling.

- The mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, not requiring the use of a Home Address option in the packet. This is particularly useful for short-term communication that may easily be retried if it fails. Using the mobile node's care-of address as the source for such queries will generally have a lower overhead than using the mobile node's home address, since no extra options need be used in either the query or its reply. Such packets can be routed normally, directly between their source and destination without relying on Mobile IPv6. If application running on the mobile node has no particular knowledge that the communication being sent fits within this general type of communication, however, the mobile node should not use its care-of address as the source of the packet in this way.

  The choice of the most efficient communications method is application specific, and outside the scope of this specification. The APIs necessary for controlling the choice are also out of scope.

- While not at its home link, the mobile node MUST NOT use the Home Address destination option when communicating with link-local or site-local peers, if the scope of the home address is larger than the scope of the peer's address.

  Similarly, **the mobile node MUST NOT use the Home Address destination option for IPv6 Neighbor Discovery [12] packets**.

Identifier: RQ_001_1619
RFC Clause: 11.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
For packets sent by the mobile node while away from home using the mobile node's home address as the source, special Mobile IPv6 processing of the packet is required using Route Optimization or Reverse Tunneling.

RFC Text:
For packets sent by the mobile node sent while away from home using the mobile node's home address as the source, special Mobile IPv6 processing of the packet is required.

Identifier: RQ_001_1620
RFC Clause: 11.3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When using Route Optimization, the mobile node SHOULD examine its Binding Update List for an entry which fulfills the following conditions:

* The Source Address field of the packet being sent is equal to the home address in the entry.
* The Destination Address field of the packet being sent is equal to the address of the correspondent node in the entry.
* One of the current care-of addresses of the mobile node appears as the care-of address in the entry.
* The entry indicates that a binding has been successfully created.
* The remaining lifetime of the binding is greater than zero.

When these conditions are met, the mobile node knows that the correspondent node has a suitable Binding Cache entry.

RFC Text:
Route Optimization

This manner of delivering packets does not require going through the home network, and typically will enable faster and more reliable transmission.

The mobile node needs to ensure that a Binding Cache entry exists for its home address so that the correspondent node can process the packet (Section 9.3.1 specifies the rules for Home Address Destination Option Processing at a correspondent node). The mobile node SHOULD examine its Binding Update List for an entry which fulfills the following conditions:

*** The Source Address field of the packet being sent is equal to the home address in the entry.**

*** The Destination Address field of the packet being sent is equal to the address of the correspondent node in the entry.**

*** One of the current care-of addresses of the mobile node appears as the care-of address in the entry.**

*** The entry indicates that a binding has been successfully created.**

*** The remaining lifetime of the binding is greater than zero.**

When these conditions are met, the mobile node knows that the correspondent node has a suitable Binding Cache entry.

A mobile node SHOULD arrange to supply the home address in a Home Address option, and MUST set the IPv6 header's Source Address field to the care-of address which the mobile node has registered to be used with this correspondent node. The correspondent node will then use the address supplied in the Home Address option to serve the function traditionally done by the Source IP address in the IPv6 header. The mobile node's home address is then supplied to higher protocol layers and applications.

Specifically:

* Construct the packet using the mobile node's home address as the
  packet's Source Address, in the same way as if the mobile node
  were at home. This includes the calculation of upper layer
  checksums using the home address as the value of the source.

* Insert a Home Address option into the packet with the Home Address
  field copied from the original value of the Source Address field
  in the packet.

* Change the Source Address field in the packet's IPv6 header to one
  of the mobile node's care-of addresses. This will typically be
  the mobile node's current primary care-of address, but MUST be an
  address assigned to the interface on the link being used.

By using the care-of address as the Source Address in the IPv6 header, with the mobile node's home address instead in the Home Address option, the packet will be able to safely pass through any router implementing ingress filtering [26].

Identifier: RQ_001_1621
RFC Clause: 11.3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When using Route Optimization, A mobile node SHOULD arrange to supply the home address in a Home Address option.

RFC Text:
Route Optimization

This manner of delivering packets does not require going through the home network, and typically will enable faster and more reliable transmission.

The mobile node needs to ensure that a Binding Cache entry exists for its home address so that the correspondent node can process the packet (Section 9.3.1 specifies the rules for Home Address Destination Option Processing at a correspondent node). The mobile node SHOULD examine its Binding Update List for an entry which fulfills the following conditions:

* The Source Address field of the packet being sent is equal to the home address in the entry.

* The Destination Address field of the packet being sent is equal to the address of the correspondent node in the entry.

* One of the current care-of addresses of the mobile node appears as the care-of address in the entry.

* The entry indicates that a binding has been successfully created.

* The remaining lifetime of the binding is greater than zero.

When these conditions are met, the mobile node knows that the correspondent node has a suitable Binding Cache entry.

A mobile node SHOULD arrange to supply the home address in a Home Address option, and MUST set the IPv6 header's Source Address field to the care-of address which the mobile node has registered to be used with this correspondent node. The correspondent node will then use the address supplied in the Home Address option to serve the function traditionally done by the Source IP address in the IPv6 header. The mobile node's home address is then supplied to higher protocol layers and applications.

Specifically:

* Construct the packet using the mobile node's home address as the packet's Source Address, in the same way as if the mobile node were at home. This includes the calculation of upper layer checksums using the home address as the value of the source.

* Insert a Home Address option into the packet with the Home Address field copied from the original value of the Source Address field in the packet.

* Change the Source Address field in the packet's IPv6 header to one of the mobile node's care-of addresses. This will typically be the mobile node's current primary care-of address, but MUST be an address assigned to the interface on the link being used.

By using the care-of address as the Source Address in the IPv6 header, with the mobile node's home address instead in the Home Address option, the packet will be able to safely pass through any router implementing ingress filtering [26].

Identifier: RQ_001_1622
RFC Clause: 11.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When using Route Optimization, a mobile node , MUST set the IPv6 header's Source Address field to the care-of address which the mobile node has registered to be used with this correspondent node.

RFC Text:
Route Optimization

This manner of delivering packets does not require going through the home network, and typically will enable faster and more reliable transmission.

The mobile node needs to ensure that a Binding Cache entry exists for its home address so that the correspondent node can process the packet (Section 9.3.1 specifies the rules for Home Address Destination Option Processing at a correspondent node). The mobile node SHOULD examine its Binding Update List for an entry which fulfills the following conditions:

* The Source Address field of the packet being sent is equal to the home address in the entry.

* The Destination Address field of the packet being sent is equal to the address of the correspondent node in the entry.

* One of the current care-of addresses of the mobile node appears as the care-of address in the entry.

* The entry indicates that a binding has been successfully created.

* The remaining lifetime of the binding is greater than zero.

When these conditions are met, the mobile node knows that the correspondent node has a suitable Binding Cache entry.

A mobile node SHOULD arrange to supply the home address in a Home Address option, and **MUST set the IPv6 header's Source Address field to the care-of address which the mobile node has registered to be used with this correspondent node.** The correspondent node will then use the address supplied in the Home Address option to serve the function traditionally done by the Source IP address in the IPv6 header. The mobile node's home address is then supplied to higher protocol layers and applications.

Specifically:

* Construct the packet using the mobile node's home address as the packet's Source Address, in the same way as if the mobile node were at home. This includes the calculation of upper layer checksums using the home address as the value of the source.

* Insert a Home Address option into the packet with the Home Address field copied from the original value of the Source Address field in the packet.

* Change the Source Address field in the packet's IPv6 header to one of the mobile node's care-of addresses. This will typically be the mobile node's current primary care-of address, but MUST be an address assigned to the interface on the link being used.

By using the care-of address as the Source Address in the IPv6 header, with the mobile node's home address instead in the Home Address option, the packet will be able to safely pass through any router implementing ingress filtering [26].

Identifier: RQ_001_1623
RFC Clause: 11.3.2
Type: Optional
Applies to: Mobile_Node

Requirement:
Any specific implementation MAY use algorithms and data structures other than those suggested in RFC3375.

RFC Text:
This section sketches the interaction between outbound Mobile IPv6 processing and outbound IP Security (IPsec) processing for packets sent by a mobile node while away from home. **Any specific implementation MAY use algorithms and data structures other than those suggested here, but its processing MUST be consistent with the effect of the operation described here and with the relevant IPsec specifications.** In the steps described below, it is assumed that IPsec is being used in transport mode [4] and that the mobile node is using its home address as the source for the packet (from the point of view of higher protocol layers or applications, as described in Section 11.3.1):

- The packet is created by higher layer protocols and applications (e.g., by TCP) as if the mobile node were at home and Mobile IPv6 were not being used.

- Determine the outgoing interface for the packet. (Note that the selection between reverse tunneling and route optimization may imply different interfaces, particularly if tunnels are considered interfaces as well.)

- As part of outbound packet processing in IP, the packet is compared against the IPsec security policy database to determine what processing is required for the packet [4].

- If IPsec processing is required, the packet is either mapped to an existing Security Association (or SA bundle), or a new SA (or SA bundle) is created for the packet, according to the procedures defined for IPsec.

- Since the mobile node is away from home, the mobile is either using reverse tunneling or route optimization to reach the correspondent node.

  If reverse tunneling is used, the packet is constructed in the normal manner and then tunneled through the home agent.

  If route optimization is in use, the mobile node inserts a Home Address destination option into the packet, replacing the Source Address in the packet's IP header with the care-of address used with this correspondent node, as described in Section 11.3.1. The Destination Options header in which the Home Address destination option is inserted MUST appear in the packet after the routing header, if present, and before the IPsec (AH [5] or ESP [6]) header, so that the Home Address destination option is processed by the destination node before the IPsec header is processed.

  Finally, once the packet is fully assembled, the necessary IPsec authentication (and encryption, if required) processing is performed on the packet, initializing the Authentication Data in the IPsec header.

  RFC 2402 treatment of destination options is extended as follows. The AH authentication data MUST be calculated as if the following were true:

  * the IPv6 source address in the IPv6 header contains the mobile node's home address,

  * the Home Address field of the Home Address destination option (Section 6.3) contains the new care-of address.

- This allows, but does not require, the receiver of the packet containing a Home Address destination option to exchange the two fields of the incoming packet to reach the above situation, simplifying processing for all subsequent packet headers. However, such an exchange is not required, as long as the result of the authentication calculation remains the same.

Identifier: RQ_001_1624
RFC Clause: 11.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Any specific implementation's processing MUST be consistent with the effect of the operation described here and with the relevant IPsec specifications.

RFC Text:
This section sketches the interaction between outbound Mobile IPv6 processing and outbound IP Security (IPsec) processing for packets sent by a mobile node while away from home. **Any specific implementation MAY use algorithms and data structures other than those suggested here, but its processing MUST be consistent with the effect of the operation described here and with the relevant IPsec specifications.** In the steps described below, it is assumed that IPsec is being used in transport mode [4] and that the mobile node is using its home address as the source for the packet (from the point of view of higher protocol layers or applications, as described in Section 11.3.1):

- The packet is created by higher layer protocols and applications (e.g., by TCP) as if the mobile node were at home and Mobile IPv6 were not being used.

- Determine the outgoing interface for the packet. (Note that the selection between reverse tunneling and route optimization may imply different interfaces, particularly if tunnels are considered interfaces as well.)

- As part of outbound packet processing in IP, the packet is compared against the IPsec security policy database to determine what processing is required for the packet [4].

- If IPsec processing is required, the packet is either mapped to an existing Security Association (or SA bundle), or a new SA (or SA bundle) is created for the packet, according to the procedures defined for IPsec.

- Since the mobile node is away from home, the mobile is either using reverse tunneling or route optimization to reach the correspondent node.

  If reverse tunneling is used, the packet is constructed in the normal manner and then tunneled through the home agent.

  If route optimization is in use, the mobile node inserts a Home Address destination option into the packet, replacing the Source Address in the packet's IP header with the care-of address used with this correspondent node, as described in Section 11.3.1. The Destination Options header in which the Home Address destination option is inserted MUST appear in the packet after the routing header, if present, and before the IPsec (AH [5] or ESP [6]) header, so that the Home Address destination option is processed by the destination node before the IPsec header is processed.

  Finally, once the packet is fully assembled, the necessary IPsec authentication (and encryption, if required) processing is performed on the packet, initializing the Authentication Data in the IPsec header.

  RFC 2402 treatment of destination options is extended as follows. The AH authentication data MUST be calculated as if the following were true:

  * the IPv6 source address in the IPv6 header contains the mobile node's home address,

  * the Home Address field of the Home Address destination option (Section 6.3) contains the new care-of address.

- This allows, but does not require, the receiver of the packet containing a Home Address destination option to exchange the two fields of the incoming packet to reach the above situation, simplifying processing for all subsequent packet headers. However, such an exchange is not required, as long as the result of the authentication calculation remains the same.

Identifier: RQ_001_1625
RFC Clause: 11.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When IPsec is being used in transport mode and the mobile node is using its home address as the source for the packet and if route optimization is in use, the Destination Options header in which the Home Address destination option is inserted MUST appear in the packet after the routing header, if present.

RFC Text:
This section sketches the interaction between outbound Mobile IPv6 processing and outbound IP Security (IPsec) processing for packets sent by a mobile node while away from home. Any specific implementation MAY use algorithms and data structures other than those suggested here, but its processing MUST be consistent with the effect of the operation described here and with the relevant IPsec specifications. In the steps described below, it is assumed that **IPsec is being used in transport mode [4] and that the mobile node is using its home address as the source for the packet (from the point of view of higher protocol layers or applications, as described in Section 11.3.1):**

- The packet is created by higher layer protocols and applications (e.g., by TCP) as if the mobile node were at home and Mobile IPv6 were not being used.

- Determine the outgoing interface for the packet. (Note that the selection between reverse tunneling and route optimization may imply different interfaces, particularly if tunnels are considered interfaces as well.)

- As part of outbound packet processing in IP, the packet is compared against the IPsec security policy database to determine what processing is required for the packet [4].

- If IPsec processing is required, the packet is either mapped to an existing Security Association (or SA bundle), or a new SA (or SA bundle) is created for the packet, according to the procedures defined for IPsec.

- Since the mobile node is away from home, the mobile is either using reverse tunneling or route optimization to reach the correspondent node.

  If reverse tunneling is used, the packet is constructed in the normal manner and then tunneled through the home agent.

  If route optimization is in use, the mobile node inserts a Home Address destination option into the packet, replacing the Source Address in the packet's IP header with the care-of address used with this correspondent node, as described in Section 11.3.1. The Destination Options header in which the Home Address destination option is inserted MUST appear in the packet after the routing header, if present, and before the IPsec (AH [5] or ESP [6]) header, so that the Home Address destination option is processed by the destination node before the IPsec header is processed.

  Finally, once the packet is fully assembled, the necessary IPsec authentication (and encryption, if required) processing is performed on the packet, initializing the Authentication Data in the IPsec header.

  RFC 2402 treatment of destination options is extended as follows. The AH authentication data MUST be calculated as if the following were true:

  * the IPv6 source address in the IPv6 header contains the mobile node's home address,

  * the Home Address field of the Home Address destination option (Section 6.3) contains the new care-of address.

- This allows, but does not require, the receiver of the packet containing a Home Address destination option to exchange the two fields of the incoming packet to reach the above situation, simplifying processing for all subsequent packet headers. However, such an exchange is not required, as long as the result of the authentication calculation remains the same.

Identifier: RQ_001_1626
RFC Clause: 11.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When IPsec is being used in transport mode and the mobile node is using its home address as the source for the packet and if route optimization is in use, the Destination Options header in which the Home Address destination option is inserted MUST appear before the IPsec (AH [5] or ESP [6]) header.

RFC Text:
This section sketches the interaction between outbound Mobile IPv6 processing and outbound IP Security (IPsec) processing for packets sent by a mobile node while away from home. Any specific implementation MAY use algorithms and data structures other than those suggested here, but its processing MUST be consistent with the effect of the operation described here and with the relevant IPsec specifications. In the steps described below, it is assumed that **IPsec is being used in transport mode [4] and that the mobile node is using its home address as the source for the packet (from the point of view of higher protocol layers or applications, as described in Section 11.3.1):**

- The packet is created by higher layer protocols and applications (e.g., by TCP) as if the mobile node were at home and Mobile IPv6 were not being used.

- Determine the outgoing interface for the packet. (Note that the selection between reverse tunneling and route optimization may imply different interfaces, particularly if tunnels are considered interfaces as well.)

- As part of outbound packet processing in IP, the packet is compared against the IPsec security policy database to determine what processing is required for the packet [4].

- If IPsec processing is required, the packet is either mapped to an existing Security Association (or SA bundle), or a new SA (or SA bundle) is created for the packet, according to the procedures defined for IPsec.

- Since the mobile node is away from home, the mobile is either using reverse tunneling or route optimization to reach the correspondent node.

  If reverse tunneling is used, the packet is constructed in the normal manner and then tunneled through the home agent.

  If route optimization is in use, the mobile node inserts a Home Address destination option into the packet, replacing the Source Address in the packet's IP header with the care-of address used with this correspondent node, as described in Section 11.3.1. **The Destination Options header in which the Home Address destination option is inserted MUST appear in** the packet after the routing header, if present, and **before the IPsec (AH [5] or ESP [6]) header,** so that the Home Address destination option is processed by the destination node before the IPsec header is processed.

  Finally, once the packet is fully assembled, the necessary IPsec authentication (and encryption, if required) processing is performed on the packet, initializing the Authentication Data in the IPsec header.

  RFC 2402 treatment of destination options is extended as follows. The AH authentication data MUST be calculated as if the following were true:

  * the IPv6 source address in the IPv6 header contains the mobile node's home address,

  * the Home Address field of the Home Address destination option (Section 6.3) contains the new care-of address.

- This allows, but does not require, the receiver of the packet containing a Home Address destination option to exchange the two fields of the incoming packet to reach the above situation, simplifying processing for all subsequent packet headers. However, such an exchange is not required, as long as the result of the authentication calculation remains the same.

Identifier: RQ_001_1627
RFC Clause: 11.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

When IPsec is being used in transport mode and the mobile node is using its home address as the source for the packet The AH authentication data MUST be calculated as if the following were true:

* the IPv6 source address in the IPv6 header contains the mobile node's home address,

* the Home Address field of the Home Address destination option (Section 6.3) contains the new care-of address.

RFC Text:

This section sketches the interaction between outbound Mobile IPv6 processing and outbound IP Security (IPsec) processing for packets sent by a mobile node while away from home. Any specific implementation MAY use algorithms and data structures other than those suggested here, but its processing MUST be consistent with the effect of the operation described here and with the relevant IPsec specifications. In the steps described below, it is assumed that **IPsec is being used in transport mode [4] and that the mobile node is using its home address as the source for the packet (from the point of view of higher protocol layers or applications, as described in Section 11.3.1):**

- o The packet is created by higher layer protocols and applications (e.g., by TCP) as if the mobile node were at home and Mobile IPv6 were not being used.

- o Determine the outgoing interface for the packet. (Note that the selection between reverse tunneling and route optimization may imply different interfaces, particularly if tunnels are considered interfaces as well.)

- o As part of outbound packet processing in IP, the packet is compared against the IPsec security policy database to determine what processing is required for the packet [4].

- o If IPsec processing is required, the packet is either mapped to an existing Security Association (or SA bundle), or a new SA (or SA bundle) is created for the packet, according to the procedures defined for IPsec.

- o Since the mobile node is away from home, the mobile is either using reverse tunneling or route optimization to reach the correspondent node.

  If reverse tunneling is used, the packet is constructed in the normal manner and then tunneled through the home agent.

  If route optimization is in use, the mobile node inserts a Home Address destination option into the packet, replacing the Source Address in the packet's IP header with the care-of address used with this correspondent node, as described in Section 11.3.1. The Destination Options header in which the Home Address destination option is inserted MUST appear in the packet after the routing header, if present, and before the IPsec (AH [5] or ESP [6]) header, so that the Home Address destination option is processed by the destination node before the IPsec header is processed.

  Finally, once the packet is fully assembled, the necessary IPsec authentication (and encryption, if required) processing is performed on the packet, initializing the Authentication Data in the IPsec header.

  RFC 2402 treatment of destination options is extended as follows. **The AH authentication data MUST be calculated as if the following were true:**

  * **the IPv6 source address in the IPv6 header contains the mobile node's home address,**

  * **the Home Address field of the Home Address destination option (Section 6.3) contains the new care-of address.**

o This allows, but does not require, the receiver of the packet
  containing a Home Address destination option to exchange the two
  fields of the incoming packet to reach the above situation,
  simplifying processing for all subsequent packet headers.
  However, such an exchange is not required, as long as the result
  of the authentication calculation remains the same.

Identifier: RQ_001_1628
RFC Clause: 11.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When the mobile node is away from home, it MUST use its care-of address as the Source Address of all packets it sends as part of the key management protocol (without use of Mobile IPv6 for these packets.

RFC Text:
When an automated key management protocol is used to create new security associations for a peer, it is important to ensure that the peer can send the key management protocol packets to the mobile node. This may not be possible if the peer is the home agent of the mobile node and the purpose of the security associations would be to send a Binding Update to the home agent. Packets addressed to the home address of the mobile node cannot be used before the Binding Update has been processed. For the default case of using IKE [9] as the automated key management protocol, such problems can be avoided by the following requirements when communicating with its home agent:

- **When the mobile node is away from home, it MUST use its care-of address as the Source Address of all packets it sends as part of the key management protocol (without use of Mobile IPv6 for these packets, as suggested in Section 11.3.1).**

- In addition, for all security associations bound to the mobile node's home address established by IKE, the mobile node MUST include an ISAKMP Identification Payload [8] in the IKE phase 2 exchange, giving the mobile node's home address as the initiator of the Security Association [7].

Identifier: RQ_001_1629
RFC Clause: 11.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
For all security associations bound to the mobile node's home address established by IKE, the mobile node MUST include an ISAKMP Identification Payload [8] in the IKE phase 2 exchange, giving the mobile node's home address as the initiator of the Security Association [7].

RFC Text:
When an automated key management protocol is used to create new security associations for a peer, it is important to ensure that the peer can send the key management protocol packets to the mobile node. This may not be possible if the peer is the home agent of the mobile node and the purpose of the security associations would be to send a Binding Update to the home agent. Packets addressed to the home address of the mobile node cannot be used before the Binding Update has been processed. For the default case of using IKE [9] as the automated key management protocol, such problems can be avoided by the following requirements when communicating with its home agent:

- When the mobile node is away from home, it MUST use its care-of address as the Source Address of all packets it sends as part of the key management protocol (without use of Mobile IPv6 for these packets, as suggested in Section 11.3.1).

- **In addition, for all security associations bound to the mobile node's home address established by IKE, the mobile node MUST include an ISAKMP Identification Payload [8] in the IKE phase 2 exchange, giving the mobile node's home address as the initiator of the Security Association [7].**

Identifier: RQ_001_1630
RFC Clause: 11.3.2
Type: Optional
Applies to: Mobile_Node

Requirement:
The Key Management Mobility Capability (K) bit in Binding Updates and Acknowledgements can be used to avoid the need to rerun IKE upon movements.

RFC Text:
The Key Management Mobility Capability (K) bit in Binding Updates and Acknowledgements can be used to avoid the need to rerun IKE upon movements.

Identifier: RQ_001_1631
RFC Clause: 11.3.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If, while away from home, a mobile node receives packets addressed to its home address, sent by a correspondent node, that does not have a Binding Cache entry for the mobile node, the mobile node MUST check that the IPv6 source address of the tunneled packet is the IP address of its home agent.

RFC Text:
For packets received by the first method, the mobile node MUST check that the IPv6 source address of the tunneled packet is the IP address of its home agent. In this method, the mobile node may also send a Binding Update to the original sender of the packet as described in Section 11.7.2 and subject to the rate limiting defined in Section 11.8. The mobile node MUST also process the received packet in the manner defined for IPv6 encapsulation [15], which will result in the encapsulated (inner) packet being processed normally by upper-layer protocols within the mobile node as if it had been addressed (only) to the mobile node's home address.

Identifier: RQ_001_1632
RFC Clause: 11.3.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If, while away from home, a mobile node receives packets addressed to its home address, sent by a correspondent node, that does not have a Binding Cache entry for the mobile node, the mobile node MUST process the received packet in the manner defined for IPv6 encapsulation.

RFC Text:
For packets received by the first method, the mobile node MUST check that the IPv6 source address of the tunneled packet is the IP address of its home agent. In this method, the mobile node may also send a Binding Update to the original sender of the packet as described in Section 11.7.2 and subject to the rate limiting defined in Section 11.8. **The mobile node MUST also process the received packet in the manner defined for IPv6 encapsulation [15],** which will result in the encapsulated (inner) packet being processed normally by upper-layer protocols within the mobile node as if it had been addressed (only) to the mobile node's home address.

Identifier: RQ_001_1633
RFC Clause: 11.3.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a node, away from home, encounters a type 2 routing header during this processing, it performs the following checks. If any of these checks fail, the node MUST silently discard the packet.

o The length field in the routing header is exactly 2.

o The segments left field in the routing header is 1 on the wire. (But implementations may process the routing header so that the value may become 0 after the routing header has been processed, but before the rest of the packet is processed.)

o The Home Address field in the routing header is one of the node's home addresses, if the segments left field was 1. Thus, in particular the address field is required to be a unicast routable address.

RFC Text:
A node receiving a packet addressed to itself (i.e., one of the node's addresses is in the IPv6 destination field) follows the next header chain of headers and processes them. **When it encounters a type 2 routing header during this processing, it performs the following checks. If any of these checks fail, the node MUST silently discard the packet.**

o The length field in the routing header is exactly 2.

o The segments left field in the routing header is 1 on the wire. (But implementations may process the routing header so that the value may become 0 after the routing header has been processed, but before the rest of the packet is processed.)

o The Home Address field in the routing header is one of the node's home addresses, if the segments left field was 1. Thus, in particular the address field is required to be a unicast routable address.

Identifier: RQ_001_1634
RFC Clause: 11.3.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If a mobile node joins a multicast group, via a (local) multicast router on the foreign link being visited, the mobile node MUST use its care-of address.

RFC Text:
In order to receive packets sent to some multicast group, a mobile node must join that multicast group. One method, in which a mobile node MAY join the group, is via a (local) multicast router on the foreign link being visited. In this case, the mobile node MUST use its care-of address and MUST NOT use the Home Address destination option when sending MLD packets [17].

Identifier: RQ_001_1635
RFC Clause: 11.3.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If a mobile node joins a multicast group, via a (local) multicast router on the foreign link being visited, the mobile node MUST NOT use the Home Address destination option when sending MLD packets.

RFC Text:
In order to receive packets sent to some multicast group, a mobile node must join that multicast group. One method, in which a mobile node MAY join the group, is via a (local) multicast router on the foreign link being visited. In this case, the mobile node MUST use its care-of address and **MUST NOT use the Home Address destination option when sending MLD packets [17].**

Identifier: RQ_001_1636
RFC Clause: 11.3.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If a mobile node joins a multicast group, via a bi- directional tunnel to its home agent, the mobile node MUST NOT tunnel multicast group membership control packets until 1) the mobile node has a binding in place at the home agent, and 2) the latter sends at least one multicast group membership control packet via the tunnel.

RFC Text:
Alternatively, **a mobile node MAY join multicast groups via a bi- directional tunnel to its home agent.** The mobile node tunnels its multicast group membership control packets (such as those defined in [17] or in [37]) to its home agent, and the home agent forwards multicast packets down the tunnel to the mobile node. **A mobile node MUST NOT tunnel multicast group membership control packets until (1) the mobile node has a binding in place at the home agent, and (2) the latter sends at least one multicast group membership control packet via the tunnel.** Once this condition is true, the mobile node SHOULD assume it does not change as long as the binding does not expire.

Identifier: RQ_001_1637
RFC Clause: 11.3.4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If a mobile node joins a multicast group, via a bi- directional tunnel to its home agent, the mobile node SHOULD assume that, once established, the binding does not change as long as the binding does not expire.

RFC Text:
Alternatively, a mobile node MAY join multicast groups via a bi- directional tunnel to its home agent. The mobile node tunnels its multicast group membership control packets (such as those defined in [17] or in [37]) to its home agent, and the home agent forwards multicast packets down the tunnel to the mobile node. A mobile node MUST NOT tunnel multicast group membership control packets until (1) the mobile node has a binding in place at the home agent, and (2) the latter sends at least one multicast group membership control packet via the tunnel. **Once this condition is true, the mobile node SHOULD assume it does not change as long as the binding does not expire.**

Identifier: RQ_001_1638
RFC Clause: 11.3.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node sends packets to a multicast group directly on the foreign link being visited, the mobile node MUST NOT use Home Address destination option in such traffic.

RFC Text:
A mobile node that wishes to send packets to a multicast group also has two options:

1. Send directly on the foreign link being visited.

The application is aware of the care-of address and uses it as a source address for multicast traffic, just like it would use a stationary address. The mobile node MUST NOT use Home Address destination option in such traffic.

2. Send via a tunnel to its home agent.

Because multicast routing in general depends upon the Source Address used in the IPv6 header of the multicast packet, a mobile node that tunnels a multicast packet to its home agent MUST use its home address as the IPv6 Source Address of the inner multicast packet.

Identifier: RQ_001_1639
RFC Clause: 11.3.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node sends packets to a multicast group, via a tunnel to its home agent, it MUST use its home address as the IPv6 Source Address of the inner multicast packet.

RFC Text:
A mobile node that wishes to send packets to a multicast group also has two options:

1. Send directly on the foreign link being visited.

The application is aware of the care-of address and uses it as a source address for multicast traffic, just like it would use a stationary address. The mobile node MUST NOT use Home Address destination option in such traffic.

2. **Send via a tunnel to its home agent.**

Because multicast routing in general depends upon the Source Address used in the IPv6 header of the multicast packet, a mobile node that tunnels a multicast packet to its home agent MUST use its home address as the IPv6 Source Address of the inner multicast packet.

Identifier: RQ_001_1640
RFC Clause: 11.3.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the mobile node receives an ICMP Parameter Problem, Code 1 error message in response to a return routability procedure or Binding Update, it SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination.

RFC Text:
Any node that does not recognize the Mobility header will return an ICMP Parameter Problem, Code 1, message to the sender of the packet. If the mobile node receives such an ICMP error message in response to a return routability procedure or Binding Update, it SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination. Such Binding Update List entries SHOULD be removed after a period of time in order to allow for retrying route optimization.

Identifier: RQ_001_1641
RFC Clause: 11.3.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
Binding Update List entries updated as a result of an ICMP Parameter Problem, Code 1 error message SHOULD be removed after a period of time in order to allow for retrying route optimization.

RFC Text:
Any node that does not recognize the Mobility header will return an ICMP Parameter Problem, Code 1, message to the sender of the packet. If the mobile node receives such an ICMP error message in response to a return routability procedure or Binding Update, it SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination. **Such Binding Update List entries SHOULD be removed after a period of time in order to allow for retrying route optimization.**

Identifier: RQ_001_1642
RFC Clause: 11.3.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
New Binding Update List entries MUST NOT be created as a result of receiving ICMP error messages.

RFC Text:
New Binding Update List entries MUST NOT be created as a result of receiving ICMP error messages.

Identifier: RQ_001_1643
RFC Clause: 11.3.5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Correspondent nodes that have participated in the return routability procedure MUST implement the ability to correctly process received packets containing a Home Address destination option.

RFC Text:
Correspondent nodes that have participated in the return routability procedure MUST implement the ability to correctly process received packets containing a Home Address destination option.
Therefore, correctly implemented correspondent nodes should always be able to recognize Home Address options. If a mobile node receives an ICMP Parameter Problem, Code 2, message from some node indicating that it does not support the Home Address option, the mobile node SHOULD log the error and then discard the ICMP message.

Identifier: RQ_001_1644
RFC Clause: 11.3.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If a mobile node receives an ICMP Parameter Problem, Code 2, message from some node indicating that it does not support the Home Address option, the mobile node SHOULD log the error and then discard the ICMP message.

RFC Text:
Correspondent nodes that have participated in the return routability procedure MUST implement the ability to correctly process received packets containing a Home Address destination option. Therefore, correctly implemented correspondent nodes should always be able to recognize Home Address options. **If a mobile node receives an ICMP Parameter Problem, Code 2, message from some node indicating that it does not support the Home Address option, the mobile node SHOULD log the error and then discard the ICMP message.**

Identifier: RQ_001_1645
RFC Clause: 11.3.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet containing a Binding Error message, it should first check if the mobile node has a Binding Update List entry for the source of the Binding Error message. If the mobile node does not have such an entry, it MUST ignore the message.

RFC Text:
When a mobile node receives a packet containing a Binding Error message, it should first check if the mobile node has a Binding Update List entry for the source of the Binding Error message. If the mobile node does not have such an entry, it MUST ignore the message. This is necessary to prevent a waste of resources on, e.g., return routability procedure due to spoofed Binding Error messages.

Identifier: RQ_001_1647
RFC Clause: 11.3.6
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet containing a Binding Error message with a message Status field of 1 and if the mobile node has recent upper layer progress information, which indicates that communications with the correspondent node are progressing, the mobile node should, ignore the message.

RFC Text:
Otherwise, if the message Status field was 1 (unknown binding for Home Address destination option), the mobile node should perform one of the following two actions:

- **If the mobile node has recent upper layer progress information, which indicates that communications with the correspondent node are progressing, it MAY ignore the message. This can be done in order to limit the damage that spoofed Binding Error messages can cause to ongoing communications.**

- If the mobile node has no upper layer progress information, it MUST remove the entry and route further communications through the home agent. It MAY also optionally start a return routability procedure (see Section 5.2).

Identifier: RQ_001_1648
RFC Clause: 11.3.6
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet containing a Binding Error message with a message Status field of 1 and if the mobile node has no upper layer progress information, it MUST remove the entry and route further communications through the home agent.

RFC Text:
Otherwise, if the message Status field was 1 (unknown binding for Home Address destination option), the mobile node should perform one of the following two actions:

- o If the mobile node has recent upper layer progress information, which indicates that communications with the correspondent node are progressing, it MAY ignore the message. This can be done in order to limit the damage that spoofed Binding Error messages can cause to ongoing communications.

- **o If the mobile node has no upper layer progress information, it MUST remove the entry and route further communications through the home agent.** It MAY also optionally start a return routability procedure (see Section 5.2).

Identifier: RQ_001_1649
RFC Clause: 11.3.6
Type: Optional
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet containing a Binding Error message with a message Status field of 1 and if the mobile node has no upper layer progress information, it MAY also optionally start a return routability procedure.

RFC Text:
Otherwise, if the message Status field was 1 (unknown binding for Home Address destination option), the mobile node should perform one of the following two actions:

- o If the mobile node has recent upper layer progress information, which indicates that communications with the correspondent node are progressing, it MAY ignore the message. This can be done in order to limit the damage that spoofed Binding Error messages can cause to ongoing communications.

- o **If the mobile node has no upper layer progress information,** it MUST remove the entry and route further communications through the home agent. **It MAY also optionally start a return routability procedure (see Section 5.2).**

Identifier: RQ_001_1650
RFC Clause: 11.3.6
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet containing a Binding Error message with a message Status field of 2, if the mobile node is not expecting an acknowledgement or response from the correspondent node, the mobile node SHOULD ignore this message.

RFC Text:
If the message Status field was 2 (unrecognized MH Type value), the mobile node should perform one of the following two actions:

- **If the mobile node is not expecting an acknowledgement or response from the correspondent node, the mobile node SHOULD ignore this message.**

- Otherwise, the mobile node SHOULD cease the use of any extensions to this specification. If no extensions had been used, the mobile node should cease the attempt to use route optimization.

Identifier: RQ_001_1651
RFC Clause: 11.3.6
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet containing a Binding Error message with a message Status field of 2 and if the mobile node is expecting an acknowledgement or response the mobile node it SHOULD cease the use of any extensions to this specification. If no extensions had been used, the mobile node should cease the attempt to use route optimization.

RFC Text:
If the message Status field was 2 (unrecognized MH Type value), the mobile node should perform one of the following two actions:

- If the mobile node is not expecting an acknowledgement or response from the correspondent node, the mobile node SHOULD ignore this message.

- **Otherwise, the mobile node SHOULD cease the use of any extensions to this specification. If no extensions had been used, the mobile node should cease the attempt to use route optimization.**

Identifier: RQ_001_1652
RFC Clause: 11.4.1
Type: Optional
Applies to: Mobile_Node

Requirement:
The mobile node, upon receiving a Home Agent Address Discovery Reply message, MAY then send its home registration Binding Update to any of the unicast IP addresses listed in the Home Agent Addresses field in the Reply.

RFC Text:
The mobile node, upon receiving this Home Agent Address Discovery Reply message, MAY then send its home registration Binding Update to any of the unicast IP addresses listed in the Home Agent Addresses field in the Reply. For example, the mobile node MAY attempt its home registration to each of these addresses, in turn, until its registration is accepted. The mobile node sends a Binding Update to an address and waits for the matching Binding Acknowledgement, moving on to the next address if there is no response. The mobile node MUST, however, wait at least InitialBindackTimeoutFirstReg seconds (see Section 13) before sending a Binding Update to the next home agent. In trying each of the returned home agent addresses, the mobile node SHOULD try each of them in the order they appear in the Home Agent Addresses field in the received Home Agent Address Discovery Reply message.

Identifier: RQ_001_1653
RFC Clause: 11.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If there is no response to a Binding Update, the mobile node MUST, wait at least InitialBindackTimeoutFirstReg seconds before sending a Binding Update to the next home agent.

RFC Text:
The mobile node, upon receiving this Home Agent Address Discovery Reply message, MAY then send its home registration Binding Update to any of the unicast IP addresses listed in the Home Agent Addresses field in the Reply. For example, the mobile node MAY attempt its home registration to each of these addresses, in turn, until its registration is accepted. **The mobile node sends a Binding Update to an address and waits for the matching Binding Acknowledgement, moving on to the next address if there is no response. The mobile node MUST, however, wait at least InitialBindackTimeoutFirstReg seconds (see Section 13) before sending a Binding Update to the next home agent.** In trying each of the returned home agent addresses, the mobile node SHOULD try each of them in the order they appear in the Home Agent Addresses field in the received Home Agent Address Discovery Reply message.

Identifier: RQ_001_1654
RFC Clause: 11.4.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
In trying each of the returned home agent addresses, the mobile node SHOULD try each of them in the order they appear in the Home Agent Addresses field in the received Home Agent Address Discovery Reply message.

RFC Text:
The mobile node, upon receiving this Home Agent Address Discovery Reply message, MAY then send its home registration Binding Update to any of the unicast IP addresses listed in the Home Agent Addresses field in the Reply. For example, the mobile node MAY attempt its home registration to each of these addresses, in turn, until its registration is accepted. The mobile node sends a Binding Update to an address and waits for the matching Binding Acknowledgement, moving on to the next address if there is no response. The mobile node MUST, however, wait at least InitialBindackTimeoutFirstReg seconds (see Section 13) before sending a Binding Update to the next home agent. **In trying each of the returned home agent addresses, the mobile node SHOULD try each of them in the order they appear in the Home Agent Addresses field in the received Home Agent Address Discovery Reply message.**

Identifier: RQ_001_1655
RFC Clause: 11.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the mobile node has a current registration with some home agent (the Lifetime for that registration has not yet expired), then the mobile node MUST attempt any new registration first with that home agent.

RFC Text:
If the mobile node has a current registration with some home agent (the Lifetime for that registration has not yet expired), then the mobile node MUST attempt any new registration first with that home agent. If that registration attempt fails (e.g., timed out or rejected), the mobile node SHOULD then reattempt this registration with another home agent. If the mobile node knows of no other suitable home agent, then it MAY attempt the dynamic home agent address discovery mechanism described above.

Identifier: RQ_001_1656
RFC Clause: 11.4.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the registration attempt with the current home agent fails (e.g., timed out or rejected), the mobile node SHOULD then reattempt this registration with another home agent.

RFC Text:
If the mobile node has a current registration with some home agent (the Lifetime for that registration has not yet expired), then the mobile node MUST attempt any new registration first with that home agent. If that registration attempt fails (e.g., timed out or rejected), the mobile node SHOULD then reattempt this registration with another home agent. If the mobile node knows of no other suitable home agent, then it MAY attempt the dynamic home agent address discovery mechanism described above.

Identifier: RQ_001_1657
RFC Clause: 11.4.1
Type: Optional
Applies to: Mobile_Node

Requirement:
If the registration attempt with the current home agent fails and the mobile node knows of no other suitable home agent, then it MAY attempt the dynamic home agent address discovery mechanism.

RFC Text:
If the mobile node has a current registration with some home agent (the Lifetime for that registration has not yet expired), then the mobile node MUST attempt any new registration first with that home agent. If that registration attempt fails (e.g., timed out or rejected), the mobile node SHOULD then reattempt this registration with another home agent. **If the mobile node knows of no other suitable home agent, then it MAY attempt the dynamic home agent address discovery mechanism described above.**

Identifier: RQ_001_1658
RFC Clause: 11.4.1
Type: Optional
Applies to: Mobile_Node

Requirement:
If, after a mobile node transmits a Home Agent Address Discovery Request message to the Home Agents Anycast address, it does not receive a corresponding Home Agent Address Discovery Reply message within INITIAL_DHAAD_TIMEOUT seconds, the mobile node MAY retransmit the same Request message to the same anycast address.

RFC Text:
If, after a mobile node transmits a Home Agent Address Discovery Request message to the Home Agents Anycast address, it does not receive a corresponding Home Agent Address Discovery Reply message within INITIAL_DHAAD_TIMEOUT (see Section 12) seconds, the mobile node MAY retransmit the same Request message to the same anycast address. This retransmission MAY be repeated up to a maximum of DHAAD_RETRIES (see Section 12) attempts. Each retransmission MUST be delayed by twice the time interval of the previous retransmission.

Identifier: RQ_001_1659
RFC Clause: 11.4.1
Type: Optional
Applies to: Mobile_Node

Requirement:
In the event that a corresponding Home Agent Address Discovery Reply message is not received within INITIAL_DHAAD_TIMEOUT (see Section 12) seconds, the retransmission of Home Agent Address Discovery Request message to the Home Agents Anycast address MAY be repeated up to a maximum of DHAAD_RETRIES attempts.

RFC Text:
If, after a mobile node transmits a Home Agent Address Discovery Request message to the Home Agents Anycast address, it does not receive a corresponding Home Agent Address Discovery Reply message within INITIAL_DHAAD_TIMEOUT (see Section 12) seconds, the mobile node MAY retransmit the same Request message to the same anycast address. **This retransmission MAY be repeated up to a maximum of DHAAD_RETRIES (see Section 12) attempts.** Each retransmission MUST be delayed by twice the time interval of the previous retransmission.

Identifier: RQ_001_1660
RFC Clause: 11.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the event that a corresponding Home Agent Address Discovery Reply message is not received within INITIAL_DHAAD_TIMEOUT (see Section 12) seconds, each retransmission MUST be delayed by twice the time interval of the previous retransmission.

RFC Text:
If, after a mobile node transmits a Home Agent Address Discovery Request message to the Home Agents Anycast address, it does not receive a corresponding Home Agent Address Discovery Reply message within INITIAL_DHAAD_TIMEOUT (see Section 12) seconds, the mobile node MAY retransmit the same Request message to the same anycast address. This retransmission MAY be repeated up to a maximum of DHAAD_RETRIES (see Section 12) attempts. **Each retransmission MUST be delayed by twice the time interval of the previous retransmission.**

Identifier: RQ_001_1661
RFC Clause: 11.4.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node has a home address that is about to become invalid, it SHOULD send a Mobile Prefix Solicitation to its home agent in an attempt to acquire fresh routing prefix information.

RFC Text:
When a mobile node has a home address that is about to become invalid, it SHOULD send a Mobile Prefix Solicitation to its home agent in an attempt to acquire fresh routing prefix information. The new information also enables the mobile node to participate in renumbering operations affecting the home network, as described in Section 10.6.

Identifier: RQ_001_1662
RFC Clause: 11.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When sending mobile prefix solicitations, the mobile node MUST use the Home Address destination option to carry its home address.

RFC Text:
The mobile node MUST use the Home Address destination option to carry its home address. The mobile node MUST support and SHOULD use IPsec to protect the solicitation. The mobile node MUST set the Identifier field in the ICMP header to a random value.

Identifier: RQ_001_1663
RFC Clause: 11.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When sending mobile prefix solicitations, the mobile node MUST support IPsec to protect the solicitation.

RFC Text:
The mobile node MUST use the Home Address destination option to carry its home address. **The mobile node MUST support and SHOULD use IPsec to protect the solicitation.** The mobile node MUST set the Identifier field in the ICMP header to a random value.

Identifier: RQ_001_1664
RFC Clause: 11.4.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When sending mobile prefix solicitations, the mobile node SHOULD use IPsec to protect the solicitation.

RFC Text:
The mobile node MUST use the Home Address destination option to carry its home address. **The mobile node MUST support and SHOULD use IPsec to protect the solicitation.** The mobile node MUST set the Identifier field in the ICMP header to a random value.

Identifier: RQ_001_1665
RFC Clause: 11.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When sending mobile prefix solicitations, the mobile node MUST set the Identifier field in the ICMP header to a random value.

RFC Text:
The mobile node MUST use the Home Address destination option to carry its home address. The mobile node MUST support and SHOULD use IPsec to protect the solicitation. **The mobile node MUST set the Identifier field in the ICMP header to a random value.**

Identifier: RQ_001_1666
RFC Clause: 11.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Binding Updates sent by the mobile node to other nodes MUST use a lifetime no greater than the remaining lifetime of its home registration of its primary care-of address.

RFC Text:
As described in Section 11.7.2, **Binding Updates sent by the mobile node to other nodes MUST use a lifetime no greater than the remaining lifetime of its home registration of its primary care-of address.** The mobile node SHOULD further limit the lifetimes that it sends on any Binding Updates to be within the remaining valid lifetime (see Section 10.6.2) for the prefix in its home address.

Identifier: RQ_001_1667
RFC Clause: 11.4.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The mobile node SHOULD limit the lifetimes that it sends on any Binding Updates to be within the remaining valid lifetime (see Section 10.6.2) for the prefix in its home address.

RFC Text:
As described in Section 11.7.2, Binding Updates sent by the mobile node to other nodes MUST use a lifetime no greater than the remaining lifetime of its home registration of its primary care-of address. **The mobile node SHOULD further limit the lifetimes that it sends on any Binding Updates to be within the remaining valid lifetime (see Section 10.6.2) for the prefix in its home address.**

Identifier: RQ_001_1668
RFC Clause: 11.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When the lifetime for a changed prefix decreases, and the change would cause cached bindings at correspondent nodes in the Binding Update List to be stored past the newly shortened lifetime, the mobile node MUST issue a Binding Update to all such correspondent nodes.

RFC Text:
When the lifetime for a changed prefix decreases, and the change would cause cached bindings at correspondent nodes in the Binding Update List to be stored past the newly shortened lifetime, the mobile node MUST issue a Binding Update to all such correspondent nodes.

Identifier: RQ_001_1669
RFC Clause: 11.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node receives a Mobile Prefix Advertisement, it MUST validate it to confirm that the Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address.

RFC Text:
When a mobile node receives a Mobile Prefix Advertisement, it MUST validate it according to the following test:

o The Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address. Otherwise, if no such registrations have been made, it SHOULD be the mobile node's stored home agent address, if one exists. Otherwise, if the mobile node has not yet discovered its home agent's address, it MUST NOT accept Mobile Prefix Advertisements.

o The packet MUST have a type 2 routing header and SHOULD be protected by an IPsec header as described in Section 5.4 and Section 6.8.

o If the ICMP Identifier value matches the ICMP Identifier value of the most recently sent Mobile Prefix Solicitation and no other advertisement has yet been received for this value, then the advertisement is considered to be solicited and will be processed further.

Otherwise, the advertisement is unsolicited, and MUST be discarded. In this case the mobile node SHOULD send a Mobile Prefix Solicitation.

Identifier: RQ_001_1670
RFC Clause: 11.4.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:

When a mobile node receives a Mobile Prefix Advertisement, it is unable to validate it to confirm that the Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address, it SHOULD use the mobile node's stored home agent address, if one exists.

RFC Text:

When a mobile node receives a Mobile Prefix Advertisement, it MUST validate it according to the following test:

- **The Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address. Otherwise, if no such registrations have been made, it SHOULD be the mobile node's stored home agent address, if one exists.** Otherwise, if the mobile node has not yet discovered its home agent's address, it MUST NOT accept Mobile Prefix Advertisements.

- The packet MUST have a type 2 routing header and SHOULD be protected by an IPsec header as described in Section 5.4 and Section 6.8.

- If the ICMP Identifier value matches the ICMP Identifier value of the most recently sent Mobile Prefix Solicitation and no other advertisement has yet been received for this value, then the advertisement is considered to be solicited and will be processed further.

  Otherwise, the advertisement is unsolicited, and MUST be discarded. In this case the mobile node SHOULD send a Mobile Prefix Solicitation.

Identifier: RQ_001_1671
RFC Clause: 11.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node receives a Mobile Prefix Advertisement for which the mobile node has not yet discovered its home agent's address, it MUST NOT accept Mobile Prefix Advertisements.

RFC Text:
When a mobile node receives a Mobile Prefix Advertisement, it MUST validate it according to the following test:

- The Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address. Otherwise, if no such registrations have been made, it SHOULD be the mobile node's stored home agent address, if one exists. **Otherwise, if the mobile node has not yet discovered its home agent's address, it MUST NOT accept Mobile Prefix Advertisements.**

- The packet MUST have a type 2 routing header and SHOULD be protected by an IPsec header as described in Section 5.4 and Section 6.8.

- If the ICMP Identifier value matches the ICMP Identifier value of the most recently sent Mobile Prefix Solicitation and no other advertisement has yet been received for this value, then the advertisement is considered to be solicited and will be processed further.

  Otherwise, the advertisement is unsolicited, and MUST be discarded. In this case the mobile node SHOULD send a Mobile Prefix Solicitation.

Identifier: RQ_001_1672
RFC Clause: 11.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node receives a Mobile Prefix Advertisement, the packet MUST have a type 2 routing header.

RFC Text:
When a mobile node receives a Mobile Prefix Advertisement, it MUST validate it according to the following test:

- The Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address. Otherwise, if no such registrations have been made, it SHOULD be the mobile node's stored home agent address, if one exists. Otherwise, if the mobile node has not yet discovered its home agent's address, it MUST NOT accept Mobile Prefix Advertisements.

- **The packet MUST have a type 2 routing header** and SHOULD be protected by an IPsec header as described in Section 5.4 and Section 6.8.

- If the ICMP Identifier value matches the ICMP Identifier value of the most recently sent Mobile Prefix Solicitation and no other advertisement has yet been received for this value, then the advertisement is considered to be solicited and will be processed further.

  Otherwise, the advertisement is unsolicited, and MUST be discarded. In this case the mobile node SHOULD send a Mobile Prefix Solicitation.

Identifier: RQ_001_1673
RFC Clause: 11.4.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node receives a Mobile Prefix Advertisement, the packet SHOULD be protected by an IPsec header.

RFC Text:
When a mobile node receives a Mobile Prefix Advertisement, it MUST validate it according to the following test:

o The Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address. Otherwise, if no such registrations have been made, it SHOULD be the mobile node's stored home agent address, if one exists. Otherwise, if the mobile node has not yet discovered its home agent's address, it MUST NOT accept Mobile Prefix Advertisements.

o The packet MUST have a type 2 routing header and SHOULD be protected by an IPsec header as described in Section 5.4 and Section 6.8.

o If the ICMP Identifier value matches the ICMP Identifier value of the most recently sent Mobile Prefix Solicitation and no other advertisement has yet been received for this value, then the advertisement is considered to be solicited and will be processed further.

Otherwise, the advertisement is unsolicited, and MUST be discarded. In this case the mobile node SHOULD send a Mobile Prefix Solicitation.

Identifier: RQ_001_1674
RFC Clause: 11.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node receives an unsolicted Mobile Prefix Advertisement and is unable to validate it, it MUST be discarded.

RFC Text:
When a mobile node receives a Mobile Prefix Advertisement, it MUST validate it according to the following test:

o The Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address. Otherwise, if no such registrations have been made, it SHOULD be the mobile node's stored home agent address, if one exists. Otherwise, if the mobile node has not yet discovered its home agent's address, it MUST NOT accept Mobile Prefix Advertisements.

o The packet MUST have a type 2 routing header and SHOULD be protected by an IPsec header as described in Section 5.4 and Section 6.8.

o If the ICMP Identifier value matches the ICMP Identifier value of the most recently sent Mobile Prefix Solicitation and no other advertisement has yet been received for this value, then the advertisement is considered to be solicited and will be processed further.

Otherwise, the advertisement is unsolicited, and MUST be discarded. In this case the mobile node SHOULD send a Mobile Prefix Solicitation.

Identifier: RQ_001_1675
RFC Clause: 11.4.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node receives an unsolicted Mobile Prefix Advertisement and is unable to validate it, it SHOULD send a Mobile Prefix Solicitation.

RFC Text:
When a mobile node receives a Mobile Prefix Advertisement, it MUST validate it according to the following test:

- The Source Address of the IP packet carrying the Mobile Prefix Advertisement is the same as the home agent address to which the mobile node last sent an accepted home registration Binding Update to register its primary care-of address. Otherwise, if no such registrations have been made, it SHOULD be the mobile node's stored home agent address, if one exists. Otherwise, if the mobile node has not yet discovered its home agent's address, it MUST NOT accept Mobile Prefix Advertisements.

- The packet MUST have a type 2 routing header and SHOULD be protected by an IPsec header as described in Section 5.4 and Section 6.8.

- If the ICMP Identifier value matches the ICMP Identifier value of the most recently sent Mobile Prefix Solicitation and no other advertisement has yet been received for this value, then the advertisement is considered to be solicited and will be processed further.

  Otherwise, the advertisement is unsolicited, and MUST be discarded. In this case **the mobile node SHOULD send a Mobile Prefix Solicitation.**

Identifier: RQ_001_1676
RFC Clause: 11.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node receives a Mobile Prefix Advertisement which it cannot validate, it MUST be silently discarded.

RFC Text:
Any received Mobile Prefix Advertisement not meeting these tests MUST be silently discarded.

Identifier: RQ_001_1677
RFC Clause: 11.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
For an accepted Mobile Prefix Advertisement, the mobile node MUST process Managed Address Configuration (M), Other Stateful Configuration (O), and the Prefix Information Options as if they arrived in a Router Advertisement [12] on the mobile node's home link.

RFC Text:
For an accepted Mobile Prefix Advertisement, the mobile node MUST process Managed Address Configuration (M), Other Stateful Configuration (O), and the Prefix Information Options as if they arrived in a Router Advertisement [12] on the mobile node's home link. (This specification does not, however, describe how to acquire home addresses through stateful protocols.) Such processing may result in the mobile node configuring a new home address, although due to separation between preferred lifetime and valid lifetime, such changes should not affect most communications by the mobile node, in the same way as for nodes that are at home.

Identifier: RQ_001_1678
RFC Clause: 11.5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When the mobile node detects that the default router is no longer bi-directionally reachable, it must discover a new default router (usually on a new link).

RFC Text:
Generic movement detection uses Neighbor Unreachability Detection to detect when the default router is no longer bi-directionally reachable, in which case the mobile node must discover a new default router (usually on a new link). However, this detection only occurs when the mobile node has packets to send, and in the absence of frequent Router Advertisements or indications from the link-layer, the mobile node might become unaware of an L3 handover that occurred. Therefore, the mobile node should supplement this method with other information whenever it is available to the mobile node (e.g., from lower protocol layers).

Identifier: RQ_001_1679
RFC Clause: 11.5.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
To augment generic movement detection, using Neighbor Unreachability Detection, the mobile node should supplement this method with other information whenever it is available to the mobile node (e.g., from lower protocol layers).

RFC Text:
Generic movement detection uses Neighbor Unreachability Detection to detect when the default router is no longer bi-directionally reachable, in which case the mobile node must discover a new default router (usually on a new link). However, this detection only occurs when the mobile node has packets to send, and in the absence of frequent Router Advertisements or indications from the link-layer, the mobile node might become unaware of an L3 handover that occurred. Therefore, the mobile node should supplement this method with other information whenever it is available to the mobile node (e.g., from lower protocol layers).

Identifier: RQ_001_1680
RFC Clause: 11.5.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The mobile node should avoid performing an L3 handover until it is strictly necessary.

RFC Text:
Due to the temporary packet flow disruption and signaling overhead involved in updating mobility bindings, the mobile node should avoid performing an L3 handover until it is strictly necessary. Specifically, when the mobile node receives a Router Advertisement from a new router that contains a different set of on-link prefixes, if the mobile node detects that the currently selected default router on the old link is still bi-directionally reachable, it should generally continue to use the old router on the old link rather than switch away from it to use a new default router.

Identifier: RQ_001_1681
RFC Clause: 11.5.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:

When the mobile node receives a Router Advertisement from a new router that contains a different set of on-link prefixes, if the mobile node detects that the currently selected default router on the old link is still bi-directionally reachable, it should generally continue to use the old router on the old link rather than switch away from it to use a new default router.

RFC Text:

Due to the temporary packet flow disruption and signaling overhead involved in updating mobility bindings, the mobile node should avoid performing an L3 handover until it is strictly necessary. **Specifically, when the mobile node receives a Router Advertisement from a new router that contains a different set of on-link prefixes, if the mobile node detects that the currently selected default router on the old link is still bi-directionally reachable, it should generally continue to use the old router on the old link rather than switch away from it to use a new default router.**

Identifier: RQ_001_1682
RFC Clause: 11.5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Upon receiving indications that an L3 handover may have occurred, the mobile node needs to perform Router Discovery to discover routers and prefixes on the new link, as described in Section 6.3.7 of RFC 2461.

RFC Text:
In addition, the mobile node should consider the following events as indications that an L3 handover may have occurred. Upon receiving such indications, the mobile node needs to perform Router Discovery to discover routers and prefixes on the new link, as described in Section 6.3.7 of RFC 2461 [12].

o If Router Advertisements that the mobile node receives include an Advertisement Interval option, the mobile node may use its Advertisement Interval field as an indication of the frequency with which it should expect to continue to receive future Advertisements from that router. This field specifies the minimum rate (the maximum amount of time between successive Advertisements) that the mobile node should expect. If this amount of time elapses without the mobile node receiving any Advertisement from this router, the mobile node can be sure that at least one Advertisement sent by the router has been lost. The mobile node can then implement its own policy to determine how many lost Advertisements from its current default router constitute an L3 handover indication.

o Neighbor Unreachability Detection determines that the default router is no longer reachable.

o With some types of networks, notification that an L2 handover has occurred might be obtained from lower layer protocols or device driver software within the mobile node. While further details around handling L2 indications as movement hints is an item for further study, at the time of writing this specification the following is considered reasonable:

An L2 handover indication may or may not imply L2 movement and L2 movement may or may not imply L3 movement; the correlations might be a function of the type of L2 but might also be a function of actual deployment of the wireless topology.

Unless it is well-known that an L2 handover indication is likely to imply L3 movement, instead of immediately multicasting a router solicitation it may be better to attempt to verify whether the default router is still bi-directionally reachable. This can be accomplished by sending a unicast Neighbor Solicitation and waiting for a Neighbor Advertisement with the solicited flag set. Note that this is similar to Neighbor Unreachability detection but it does not have the same state machine, such as the STALE state.

If the default router does not respond to the Neighbor Solicitation it makes sense to proceed to multicasting a Router Solicitation.

Identifier: RQ_001_1683
RFC Clause: 11.5.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
After detecting that it has moved a mobile node SHOULD generate a new primary care-of address using normal IPv6 mechanisms.

RFC Text:
After detecting that it has moved a mobile node SHOULD generate a new primary care-of address using normal IPv6 mechanisms. This SHOULD also be done when the current primary care-of address becomes deprecated. A mobile node MAY form a new primary care-of address at any time, but a mobile node MUST NOT send a Binding Update about a new care-of address to its home agent more than MAX_UPDATE_RATE times within a second.

Identifier: RQ_001_1684
RFC Clause: 11.5.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The mobile node SHOULD generate a new primary care-of address using normal IPv6 mechanisms when the current primary care-of address becomes deprecated.

RFC Text:
After detecting that it has moved a mobile node SHOULD generate a new primary care-of address using normal IPv6 mechanisms. **This SHOULD also be done when the current primary care-of address becomes deprecated.** A mobile node MAY form a new primary care-of address at any time, but a mobile node MUST NOT send a Binding Update about a new care-of address to its home agent more than MAX_UPDATE_RATE times within a second.

Identifier: RQ_001_1685
RFC Clause: 11.5.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
A mobile node MUST NOT send a Binding Update about a new care-of address to its home agent more than MAX_UPDATE_RATE times within a second.

RFC Text:
After detecting that it has moved a mobile node SHOULD generate a new primary care-of address using normal IPv6 mechanisms. This SHOULD also be done when the current primary care-of address becomes deprecated. A mobile node MAY form a new primary care-of address at any time, but **a mobile node MUST NOT send a Binding Update about a new care-of address to its home agent more than MAX_UPDATE_RATE times within a second.**

Identifier: RQ_001_1686
RFC Clause: 11.5.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If a mobile node needs to use a source address (other than the unspecified address) in packets sent as a part of address autoconfiguration, it MUST use an IPv6 link- local address rather than its own IPv6 home address

RFC Text:
As described in Section 4, in order to form a new care-of address, a mobile node MAY use either stateless [13] or stateful (e.g., DHCPv6 [29]) Address Autoconfiguration. **If a mobile node needs to use a source address (other than the unspecified address) in packets sent as a part of address autoconfiguration, it MUST use an IPv6 link- local address rather than its own IPv6 home address**

Identifier: RQ_001_1687
RFC Clause: 11.5.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When the Mobile Node moves to a new link, the Mobile Node preferably SHOULD NOT delay DAD when configuring a new care-of address.

RFC Text:
RFC 2462 [13] specifies that in normal processing for Duplicate Address Detection, the node SHOULD delay sending the initial Neighbor Solicitation message by a random delay between 0 and MAX_RTR_SOLICITATION_DELAY. **Since delaying DAD can result in significant delays in configuring a new care-of address when the Mobile Node moves to a new link, the Mobile Node preferably SHOULD NOT delay DAD when configuring a new care-of address.** The Mobile Node SHOULD delay according to the mechanisms specified in RFC 2462 unless the implementation has a behavior that desynchronizes the steps that happen before the DAD in the case that multiple nodes experience handover at the same time. Such desynchronizing behaviors might be due to random delays in the L2 protocols or device drivers, or due to the movement detection mechanism that is used.

Identifier: RQ_001_1688
RFC Clause: 11.5.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When the Mobile Node moves to a new link, the Mobile Node preferably SHOULD delay DAD according to the mechanisms specified in RFC 2462 unless the implementation has a behavior that desynchronizes the steps that happen before the DAD in the case that multiple nodes experience handover at the same time.

RFC Text:
RFC 2462 [13] specifies that in normal processing for Duplicate Address Detection, the node SHOULD delay sending the initial Neighbor Solicitation message by a random delay between 0 and MAX_RTR_SOLICITATION_DELAY. Since delaying DAD can result in significant delays in configuring a new care-of address when the Mobile Node moves to a new link, the Mobile Node preferably SHOULD NOT delay DAD when configuring a new care-of address. **The Mobile Node SHOULD delay according to the mechanisms specified in RFC 2462 unless the implementation has a behavior that desynchronizes the steps that happen before the DAD in the case that multiple nodes experience handover at the same time.** Such desynchronizing behaviors might be due to random delays in the L2 protocols or device drivers, or due to the movement detection mechanism that is used.

Identifier: RQ_001_1689
RFC Clause: 11.5.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The mobile node MUST ensure that its primary care-of address always has a prefix that is advertised by its current default router.

RFC Text:
As described in Section 11.5.2, a mobile node MAY use more than one care-of address at a time. Particularly in the case of many wireless networks, a mobile node effectively might be reachable through multiple links at the same time (e.g., with overlapping wireless cells), on which different on-link subnet prefixes may exist. **The mobile node MUST ensure that its primary care-of address always has a prefix that is advertised by its current default router.** After selecting a new primary care-of address, the mobile node MUST send a Binding Update containing that care-of address to its home agent. The Binding Update MUST have the Home Registration (H) and Acknowledge (A) bits set its home agent, as described on Section 11.7.1.

Identifier: RQ_001_1690
RFC Clause: 11.5.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
After selecting a new primary care-of address, the mobile node MUST send a Binding Update containing that care-of address to its home agent.

RFC Text:
As described in Section 11.5.2, a mobile node MAY use more than one care-of address at a time. Particularly in the case of many wireless networks, a mobile node effectively might be reachable through multiple links at the same time (e.g., with overlapping wireless cells), on which different on-link subnet prefixes may exist. The mobile node MUST ensure that its primary care-of address always has a prefix that is advertised by its current default router. **After selecting a new primary care-of address, the mobile node MUST send a Binding Update containing that care-of address to its home agent.** The Binding Update MUST have the Home Registration (H) and Acknowledge (A) bits set its home agent, as described on Section 11.7.1.

Identifier: RQ_001_1691
RFC Clause: 11.5.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
After selecting a new primary care-of address, the mobile node MUST send a Binding Update with the Home Registration (H) and Acknowledge (A) bits set.

RFC Text:
As described in Section 11.5.2, a mobile node MAY use more than one care-of address at a time. Particularly in the case of many wireless networks, a mobile node effectively might be reachable through multiple links at the same time (e.g., with overlapping wireless cells), on which different on-link subnet prefixes may exist. The mobile node MUST ensure that its primary care-of address always has a prefix that is advertised by its current default router. After selecting a new primary care-of address, the mobile node MUST send a Binding Update containing that care-of address to its home agent**. The Binding Update MUST have the Home Registration (H) and Acknowledge (A) bits set its home agent, as described on Section 11.7.1.**

Identifier: RQ_001_1693
RFC Clause: 11.5.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
To assist with smooth handovers, a mobile node SHOULD still accept packets at its previous primary care-of address as a (non-primary) care-of address, even after registering its new primary care-of address with its home agent.

RFC Text:
To assist with smooth handovers, a mobile node SHOULD retain its previous primary care-of address as a (non-primary) care-of address, and **SHOULD still accept packets at this address, even after registering its new primary care-of address with its home agent.** This is reasonable, since the mobile node could only receive packets at its previous primary care-of address if it were indeed still connected to that link. If the previous primary care-of address was allocated using stateful Address Autoconfiguration [29], the mobile node may not wish to release the address immediately upon switching to a new primary care-of address.

Identifier: RQ_001_1694
RFC Clause: 11.5.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
Whenever a mobile node determines that it is no longer reachable through a given link, it SHOULD invalidate all care-of addresses associated with address prefixes that it discovered from routers on the unreachable link which are not in the current set of address prefixes advertised by the (possibly new) current default router.

RFC Text:
Whenever a mobile node determines that it is no longer reachable through a given link, it SHOULD invalidate all care-of addresses associated with address prefixes that it discovered from routers on the unreachable link which are not in the current set of address prefixes advertised by the (possibly new) current default router.

Identifier: RQ_001_1695
RFC Clause: 11.5.4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When the mobile node detects that its home subnet prefix is again on-link (i.e. the Mobile Node has returned to its home link), the mobile node SHOULD then send a Binding Update to its home agent, to instruct its home agent to no longer intercept or tunnel packets for it.

RFC Text:
A mobile node detects that it has returned to its home link through the movement detection algorithm in use (Section 11.5.1), **when the mobile node detects that its home subnet prefix is again on-link. The mobile node SHOULD then send a Binding Update to its home agent, to instruct its home agent to no longer intercept or tunnel packets for it.** In this home registration, the mobile node MUST set the Acknowledge (A) and Home Registration (H) bits, set the Lifetime field to zero, and set the care-of address for the binding to the mobile node's own home address. The mobile node MUST use its home address as the source address in the Binding Update.

Identifier: RQ_001_1696
RFC Clause: 11.5.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the Mobile Node that has returned home sends a Binding Update to instruct its Home Agent to no longer intercept or tunnel packets for it, the Mobile Node MUST set the Acknowledge (A) and Home Registration (H) bits, reset the Lifetime field to zero, set the care-of address for the binding to the mobile node's own home address and MUST use its home address as the source address in the Binding Update.

RFC Text:
A mobile node detects that it has returned to its home link through the movement detection algorithm in use (Section 11.5.1), when the mobile node detects that its home subnet prefix is again on-link. The mobile node SHOULD then send a Binding Update to its home agent, to instruct its home agent to no longer intercept or tunnel packets for it. **In this home registration, the mobile node MUST set the Acknowledge (A) and Home Registration (H) bits, set the Lifetime field to zero, and set the care-of address for the binding to the mobile node's own home address. The mobile node MUST use its home address as the source address in the Binding Update.**

Identifier: RQ_001_1697
RFC Clause: 11.5.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If, on returning home, a mobile node detects multiple home agents and decides to send a neighbour solicitation, the mobile node MUST multicast the packet and set the Source Address of this Neighbor Solicitation to the unspecified address (0:0:0:0:0:0:0:0), also, the target of the Neighbor Solicitation MUST be set to the mobile node's home address and the destination IP address MUST be set to the Solicited-Node multicast address

RFC Text:
Neighbor Solicitation by the mobile node for the home agent's address will normally not be necessary, since the mobile node has already learned the home agent's link-layer address from a Source Link-Layer Address option in a Router Advertisement. However, if there are multiple home agents it may still be necessary to send a solicitation. In this special case of the mobile node returning home, the mobile node MUST multicast the packet, and in addition set the Source Address of this Neighbor Solicitation to the unspecified address (0:0:0:0:0:0:0:0). The target of the Neighbor Solicitation MUST be set to the mobile node's home address. The destination IP address MUST be set to the Solicited-Node multicast address [3]. The home agent will send a multicast Neighbor Advertisement back to the mobile node with the Solicited flag (S) set to zero. In any case, the mobile node SHOULD record the information from the Source Link- Layer Address option or from the advertisement, and set the state of the Neighbor Cache entry for the home agent to REACHABLE.

Identifier: RQ_001_1698
RFC Clause: 11.5.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent SHALL respond to a neighbour solicitation from the mobile node, with a multicast Neighbor Advertisement with the Solicited flag (S) set to zero.

RFC Text:
Neighbor Solicitation by the mobile node for the home agent's address will normally not be necessary, since the mobile node has already learned the home agent's link-layer address from a Source Link-Layer Address option in a Router Advertisement. However, if there are multiple home agents it may still be necessary to send a solicitation. In this special case of the mobile node returning home, the mobile node MUST multicast the packet, and in addition set the Source Address of this Neighbor Solicitation to the unspecified address (0:0:0:0:0:0:0:0). The target of the Neighbor Solicitation MUST be set to the mobile node's home address. The destination IP address MUST be set to the Solicited-Node multicast address [3]**. The home agent will send a multicast Neighbor Advertisement back to the mobile node with the Solicited flag (S) set to zero.** In any case, the mobile node SHOULD record the information from the Source Link- Layer Address option or from the advertisement, and set the state of the Neighbor Cache entry for the home agent to REACHABLE.

Identifier: RQ_001_1699
RFC Clause: 11.5.4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The mobile node, on receipt of a multicast Neighbor Advertisement in response to its neighbour solicitation, SHOULD record the information from the Source Link- Layer Address option or from the advertisement, and set the state of the Neighbor Cache entry for the home agent to REACHABLE.

RFC Text:
Neighbor Solicitation by the mobile node for the home agent's address will normally not be necessary, since the mobile node has already learned the home agent's link-layer address from a Source Link-Layer Address option in a Router Advertisement. However, if there are multiple home agents it may still be necessary to send a solicitation. In this special case of the mobile node returning home, the mobile node MUST multicast the packet, and in addition set the Source Address of this Neighbor Solicitation to the unspecified address (0:0:0:0:0:0:0:0). The target of the Neighbor Solicitation MUST be set to the mobile node's home address. The destination IP address MUST be set to the Solicited-Node multicast address [3]. The home agent will send a multicast Neighbor Advertisement back to the mobile node with the Solicited flag (S) set to zero. **In any case, the mobile node SHOULD record the information from the Source Link- Layer Address option or from the advertisement, and set the state of the Neighbor Cache entry for the home agent to REACHABLE.**

Identifier: RQ_001_1700
RFC Clause: 11.5.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When returning home prior to the expiration of its bindings, the mobile node MUST NOT perform Duplicate Address Detection on its own home address.

RFC Text:
The mobile node then sends its Binding Update to the home agent's link-layer address, instructing its home agent to no longer serve as a home agent for it. By processing this Binding Update, the home agent will cease defending the mobile node's home address for Duplicate Address Detection and will no longer respond to Neighbor Solicitations for the mobile node's home address. The mobile node is then the only node on the link receiving packets at the mobile node's home address. In addition, **when returning home prior to the expiration of a current binding for its home address, and configuring its home address on its network interface on its home link, the mobile node MUST NOT perform Duplicate Address Detection on its own home address,** in order to avoid confusion or conflict with its home agent's use of the same address. This rule also applies to the derived link-local address of the mobile node, if the Link Local Address Compatibility (L) bit was set when the binding was created. If the mobile node returns home after the bindings for all of its care-of addresses have expired, then it SHOULD perform DAD.

Identifier: RQ_001_1701
RFC Clause: 11.5.4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the mobile node returns home after the bindings for all of its care-of addresses have expired, then it SHOULD perform DAD.

RFC Text:
The mobile node then sends its Binding Update to the home agent's link-layer address, instructing its home agent to no longer serve as a home agent for it. By processing this Binding Update, the home agent will cease defending the mobile node's home address for Duplicate Address Detection and will no longer respond to Neighbor Solicitations for the mobile node's home address. The mobile node is then the only node on the link receiving packets at the mobile node's home address. In addition, when returning home prior to the expiration of a current binding for its home address, and configuring its home address on its network interface on its home link, the mobile node MUST NOT perform Duplicate Address Detection on its own home address, in order to avoid confusion or conflict with its home agent's use of the same address. This rule also applies to the derived link-local address of the mobile node, if the Link Local Address Compatibility (L) bit was set when the binding was created. **If the mobile node returns home after the bindings for all of its care-of addresses have expired, then it SHOULD perform DAD.**

Identifier: RQ_001_1702
RFC Clause: 11.5.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
After the Mobile Node sends the Binding Update, it MUST be prepared to reply to Neighbor Solicitations for its home address.

RFC Text:
After the Mobile Node sends the Binding Update, it MUST be prepared to reply to Neighbor Solicitations for its home address. Such replies MUST be sent using a unicast Neighbor Advertisement to the sender's link-layer address. It is necessary to reply, since sending the Binding Acknowledgement from the home agent may require performing Neighbor Discovery, and the mobile node may not be able to distinguish Neighbor Solicitations coming from the home agent from other Neighbor Solicitations. Note that a race condition exists where both the mobile node and the home agent respond to the same solicitations sent by other nodes; this will be only temporary, however, until the Binding Update is accepted.

Identifier: RQ_001_1703
RFC Clause: 11.5.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
After the Mobile Node sends the Binding Update, any replies to Neighbor Solicitations for its home address MUST be sent using a unicast Neighbor Advertisement to the sender's link-layer address.

RFC Text:
After the Mobile Node sends the Binding Update, it MUST be prepared to reply to Neighbor Solicitations for its home address. **Such replies MUST be sent using a unicast Neighbor Advertisement to the sender's link-layer address.** It is necessary to reply, since sending the Binding Acknowledgement from the home agent may require performing Neighbor Discovery, and the mobile node may not be able to distinguish Neighbor Solicitations coming from the home agent from other Neighbor Solicitations. Note that a race condition exists where both the mobile node and the home agent respond to the same solicitations sent by other nodes; this will be only temporary, however, until the Binding Update is accepted.

Identifier: RQ_001_1704
RFC Clause: 11.5.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
After receiving the Binding Acknowledgement from the Home Agent (in response to its Binding Update), the mobile node returning home MUST send a Neighbor Advertisement to the link-local all-nodes multicast address, to advertise the mobile node's own link-layer address for its own home address.

RFC Text:
After receiving the Binding Acknowledgement for its Binding Update to its home agent, the mobile node MUST multicast onto the home link (to the all-nodes multicast address) a Neighbor Advertisement [12], to advertise the mobile node's own link-layer address for its own home address. The Target Address in this Neighbor Advertisement MUST be set to the mobile node's home address, and the Advertisement MUST include a Target Link-layer Address option specifying the mobile node's link-layer address. The mobile node MUST multicast such a Neighbor Advertisement for each of its home addresses, as defined by the current on-link prefixes, including its link-local address and site-local address. The Solicited Flag (S) in these Advertisements MUST NOT be set, since they were not solicited by any Neighbor Solicitation. The Override Flag (O) in these Advertisements MUST be set, indicating that the Advertisements SHOULD override any existing Neighbor Cache entries at any node receiving them.

Identifier: RQ_001_1705
RFC Clause: 11.5.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
After receiving the Binding Acknowledgement from the Home Agent (in response to its Binding Update), the mobile node returning home MUST send a Neighbor Advertisement to the link-local all-nodes multicast address. In this Neighbor Advertisement the Target Address MUST be set to the mobile node's home address, and a Target Link-layer Address option MUST be included specifying the mobile node's link-layer address.

RFC Text:
After receiving the Binding Acknowledgement for its Binding Update to its home agent, the mobile node MUST multicast onto the home link (to the all-nodes multicast address) a Neighbor Advertisement [12], to advertise the mobile node's own link-layer address for its own home address. **The Target Address in this Neighbor Advertisement MUST be set to the mobile node's home address, and the Advertisement MUST include a Target Link-layer Address option specifying the mobile node's link-layer address.** The mobile node MUST multicast such a Neighbor Advertisement for each of its home addresses, as defined by the current on-link prefixes, including its link-local address and site-local address. The Solicited Flag (S) in these Advertisements MUST NOT be set, since they were not solicited by any Neighbor Solicitation. The Override Flag (O) in these Advertisements MUST be set, indicating that the Advertisements SHOULD override any existing Neighbor Cache entries at any node receiving them.

Identifier: RQ_001_1706
RFC Clause: 11.5.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The mobile node MUST multicast such a Neighbor Advertisement for each of its home addresses, as defined by the current on-link prefixes, including its link-local address and site-local address. The Solicited Flag (S) in these Advertisements MUST NOT be set and the Override Flag (O) in these Advertisements MUST be set.

RFC Text:
After receiving the Binding Acknowledgement for its Binding Update to its home agent, the mobile node MUST multicast onto the home link (to the all-nodes multicast address) a Neighbor Advertisement [12], to advertise the mobile node's own link-layer address for its own home address. The Target Address in this Neighbor Advertisement MUST be set to the mobile node's home address, and the Advertisement MUST include a Target Link-layer Address option specifying the mobile node's link-layer address. **The mobile node MUST multicast such a Neighbor Advertisement for each of its home addresses, as defined by the current on-link prefixes, including its link-local address and site-local address. The Solicited Flag (S) in these Advertisements MUST NOT be set, since they were not solicited by any Neighbor Solicitation.** The Override Flag (O) in these Advertisements MUST be set, indicating that the Advertisements SHOULD override any existing Neighbor Cache entries at any node receiving them.

Identifier: RQ_001_1707
RFC Clause: 11.5.4
Type: Recommendation
Applies to: Node

Requirement:
On receipt of the Neighbor Advertisement, with the Override Flag (O) set, the Advertisements SHOULD override any existing Neighbor Cache entries at any node receiving them.

RFC Text:
After receiving the Binding Acknowledgement for its Binding Update to its home agent, the mobile node MUST multicast onto the home link (to the all-nodes multicast address) a Neighbor Advertisement [12], to advertise the mobile node's own link-layer address for its own home address. The Target Address in this Neighbor Advertisement MUST be set to the mobile node's home address, and the Advertisement MUST include a Target Link-layer Address option specifying the mobile node's link-layer address. The mobile node MUST multicast such a Neighbor Advertisement for each of its home addresses, as defined by the current on-link prefixes, including its link-local address and site-local address. The Solicited Flag (S) in these Advertisements MUST NOT be set, since they were not solicited by any Neighbor Solicitation. **The Override Flag (O) in these Advertisements MUST be set, indicating that the Advertisements SHOULD override any existing Neighbor Cache entries at any node receiving them.**

Identifier: RQ_001_1708
RFC Clause: 11.5.4
Type: Optional
Applies to: Mobile_Node

Requirement:
Since multicasting on the local link (such as Ethernet) is typically not guaranteed to be reliable, the mobile node MAY retransmit these Neighbor Advertisements [12] up to MAX_NEIGHBOR_ADVERTISEMENT times to increase their reliability.

RFC Text:
Since multicasting on the local link (such as Ethernet) is typically not guaranteed to be reliable, the mobile node MAY retransmit these Neighbor Advertisements [12] up to MAX_NEIGHBOR_ADVERTISEMENT times to increase their reliability. It is still possible that some nodes on the home link will not receive any of these Neighbor Advertisements, but these nodes will eventually be able to recover through use of Neighbor Unreachability Detection [12].

Identifier: RQ_001_1709
RFC Clause: 11.6.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Unless the mobile node has recently received one or both home or care-of keygen tokens, and associated nonce indices for the desired addresses, a mobile node that initiates a return routability procedure MUST send (in parallel) a Home Test Init message and a Care-of Test Init messages.

RFC Text:
A mobile node that initiates a return routability procedure MUST send (in parallel) a Home Test Init message and a Care-of Test Init messages. However, if the mobile node has recently received (see Section 5.2.7) one or both home or care-of keygen tokens, and associated nonce indices for the desired addresses, it MAY reuse them. Therefore, the return routability procedure may in some cases be completed with only one message pair. It may even be completed without any messages at all, if the mobile node has a recent home keygen token and has previously visited the same care-of address so that it also has a recent care-of keygen token. If the mobile node intends to send a Binding Update with the Lifetime set to zero and the care-of address equal to its home address - such as when returning home - sending a Home Test Init message is sufficient. In this case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5).

Identifier: RQ_001_1710
RFC Clause: 11.6.1
Type: Optional
Applies to: Mobile_Node

Requirement:
If the mobile node has recently received one or both home or care-of keygen tokens, and associated nonce indices for the desired addresses, it MAY reuse them.

RFC Text:
A mobile node that initiates a return routability procedure MUST send (in parallel) a Home Test Init message and a Care-of Test Init messages. **However, if the mobile node has recently received (see Section 5.2.7) one or both home or care-of keygen tokens, and associated nonce indices for the desired addresses, it MAY reuse them.** Therefore, the return routability procedure may in some cases be completed with only one message pair. It may even be completed without any messages at all, if the mobile node has a recent home keygen token and has previously visited the same care-of address so that it also has a recent care-of keygen token. If the mobile node intends to send a Binding Update with the Lifetime set to zero and the care-of address equal to its home address - such as when returning home - sending a Home Test Init message is sufficient. In this case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5).

Identifier: RQ_001_1711
RFC Clause: 11.6.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
A Home Test Init message MUST be created as described in Section 6.1.3.

RFC Text:
A Home Test Init message MUST be created as described in Section 6.1.3.

Identifier: RQ_001_1712
RFC Clause: 11.6.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
A Care-of Test Init message MUST be created as described in RFC3775 Section 6.1.4.

RFC Text:
A Care-of Test Init message MUST be created as described in Section 6.1.4. When sending a Home Test Init or Care-of Test Init message the mobile node MUST record in its Binding Update List the following fields from the messages:

o The IP address of the node to which the message was sent.

o The home address of the mobile node. This value will appear in the Source Address field of the Home Test Init message. When sending the Care-of Test Init message, this address does not appear in the message, but represents the home address for which the binding is desired.

o The time at which each of these messages was sent.

o The cookies used in the messages.

Note that a single Care-of Test Init message may be sufficient even when there are multiple home addresses. In this case the mobile node MAY record the same information in multiple Binding Update List entries.

Identifier: RQ_001_1713
RFC Clause: 11.6.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When sending a Home Test Init or Care-of Test Init message the mobile node MUST record in its Binding Update List the following fields from the messages:

o The IP address of the node to which the message was sent.

o The home address of the mobile node. This value will appear in the Source Address field of the Home Test Init message. When sending the Care-of Test Init message, this address does not appear in the message, but represents the home address for which the binding is desired.

o The time at which each of these messages was sent.

o The cookies used in the messages.

RFC Text:
A Care-of Test Init message MUST be created as described in Section 6.1.4. **When sending a Home Test Init or Care-of Test Init message the mobile node MUST record in its Binding Update List the following fields from the messages:**

o The IP address of the node to which the message was sent.

o The home address of the mobile node. This value will appear in the Source Address field of the Home Test Init message. When sending the Care-of Test Init message, this address does not appear in the message, but represents the home address for which the binding is desired.

o The time at which each of these messages was sent.

o The cookies used in the messages.

Note that a single Care-of Test Init message may be sufficient even when there are multiple home addresses. In this case the mobile node MAY record the same information in multiple Binding Update List entries.

Identifier: RQ_001_1714
RFC Clause: 11.6.1
Type: Optional
Applies to: Mobile_Node

Requirement:
When there are multiple home addresses the mobile node MAY record the same information in multiple Binding Update List entries.

RFC Text:
A Care-of Test Init message MUST be created as described in Section 6.1.4. When sending a Home Test Init or Care-of Test Init message the mobile node MUST record in its Binding Update List the following fields from the messages:

- The IP address of the node to which the message was sent.
- The home address of the mobile node. This value will appear in the Source Address field of the Home Test Init message. When sending the Care-of Test Init message, this address does not appear in the message, but represents the home address for which the binding is desired.
- The time at which each of these messages was sent.
- The cookies used in the messages.

Note that a single Care-of Test Init message may be sufficient even when there are multiple home addresses. In this case the mobile node MAY record the same information in multiple Binding Update List entries.

Identifier: RQ_001_1715
RFC Clause: 11.6.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

Upon receiving a packet carrying a Home Test message, a mobile node MUST validate the packet according to the following tests:

o The Source Address of the packet belongs to a correspondent node for which the mobile node has a Binding Update List entry with a state indicating that return routability procedure is in progress. Note that there may be multiple such entries.

o The Binding Update List indicates that no home keygen token has been received yet.

o The Destination Address of the packet has the home address of the mobile node, and the packet has been received in a tunnel from the home agent.

o The Home Init Cookie field in the message matches the value stored in the Binding Update List.

RFC Text:

Upon receiving a packet carrying a Home Test message, a mobile node MUST validate the packet according to the following tests:

o The Source Address of the packet belongs to a correspondent node for which the mobile node has a Binding Update List entry with a state indicating that return routability procedure is in progress. Note that there may be multiple such entries.

o The Binding Update List indicates that no home keygen token has been received yet.

o The Destination Address of the packet has the home address of the mobile node, and the packet has been received in a tunnel from the home agent.

o The Home Init Cookie field in the message matches the value stored in the Binding Update List.

Identifier: RQ_001_1716
RFC Clause: 11.6.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

Any non valid Home Test message received MUST be silently ignored.

RFC Text:

Upon receiving a packet carrying a Home Test message, a mobile node MUST validate the packet according to the following tests:

o The Source Address of the packet belongs to a correspondent node for which the mobile node has a Binding Update List entry with a state indicating that return routability procedure is in progress. Note that there may be multiple such entries.

o The Binding Update List indicates that no home keygen token has been received yet.

o The Destination Address of the packet has the home address of the mobile node, and the packet has been received in a tunnel from the home agent.

o The Home Init Cookie field in the message matches the value stored in the Binding Update List.

Any Home Test message not satisfying all of these tests MUST be silently ignored.

Identifier: RQ_001_1717
RFC Clause: 11.6.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
On receipt of a valid Home Test message, the mobile node MUST record the Home Nonce Index and home keygen token in the Binding Update List.

RFC Text:
Upon receiving a packet carrying a Home Test message, a mobile node MUST validate the packet according to the following tests:

- The Source Address of the packet belongs to a correspondent node for which the mobile node has a Binding Update List entry with a state indicating that return routability procedure is in progress. Note that there may be multiple such entries.
- The Binding Update List indicates that no home keygen token has been received yet.
- The Destination Address of the packet has the home address of the mobile node, and the packet has been received in a tunnel from the home agent.
- The Home Init Cookie field in the message matches the value stored in the Binding Update List.

Any Home Test message not satisfying all of these tests MUST be silently ignored. **Otherwise, the mobile node MUST record the Home Nonce Index and home keygen token in the Binding Update List.** If the Binding Update List entry does not have a care-of keygen token, the mobile node SHOULD continue waiting for the Care-of Test message.

Identifier: RQ_001_1718
RFC Clause: 11.6.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
On receipt of a validated Home Test message, if the Binding Update List entry does not have a care-of keygen token, the mobile node SHOULD continue waiting for the Care-of Test message.

RFC Text:
Upon receiving a packet carrying a Home Test message, a mobile node MUST validate the packet according to the following tests:

- The Source Address of the packet belongs to a correspondent node for which the mobile node has a Binding Update List entry with a state indicating that return routability procedure is in progress. Note that there may be multiple such entries.
- The Binding Update List indicates that no home keygen token has been received yet.
- The Destination Address of the packet has the home address of the mobile node, and the packet has been received in a tunnel from the home agent.
- The Home Init Cookie field in the message matches the value stored in the Binding Update List.

Any Home Test message not satisfying all of these tests MUST be silently ignored. Otherwise, the mobile node MUST record the Home Nonce Index and home keygen token in the Binding Update List. **If the Binding Update List entry does not have a care-of keygen token, the mobile node SHOULD continue waiting for the Care-of Test message.**

Identifier: RQ_001_1719
RFC Clause: 11.6.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Upon receiving a packet carrying a Care-of Test message, a mobile node MUST validate the packet according to the following tests:

o The Source Address of the packet belongs to a correspondent node for which the mobile node has a Binding Update List entry with a state indicating that return routability procedure is in progress. Note that there may be multiple such entries.

o The Binding Update List indicates that no care-of keygen token has been received yet.

o The Destination Address of the packet is the current care-of address of the mobile node.

o The Care-of Init Cookie field in the message matches the value stored in the Binding Update List.

RFC Text:
Upon receiving a packet carrying a Care-of Test message, a mobile node MUST validate the packet according to the following tests:

o The Source Address of the packet belongs to a correspondent node for which the mobile node has a Binding Update List entry with a state indicating that return routability procedure is in progress. Note that there may be multiple such entries.

o The Binding Update List indicates that no care-of keygen token has been received yet.

o The Destination Address of the packet is the current care-of address of the mobile node.

o The Care-of Init Cookie field in the message matches the value stored in the Binding Update List.

Identifier: RQ_001_1720
RFC Clause: 11.6.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Any non-valid Care-of Test message MUST be silently ignored.

RFC Text:
Any Care-of Test message not satisfying all of these tests MUST be silently ignored. Otherwise, the mobile node MUST record the Care-of Nonce Index and care-of keygen token in the Binding Update List. If the Binding Update List entry does not have a home keygen token, the mobile node SHOULD continue waiting for the Home Test message.

Identifier: RQ_001_1721
RFC Clause: 11.6.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
On receipt of a validated Care-of Test message , the mobile node MUST record the Care-of Nonce Index and care-of keygen token in the Binding Update List.

RFC Text:
Any Care-of Test message not satisfying all of these tests MUST be silently ignored. **Otherwise, the mobile node MUST record the Care-of Nonce Index and care-of keygen token in the Binding Update List.** If the Binding Update List entry does not have a home keygen token, the mobile node SHOULD continue waiting for the Home Test message.

Identifier: RQ_001_1722
RFC Clause: 11.6.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
On receipt of a validated Care-of Test message, if the Binding Update List entry does not have a home keygen token, the mobile node SHOULD continue waiting for the Home Test message.

RFC Text:
Any Care-of Test message not satisfying all of these tests MUST be silently ignored. Otherwise, the mobile node MUST record the Care-of Nonce Index and care-of keygen token in the Binding Update List. **If the Binding Update List entry does not have a home keygen token, the mobile node SHOULD continue waiting for the Home Test message.**

Identifier: RQ_001_1723
RFC Clause: 11.6.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
Once the return routability procedure is complete, the mobile node SHOULD then proceed with sending a Binding Update.

RFC Text:
If after receiving either the Home Test or the Care-of Test message and performing the above actions, the Binding Update List entry has both the home and the care-of keygen tokens, the return routability procedure is complete. The mobile node SHOULD then proceed with sending a Binding Update as described in Section 11.7.2.

Identifier: RQ_001_1724
RFC Clause: 11.6.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The mobile node SHOULD, on receipt of with an ICMP Parameter Problem code 1, in responce to Home Test Init and Care-of Test Init messages, take such messages as an indication that the correspondent node cannot provide route optimization, and revert back to the use of bidirectional tunneling.

RFC Text:
Correspondent nodes from the time before this specification was published may not support the Mobility Header protocol. These nodes will respond to Home Test Init and Care-of Test Init messages with an ICMP Parameter Problem code 1. The mobile node SHOULD take such messages as an indication that the correspondent node cannot provide route optimization, and revert back to the use of bidirectional tunneling.

Identifier: RQ_001_1725
RFC Clause: 11.6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The mobile node MUST support the protection of Home Test and Home Test Init messages as described in RFC3775 Section 10.4.6.

RFC Text:
The mobile node MUST support the protection of Home Test and Home Test Init messages as described in Section 10.4.6.

Identifier: RQ_001_1726
RFC Clause: 11.6.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When IPsec is used to protect return routability signaling or payload packets, the mobile node MUST set the source address it uses for the outgoing tunnel packets to the current primary care-of address.

RFC Text:
When IPsec is used to protect return routability signaling or payload packets, the mobile node MUST set the source address it uses for the outgoing tunnel packets to the current primary care-of address. The mobile node starts to use a new primary care-of address immediately after sending a Binding Update to the home agent to register this new address.

Identifier: RQ_001_1727
RFC Clause: 11.7.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
After deciding to change its primary care-of address as described in RFC3775 Section 11.5.1 and 11.5.2, a mobile node MUST register this care-of address with its home agent in order to make this its primary care-of address.

RFC Text:
After deciding to change its primary care-of address as described in Section 11.5.1 and Section 11.5.2, a mobile node MUST register this care-of address with its home agent in order to make this its primary care-of address.

Identifier: RQ_001_1728
RFC Clause: 11.7.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
if the mobile node wants the services of the home agent beyond the current registration period, the mobile node should send a new Binding Update to it well before the expiration of this period,

RFC Text:
Also, if the mobile node wants the services of the home agent beyond the current registration period, the mobile node should send a new Binding Update to it well before the expiration of this period, even if it is not changing its primary care-of address. However, if the home agent returned a Binding Acknowledgement for the current registration with Status field set to 1 (accepted but prefix discovery necessary), the mobile node should not try to register again before it has learned the validity of its home prefixes through mobile prefix discovery. This is typically necessary every time this Status value is received, because information learned earlier may have changed.

Identifier: RQ_001_1729
RFC Clause: 11.7.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the home agent returned a Binding Acknowledgement for the current registration with Status field set to 1 (accepted but prefix discovery necessary), the mobile node should not try to register again before it has learned the validity of its home prefixes through mobile prefix discovery.

RFC Text:
Also, if the mobile node wants the services of the home agent beyond the current registration period, the mobile node should send a new Binding Update to it well before the expiration of this period, even if it is not changing its primary care-of address. **However, if the home agent returned a Binding Acknowledgement for the current registration with Status field set to 1 (accepted but prefix discovery necessary), the mobile node should not try to register again before it has learned the validity of its home prefixes through mobile prefix discovery.** This is typically necessary every time this Status value is received, because information learned earlier may have changed.

Identifier: RQ_001_1730
RFC Clause: 11.7.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:

To register a care-of address or to extend the lifetime of an existing registration, the mobile node sends a packet to its home agent containing a Binding Update, the packet MUST be constructed as follows:

o The Home Registration (H) bit MUST be set in the Binding Update.

o The Acknowledge (A) bit MUST be set in the Binding Update.

o The packet MUST contain a Home Address destination option, giving the mobile node's home address for the binding.

o The care-of address for the binding MUST be used as the Source Address in the packet's IPv6 header, unless an Alternate Care-of Address mobility option is included in the Binding Update. This option MUST be included in all home registrations.

o If the home address was generated using RFC 3041 [18], then the link local address is unlikely to have a compatible interface identifier. In this case, the mobile node MUST clear the Link-Local Address Compatibility (L) bit.

o If the IPsec security associations between the mobile node and the home agent have NOT been established dynamically or the mobile node
does not have the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves, the Binding Update MUST clear the Key Management Mobility Capability (K) bit.

RFC Text:

To register a care-of address or to extend the lifetime of an existing registration, the mobile node sends a packet to its home agent containing a Binding Update, with the packet constructed as follows:

o The Home Registration (H) bit MUST be set in the Binding Update.

o The Acknowledge (A) bit MUST be set in the Binding Update.

o The packet MUST contain a Home Address destination option, giving the mobile node's home address for the binding.

o The care-of address for the binding MUST be used as the Source Address in the packet's IPv6 header, unless an Alternate Care-of Address mobility option is included in the Binding Update. This option MUST be included in all home registrations, as the ESP protocol will not be able to protect care-of addresses in the IPv6 header. (Mobile IPv6 implementations that know they are using IPsec AH to protect a particular message might avoid this option. For brevity the usage of AH is not discussed in this document.)}}

o If the mobile node's link-local address has the same interface identifier as the home address for which it is supplying a new care-of address, then the mobile node SHOULD set the Link-Local Address Compatibility (L) bit.

o **If the home address was generated using RFC 3041 [18], then the link local address is unlikely to have a compatible interface identifier. In this case, the mobile node MUST clear the Link-Local Address Compatibility (L) bit.**

o If the IPsec security associations between the mobile node and the home agent have been established dynamically, and the mobile node has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves, the mobile node SHOULD set the Key Management Mobility Capability (K) bit in the Binding Update. **Otherwise, the mobile node MUST clear the bit.**

o The value specified in the Lifetime field MUST be non-zero and SHOULD be less than or equal to the remaining valid lifetime of the home address and the care-of address specified for the binding.

Mobile nodes that use dynamic home agent address discovery should
be careful with long lifetimes. If the mobile node loses the
knowledge of its binding with a specific home agent, registering a
new binding with another home agent may be impossible as the
previous home agent is still defending the existing binding.
Therefore, to ensure that mobile nodes using home agent address
discovery do not lose information about their binding, they SHOULD
de-register before losing this information, or use small
lifetimes.

Identifier: RQ_001_1731
RFC Clause: 11.7.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:

To register a care-of address or to extend the lifetime of an existing registration, the mobile node sends a packet to its home agent containing a Binding Update, the packet SHOULD be constructed as follows:

o If the mobile node's link-local address has the same interface identifier as the home address for which it is supplying a new care-of address, then the mobile node SHOULD set the Link-Local Address Compatibility (L) bit.

o If the IPsec security associations between the mobile node and the home agent have been established dynamically, and the mobile node has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves, the mobile node SOULD set the Key Management Mobility Capability (K) bit in the Binding Update.

o The value specified in the Lifetime field MUST be non-zero and SHOULD be less than or equal to the remaining valid lifetime of the home address and the care-of address specified for the binding.

RFC Text:

To register a care-of address or to extend the lifetime of an existing registration, the mobile node sends a packet to its home agent containing a Binding Update, with the packet constructed as follows:

o The Home Registration (H) bit MUST be set in the Binding Update.

o The Acknowledge (A) bit MUST be set in the Binding Update.

o The packet MUST contain a Home Address destination option, giving the mobile node's home address for the binding.

o The care-of address for the binding MUST be used as the Source Address in the packet's IPv6 header, unless an Alternate Care-of Address mobility option is included in the Binding Update. This option MUST be included in all home registrations, as the ESP protocol will not be able to protect care-of addresses in the IPv6 header. (Mobile IPv6 implementations that know they are using IPsec AH to protect a particular message might avoid this option. For brevity the usage of AH is not discussed in this document.)

o If the mobile node's link-local address has the same interface identifier as the home address for which it is supplying a new care-of address, then the mobile node SHOULD set the Link-Local Address Compatibility (L) bit.

o If the home address was generated using RFC 3041 [18], then the link local address is unlikely to have a compatible interface identifier. In this case, the mobile node MUST clear the Link-Local Address Compatibility (L) bit.

o If the IPsec security associations between the mobile node and the home agent have been established dynamically, and the mobile node has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves, the mobile node SHOULD set the Key Management Mobility Capability (K) bit in the Binding Update. Otherwise, the mobile node MUST clear the bit.

o The value specified in the Lifetime field MUST be non-zero and SHOULD be less than or equal to the remaining valid lifetime of the home address and the care-of address specified for the binding.

Mobile nodes that use dynamic home agent address discovery should be careful with long lifetimes. If the mobile node loses the knowledge of its binding with a specific home agent, registering a new binding with another home agent may be impossible as the previous home agent is still defending the existing binding. Therefore, to ensure that mobile nodes using home agent address discovery do not lose information about their binding, they SHOULD de-register before losing this information, or use small lifetimes.

Identifier: RQ_001_1732
RFC Clause: 11.7.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
To ensure that mobile nodes using home agent address discovery do not lose information about their binding, they SHOULD de-register before losing this information, or use small lifetimes.

RFC Text:
To register a care-of address or to extend the lifetime of an existing registration, the mobile node sends a packet to its home agent containing a Binding Update, with the packet constructed as follows:

- The Home Registration (H) bit MUST be set in the Binding Update.
- The Acknowledge (A) bit MUST be set in the Binding Update.
- The packet MUST contain a Home Address destination option, giving the mobile node's home address for the binding.
- The care-of address for the binding MUST be used as the Source Address in the packet's IPv6 header, unless an Alternate Care-of Address mobility option is included in the Binding Update. This option MUST be included in all home registrations, as the ESP protocol will not be able to protect care-of addresses in the IPv6 header. (Mobile IPv6 implementations that know they are using IPsec AH to protect a particular message might avoid this option. For brevity the usage of AH is not discussed in this document.)
- If the mobile node's link-local address has the same interface identifier as the home address for which it is supplying a new care-of address, then the mobile node SHOULD set the Link-Local Address Compatibility (L) bit.
- If the home address was generated using RFC 3041 [18], then the link local address is unlikely to have a compatible interface identifier. In this case, the mobile node MUST clear the Link-Local Address Compatibility (L) bit.
- If the IPsec security associations between the mobile node and the home agent have been established dynamically, and the mobile node has the capability to update its endpoint in the used key management protocol to the new care-of address every time it moves, the mobile node SHOULD set the Key Management Mobility Capability (K) bit in the Binding Update. Otherwise, the mobile node MUST clear the bit.
- The value specified in the Lifetime field MUST be non-zero and SHOULD be less than or equal to the remaining valid lifetime of the home address and the care-of address specified for the binding.

Mobile nodes that use dynamic home agent address discovery should be careful with long lifetimes. If the mobile node loses the knowledge of its binding with a specific home agent, registering a new binding with another home agent may be impossible as the previous home agent is still defending the existing binding. Therefore, to ensure that mobile nodes using home agent address discovery do not lose information about their binding, they SHOULD de-register before losing this information, or use small lifetimes.

Identifier: RQ_001_1733
RFC Clause: 11.7.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a Mobile Node sends a Binding Update to its Home Agent with the Acknowledge (A) bit set, it SHOULD retransmit this Binding Update to its Home Agent until it receives a matching Binding Acknowledgement.

RFC Text:
The Acknowledge (A) bit in the Binding Update requests the home agent to return a Binding Acknowledgement in response to this Binding Update. **As described in Section 6.1.8, the mobile node SHOULD retransmit this Binding Update to its home agent until it receives a matching Binding Acknowledgement.** Once reaching a retransmission timeout period of MAX_BINDACK_TIMEOUT, the mobile node SHOULD restart the process of delivering the Binding Update, but trying instead the next home agent returned during dynamic home agent address discovery (see Section 11.4.1). If there was only one home agent, the mobile node instead SHOULD continue to periodically retransmit the Binding Update at this rate until acknowledged (or until it begins attempting to register a different primary care-of address). See Section 11.8 for information about retransmitting Binding Updates.

Identifier: RQ_001_1734
RFC Clause: 11.7.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Mobile Node knows several Home Agents and reaches the MAX_BINDACK_TIMEOUT retransmission timeout period, the mobile node SHOULD restart the process of delivering the Binding Update with the next known home agent (returned during Dynamic Home Agent Address Discovery).

RFC Text:
The Acknowledge (A) bit in the Binding Update requests the home agent to return a Binding Acknowledgement in response to this Binding Update. As described in Section 6.1.8, the mobile node SHOULD retransmit this Binding Update to its home agent until it receives a matching Binding Acknowledgement. **Once reaching a retransmission timeout period of MAX_BINDACK_TIMEOUT, the mobile node SHOULD restart the process of delivering the Binding Update, but trying instead the next home agent returned during dynamic home agent address discovery (see Section 11.4.1). If there was only one home agent, the mobile node instead SHOULD continue to periodically retransmit the Binding Update at this rate until acknowledged (or until it begins attempting to register a different primary care-of address). See Section 11.8 for information about retransmitting Binding Updates.**

Identifier: RQ_001_1735
RFC Clause: 11.7.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Each Binding Update MUST be authenticated as coming from the right mobile node.

RFC Text:
Each Binding Update MUST be authenticated as coming from the right mobile node, as defined in Section 5.1. The mobile node MUST use its home address - either in the Home Address destination option or in the Source Address field of the IPv6 header - in Binding Updates sent to the home agent. This is necessary in order to allow the IPsec policies to be matched with the correct home address.

Identifier: RQ_001_1736
RFC Clause: 11.7.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The mobile node MUST use its home address - either in the Home Address destination option or in the Source Address field of the IPv6 header - in Binding Updates sent to the home agent.

RFC Text:
Each Binding Update MUST be authenticated as coming from the right mobile node, as defined in Section 5.1. **The mobile node MUST use its home address - either in the Home Address destination option or in the Source Address field of the IPv6 header - in Binding Updates sent to the home agent.** This is necessary in order to allow the IPsec policies to be matched with the correct home address.

Identifier: RQ_001_1737
RFC Clause: 11.7.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When sending a Binding Update to its home agent, the mobile node MUST also create or update the corresponding Binding Update List entry (as specified in RFC3775 Section 11.7.2.)

RFC Text:
When sending a Binding Update to its home agent, the mobile node MUST also create or update the corresponding Binding Update List entry, as specified in Section 11.7.2.

Identifier: RQ_001_1738
RFC Clause: 11.7.1
Type: Optional
Applies to: Mobile_Node

Requirement:
If the sending mobile node has no knowledge of the correct Sequence Number value, it may start at any value.

RFC Text:
The last Sequence Number value sent to the home agent in a Binding Update is stored by the mobile node. **If the sending mobile node has no knowledge of the correct Sequence Number value, it may start at any value.** If the home agent rejects the value, it sends back a Binding Acknowledgement with a status code 135, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement. The mobile node MUST store this information and use the next Sequence Number value for the next Binding Update it sends.

Identifier: RQ_001_1739
RFC Clause: 11.7.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the home agent rejects the Sequence Number value, it sends back a Binding Acknowledgement with a status code 135, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement. The mobile node MUST store the last Sequence Number value sent to the home agent and use the next Sequence Number value for the next Binding Update it sends.

RFC Text:
The last Sequence Number value sent to the home agent in a Binding Update is stored by the mobile node. **If the sending mobile node has no knowledge of the correct Sequence Number value, it may start at any value. If the home agent rejects the value, it sends back a Binding Acknowledgement with a status code 135, and the last accepted sequence number in the Sequence Number field of the Binding Acknowledgement. The mobile node MUST store this information and use the next Sequence Number value for the next Binding Update it sends.**

Identifier: RQ_001_1740
RFC Clause: 11.7.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the mobile node has additional home addresses, then the mobile node SHOULD send an additional packet containing a Binding Update to its home agent to register the care-of address for each such other home address.

RFC Text:
If the mobile node has additional home addresses, then the mobile node SHOULD send an additional packet containing a Binding Update to its home agent to register the care-of address for each such other home address.

Identifier: RQ_001_1741
RFC Clause: 11.7.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The mobile node MUST treat the creation of a new binding with the home agent using an existing home address, the same as creation of a new home address.

RFC Text:
The home agent will only perform DAD for the mobile node's home address when the mobile node has supplied a valid binding between its home address and a care-of address. If some time elapses during which the mobile node has no binding at the home agent, it might be possible for another node to autoconfigure the mobile node's home address. **Therefore, the mobile node MUST treat the creation of a new binding with the home agent using an existing home address, the same as creation of a new home address.** In the unlikely event that the mobile node's home address is autoconfigured as the IPv6 address of another network node on the home network, the home agent will reply to the mobile node's subsequent Binding Update with a Binding Acknowledgement containing a Status of 134 (Duplicate Address Detection failed). In this case, the mobile node MUST NOT attempt to re-use the same home address. It SHOULD continue to register the care-of addresses for its other home addresses, if any. (Mechanisms outlined in Appendix B.5 may in the future allow mobile nodes to acquire new home addresses to replace the one for which Status 134 was received.)

Identifier: RQ_001_1742
RFC Clause: 11.7.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When the mobile node's home address is alredy used by another node on the home network, the home agent will reply to the mobile node's subsequent Binding Update with a Binding Acknowledgement containing a Status of 134 (Duplicate Address Detection failed). In this case, the mobile node MUST NOT attempt to re-use the same home address.

RFC Text:
The home agent will only perform DAD for the mobile node's home address when the mobile node has supplied a valid binding between its home address and a care-of address. If some time elapses during which the mobile node has no binding at the home agent, it might be possible for another node to autoconfigure the mobile node's home address. Therefore, the mobile node MUST treat the creation of a new binding with the home agent using an existing home address, the same as creation of a new home address. **In the unlikely event that the mobile node's home address is autoconfigured as the IPv6 address of another network node on the home network, the home agent will reply to the mobile node's subsequent Binding Update with a Binding Acknowledgement containing a Status of 134 (Duplicate Address Detection failed). In this case, the mobile node MUST NOT attempt to re-use the same home address.** It SHOULD continue to register the care-of addresses for its other home addresses, if any. (Mechanisms outlined in Appendix B.5 may in the future allow mobile nodes to acquire new home addresses to replace the one for which Status 134 was received.)

Identifier: RQ_001_1743
RFC Clause: 11.7.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node's home address is alredy used by another node on the home network, the home agent will reply to the mobile node's subsequent Binding Update with a Binding Acknowledgement containing a Status of 134 (Duplicate Address Detection failed). In this case, the mobile node SHOULD continue to register the care-of addresses for its other home addresses, if any.

RFC Text:
The home agent will only perform DAD for the mobile node's home address when the mobile node has supplied a valid binding between its home address and a care-of address. If some time elapses during which the mobile node has no binding at the home agent, it might be possible for another node to autoconfigure the mobile node's home address. Therefore, the mobile node MUST treat the creation of a new binding with the home agent using an existing home address, the same as creation of a new home address. In the unlikely event that the mobile node's home address is autoconfigured as the IPv6 address of another network node on the home network, the home agent will reply to the mobile node's subsequent Binding Update with a Binding Acknowledgement containing a Status of 134 (Duplicate Address Detection failed). In this case, the mobile node MUST NOT attempt to re-use the same home address. **It SHOULD continue to register the care-of addresses for its other home addresses, if any. (Mechanisms outlined in Appendix B.5 may in the future allow mobile nodes to acquire new home addresses to replace the one for which Status 134 was received.)**

Identifier: RQ_001_1744
RFC Clause: 11.7.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
After the mobile node has sent a Binding Update to its home agent, registering a new primary care-of address, the mobile node SHOULD initiate a correspondent registration for each node that already appears in the mobile node's Binding Update List.

RFC Text:
After the mobile node has sent a Binding Update to its home agent, registering a new primary care-of address (as described in Section 11.7.1), the mobile node SHOULD initiate a correspondent registration for each node that already appears in the mobile node's Binding Update List. The initiated procedures can be used to either update or delete binding information in the correspondent node.

Identifier: RQ_001_1745
RFC Clause: 11.7.2
Type: Optional
Applies to: Mobile_Node

Requirement:
For nodes that do not appear in the mobile node's Binding Update List, the mobile node MAY initiate a correspondent registration at any time after sending the Binding Update to its home agent.

RFC Text:
For nodes that do not appear in the mobile node's Binding Update List, the mobile node MAY initiate a correspondent registration at any time after sending the Binding Update to its home agent.

Identifier: RQ_001_1746
RFC Clause: 11.7.2
Type: Optional
Applies to: Mobile_Node

Requirement:
The mobile node MAY initiate the correspondent registration in response to receiving a packet that meets all of the following tests:

o The packet was tunneled using IPv6 encapsulation.

o The Destination Address in the tunnel (outer) IPv6 header is equal to any of the mobile node's care-of addresses.

o The Destination Address in the original (inner) IPv6 header is equal to one of the mobile node's home addresses.

o The Source Address in the tunnel (outer) IPv6 header differs from the Source Address in the original (inner) IPv6 header.

o The packet does not contain a Home Test, Home Test Init, Care-of Test, or Care-of Test Init message.

RFC Text:
In addition, the mobile node MAY initiate the correspondent registration in response to receiving a packet that meets all of the following tests:

o The packet was tunneled using IPv6 encapsulation.

o The Destination Address in the tunnel (outer) IPv6 header is equal to any of the mobile node's care-of addresses.

o The Destination Address in the original (inner) IPv6 header is equal to one of the mobile node's home addresses.

o The Source Address in the tunnel (outer) IPv6 header differs from the Source Address in the original (inner) IPv6 header.

o The packet does not contain a Home Test, Home Test Init, Care-of Test, or Care-of Test Init message.

Identifier: RQ_001_1747
RFC Clause: 11.7.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If a mobile node has multiple home addresses, the used home address MUST be the Destination Address of the original (inner) packet.

RFC Text:
If a mobile node has multiple home addresses, it becomes important to select the right home address to use in the correspondent registration. The used home address MUST be the Destination Address of the original (inner) packet.

Identifier: RQ_001_1748
RFC Clause: 11.7.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The peer address used in the correspondant registration procedure MUST be determined as follows:

- o If a Home Address destination option is present in the original (inner) packet, the address from this option is used.
- o Otherwise, the Source Address in the original (inner) IPv6 header of the packet is used.

RFC Text:
The peer address used in the procedure MUST be determined as follows:

- **o If a Home Address destination option is present in the original (inner) packet, the address from this option is used.**
- **o Otherwise, the Source Address in the original (inner) IPv6 header of the packet is used.**

Identifier: RQ_001_1749
RFC Clause: 11.7.2
Type: Optional
Applies to: Mobile_Node

Requirement:
A mobile node MAY also choose to keep its topological location private from certain correspondent nodes, and thus need not initiate the correspondent registration.

RFC Text:
A mobile node MAY also choose to keep its topological location private from certain correspondent nodes, and thus need not initiate the correspondent registration.

Identifier: RQ_001_1750
RFC Clause: 11.7.2
Type: Optional
Applies to: Mobile_Node

Requirement:
Upon successfully completing the return routability procedure, and after receiving a successful Binding Acknowledgement from the Home Agent, a Binding Update MAY be sent to the correspondent node.

RFC Text:
Upon successfully completing the return routability procedure, and after receiving a successful Binding Acknowledgement from the Home Agent, a Binding Update MAY be sent to the correspondent node.

Identifier: RQ_001_1751
RFC Clause: 11.7.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In any Binding Update sent by a mobile node, the care-of address (either the Source Address in the packet's IPv6 header or the Care-of Address in the Alternate Care-of Address mobility option of the Binding Update) MUST be set to one of the care-of addresses currently in use by the mobile node or to the mobile node's home address.

RFC Text:
In any Binding Update sent by a mobile node, the care-of address (either the Source Address in the packet's IPv6 header or the Care-of Address in the Alternate Care-of Address mobility option of the Binding Update) MUST be set to one of the care-of addresses currently in use by the mobile node or to the mobile node's home address. A mobile node MAY set the care-of address differently for sending Binding Updates to different correspondent nodes.

Identifier: RQ_001_1752
RFC Clause: 11.7.2
Type: Optional
Applies to: Mobile_Node

Requirement:
A mobile node MAY set the care-of address differently for sending Binding Updates to different correspondent nodes.

RFC Text:
In any Binding Update sent by a mobile node, the care-of address (either the Source Address in the packet's IPv6 header or the Care-of Address in the Alternate Care-of Address mobility option of the Binding Update) MUST be set to one of the care-of addresses currently in use by the mobile node or to the mobile node's home address. **A mobile node MAY set the care-of address differently for sending Binding Updates to different correspondent nodes.**

Identifier: RQ_001_1753
RFC Clause: 11.7.2
Type: Optional
Applies to: Mobile_Node

Requirement:
A mobile node MAY send a Binding Update to a correspondent node, instructing it to delete any existing binding for the mobile node from its Binding Cache.

RFC Text:
A mobile node MAY also send a Binding Update to such a correspondent node, instructing it to delete any existing binding for the mobile node from its Binding Cache, as described in Section 6.1.7.
Even in this case a successful completion of the return routability procedure is required first.

Identifier: RQ_001_1754
RFC Clause: 11.7.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
A successful completion of the return routability procedure is required before a mobile node sends a Binding Update to a correspondent node instructing it to delete any existing binding for the mobile node from its Binding Cache."

RFC Text:
A mobile node MAY also send a Binding Update to such a correspondent node, instructing it to delete any existing binding for the mobile node from its Binding Cache, as described in Section 6.1.7.
Even in this case a successful completion of the return routability procedure is required first.

Identifier: RQ_001_1755
RFC Clause: 11.7.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
In the case where the care-of address is not set to the mobile node's home address, the value specified in the Lifetime field sent in the Binding Update SHOULD be less than or equal to the remaining lifetime of the home registration and the care-of address specified for the binding.

RFC Text:
If the care-of address is not set to the mobile node's home address, the Binding Update requests that the correspondent node create or update an entry for the mobile node in the correspondent node's Binding Cache. This is done in order to record a care-of address for use in sending future packets to the mobile node. In this case, the value specified in the Lifetime field sent in the Binding Update SHOULD be less than or equal to the remaining lifetime of the home registration and the care-of address specified for the binding. The care-of address given in the Binding Update MAY differ from the mobile node's primary care-of address.

Identifier: RQ_001_1756
RFC Clause: 11.7.2
Type: Optional
Applies to: Mobile_Node

Requirement:
In the case where the care-of address is not set to the mobile node's home address, the care-of address given in the Binding Update MAY differ from the mobile node's primary care-of address.

RFC Text:
If the care-of address is not set to the mobile node's home address, the Binding Update requests that the correspondent node create or update an entry for the mobile node in the correspondent node's Binding Cache. This is done in order to record a care-of address for use in sending future packets to the mobile node. In this case, the value specified in the Lifetime field sent in the Binding Update SHOULD be less than or equal to the remaining lifetime of the home registration and the care-of address specified for the binding. **The care-of address given in the Binding Update MAY differ from the mobile node's primary care-of address.**

Identifier: RQ_001_1757
RFC Clause: 11.7.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Binding Update is sent to the correspondent node, requesting the deletion of any existing Binding Cache entry it has for the mobile node, the care-of nonce index SHOULD be set to zero.

RFC Text:
If the Binding Update is sent to the correspondent node, requesting the deletion of any existing Binding Cache entry it has for the mobile node, the care-of address is set to the mobile node's home address and the Lifetime field set to zero. In this case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5). The care-of nonce index SHOULD be set to zero in this case. In keeping with the Binding Update creation rules below, the care-of address MUST be set to the home address if the mobile node is at home, or to the current care-of address if it is away from home.

Identifier: RQ_001_1758
RFC Clause: 11.7.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a Mobile Node is sending a Binding Update to a correspondent node, requesting the deletion of any existing Binding Cache entry it has for the Mobile Node, and the Mobile Node is at home: the Mobile Node MUST set the care-of address to its home address.

RFC Text:
If the Binding Update is sent to the correspondent node, requesting the deletion of any existing Binding Cache entry it has for the mobile node, the care-of address is set to the mobile node's home address and the Lifetime field set to zero. In this case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5). The care-of nonce index SHOULD be set to zero in this case. In keeping with the Binding Update creation rules below, **the care-of address MUST be set to the home address if the mobile node is at home**, or to the current care-of address if it is away from home.

Identifier: RQ_001_1759
RFC Clause: 11.7.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
A Binding Update is created as follows:

o The current care-of address of the mobile node MUST be sent either in the Source Address of the IPv6 header, or in the Alternate Care-of Address mobility option.

o The Destination Address of the IPv6 header MUST contain the address of the correspondent node.

o The Mobility Header is constructed according to rules in Section 6.1.7 and Section 5.2.6, including the Binding Authorization Data (calculated as defined in Section 6.2.7) and possibly the Nonce Indices mobility options.

o The home address of the mobile node MUST be added to the packet in a Home Address destination option, unless the Source Address is the home address.

RFC Text:
A Binding Update is created as follows:

- **o The current care-of address of the mobile node MUST be sent either in the Source Address of the IPv6 header, or in the Alternate Care-of Address mobility option.**
- **o The Destination Address of the IPv6 header MUST contain the address of the correspondent node.**
- **o The Mobility Header is constructed according to rules in Section 6.1.7 and Section 5.2.6, including the Binding Authorization Data (calculated as defined in Section 6.2.7) and possibly the Nonce Indices mobility options.**
- **o The home address of the mobile node MUST be added to the packet in a Home Address destination option, unless the Source Address is the home address.**

Identifier: RQ_001_1760
RFC Clause: 11.7.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Each Binding Update MUST have a Sequence Number greater than the Sequence Number value sent in the previous Binding Update to the same destination address (if any).

RFC Text:
Each Binding Update MUST have a Sequence Number greater than the Sequence Number value sent in the previous Binding Update to the same destination address (if any). The sequence numbers are compared modulo 2**16, as described in Section 9.5.1. There is no requirement, however, that the Sequence Number value strictly increase by 1 with each new Binding Update sent or received, as long as the value stays within the window. The last Sequence Number value sent to a destination in a Binding Update is stored by the mobile node in its Binding Update List entry for that destination. If the sending mobile node has no Binding Update List entry, the Sequence Number SHOULD start at a random value. The mobile node MUST NOT use the same Sequence Number in two different Binding Updates to the same correspondent node, even if the Binding Updates provide different care-of addresses.

Identifier: RQ_001_1761
RFC Clause: 11.7.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the sending mobile node has no Binding Update List entry, the Sequence Number SHOULD start at a random value.

RFC Text:
Each Binding Update MUST have a Sequence Number greater than the Sequence Number value sent in the previous Binding Update to the same destination address (if any). The sequence numbers are compared modulo 2**16, as described in Section 9.5.1. There is no requirement, however, that the Sequence Number value strictly increase by 1 with each new Binding Update sent or received, as long as the value stays within the window. The last Sequence Number value sent to a destination in a Binding Update is stored by the mobile node in its Binding Update List entry for that destination. **If the sending mobile node has no Binding Update List entry, the Sequence Number SHOULD start at a random value.** The mobile node MUST NOT use the same Sequence Number in two different Binding Updates to the same correspondent node, even if the Binding Updates provide different care-of addresses.

Identifier: RQ_001_1762
RFC Clause: 11.7.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The mobile node MUST NOT use the same Sequence Number in two different Binding Updates to the same correspondent node, even if the Binding Updates provide different care-of addresses.

RFC Text:
Each Binding Update MUST have a Sequence Number greater than the Sequence Number value sent in the previous Binding Update to the same destination address (if any). The sequence numbers are compared modulo 2**16, as described in Section 9.5.1. There is no requirement, however, that the Sequence Number value strictly increase by 1 with each new Binding Update sent or received, as long as the value stays within the window. The last Sequence Number value sent to a destination in a Binding Update is stored by the mobile node in its Binding Update List entry for that destination. If the sending mobile node has no Binding Update List entry, the Sequence Number SHOULD start at a random value. **The mobile node MUST NOT use the same Sequence Number in two different Binding Updates to the same correspondent node, even if the Binding Updates provide different care-of addresses.**

Identifier: RQ_001_1763
RFC Clause: 11.7.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Upon receiving a packet carrying a Binding Acknowledgement, a mobile node MUST validate the packet according to the following tests:

o The packet meets the authentication requirements for Binding Acknowledgements defined in Section 6.1.8 and Section 5. That is, if the Binding Update was sent to the home agent, underlying IPsec protection is used. If the Binding Update was sent to the correspondent node, the Binding Authorization Data mobility option MUST be present and have a valid value.

o The Binding Authorization Data mobility option, if present, MUST be the last option and MUST not have trailing padding.

o The Sequence Number field matches the Sequence Number sent by the mobile node to this destination address in an outstanding Binding
Update.

RFC Text:
Upon receiving a packet carrying a Binding Acknowledgement, a mobile node MUST validate the packet according to the following tests:

- **The packet meets the authentication requirements for Binding Acknowledgements defined in Section 6.1.8 and Section 5. That is, if the Binding Update was sent to the home agent, underlying IPsec protection is used. If the Binding Update was sent to the correspondent node, the Binding Authorization Data mobility option MUST be present and have a valid value.**

- **The Binding Authorization Data mobility option, if present, MUST be the last option and MUST not have trailing padding.**

- **The Sequence Number field matches the Sequence Number sent by the mobile node to this destination address in an outstanding Binding Update.**

Identifier: RQ_001_1764
RFC Clause: 11.7.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Any Binding Acknowledgement not validated MUST be silently ignored.

RFC Text:
Any Binding Acknowledgement not satisfying all of these tests MUST be silently ignored.

Identifier: RQ_001_1765
RFC Clause: 11.7.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet carrying a valid Binding Acknowledgement, if the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUSTupdate the corresponding entry in its Binding Update List to indicate that the Binding Update has been acknowledged.

RFC Text:
When a mobile node receives a packet carrying a valid Binding Acknowledgement, the mobile node MUST examine the Status field as follows:

- **If the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUST update the corresponding entry in its Binding Update List to indicate that the Binding Update has been acknowledged;** the mobile node MUST then stop retransmitting the Binding Update. In addition, if the value specified in the Lifetime field in the Binding Acknowledgement is less than the Lifetime value sent in the Binding Update being acknowledged, the mobile node MUST subtract the difference between these two Lifetime values from the remaining lifetime for the binding as maintained in the corresponding Binding Update List entry (with a minimum value for the Binding Update List entry lifetime of 0). That is, if the Lifetime value sent in the Binding Update was L_update, the Lifetime value received in the Binding Acknowledgement was L_ack, and the current remaining lifetime of the Binding Update List entry is L_remain, then the new value for the remaining lifetime of the Binding Update List entry should be

  ```
  max((L_remain - (L_update - L_ack)), 0)
  ```

  where max(X, Y) is the maximum of X and Y. The effect of this step is to correctly manage the mobile node's view of the binding's remaining lifetime (as maintained in the corresponding Binding Update List entry) so that it correctly counts down from the Lifetime value given in the Binding Acknowledgement, but with the timer countdown beginning at the time that the Binding Update was sent.

  Mobile nodes SHOULD send a new Binding Update well before the expiration of this period in order to extend the lifetime. This helps to avoid disruptions in communications which might otherwise be caused by network delays or clock drift.

- Additionally, if the Status field value is 1 (accepted but prefix discovery necessary), the mobile node SHOULD send a Mobile Prefix Solicitation message to update its information about the available prefixes.

- If the Status field indicates that the Binding Update was rejected (the Status field is greater than or equal to 128), then the mobile node can take steps to correct the cause of the error and retransmit the Binding Update (with a new Sequence Number value), subject to the rate limiting restriction specified in Section 11.8. If this is not done or it fails, then the mobile node SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination.

Identifier: RQ_001_1766
RFC Clause: 11.7.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet carrying a valid Binding Acknowledgement, if the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUST then stop retransmitting the Binding Update.

RFC Text:
When a mobile node receives a packet carrying a valid Binding Acknowledgement, the mobile node MUST examine the Status field as follows:

o If the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUST update the corresponding entry in its Binding Update List to indicate that the Binding Update has been acknowledged; **the mobile node MUST then stop retransmitting the Binding Update.** In addition, if the value specified in the Lifetime field in the Binding Acknowledgement is less than the Lifetime value sent in the Binding Update being acknowledged, the mobile node MUST subtract the difference between these two Lifetime values from the remaining lifetime for the binding as maintained in the corresponding Binding Update List entry (with a minimum value for the Binding Update List entry lifetime of 0). That is, if the Lifetime value sent in the Binding Update was L_update, the Lifetime value received in the Binding Acknowledgement was L_ack, and the current remaining lifetime of the Binding Update List entry is L_remain, then the new value for the remaining lifetime of the Binding Update List entry should be

max((L_remain - (L_update - L_ack)), 0)

where max(X, Y) is the maximum of X and Y. The effect of this step is to correctly manage the mobile node's view of the binding's remaining lifetime (as maintained in the corresponding Binding Update List entry) so that it correctly counts down from the Lifetime value given in the Binding Acknowledgement, but with the timer countdown beginning at the time that the Binding Update was sent.

Mobile nodes SHOULD send a new Binding Update well before the expiration of this period in order to extend the lifetime. This helps to avoid disruptions in communications which might otherwise be caused by network delays or clock drift.

o Additionally, if the Status field value is 1 (accepted but prefix discovery necessary), the mobile node SHOULD send a Mobile Prefix Solicitation message to update its information about the available prefixes.

o If the Status field indicates that the Binding Update was rejected (the Status field is greater than or equal to 128), then the mobile node can take steps to correct the cause of the error and retransmit the Binding Update (with a new Sequence Number value), subject to the rate limiting restriction specified in Section 11.8. If this is not done or it fails, then the mobile node SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination.

Identifier: RQ_001_1767
RFC Clause: 11.7.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:

When a mobile node receives a packet carrying a valid Binding Acknowledgement, if the value specified in the Lifetime field in the Binding Acknowledgement is less than the Lifetime value sent in the Binding Update being acknowledged, the mobile node MUSTsubtract the difference between these two Lifetime values from the remaining lifetime for the binding as maintained in the corresponding Binding Update List entry (with a minimum value for the Binding Update List entry lifetime of 0).

That is, if the Lifetime value sent in the Binding Update was L_update, the Lifetime value received in the Binding Acknowledgement was L_ack, and the current remaining lifetime of the Binding Update List entry is L_remain, then the new value for the remaining lifetime of the Binding Update List entry should be

max((L_remain - (L_update - L_ack)), 0)

where max(X, Y) is the maximum of X and Y. The effect of this step is to correctly manage the mobile node's view of the binding's remaining lifetime (as maintained in the corresponding Binding Update List entry) so that it correctly counts down from the Lifetime value given in the Binding Acknowledgement, but with the timer countdown beginning at the time that the Binding Updatewas sent.

RFC Text:

When a mobile node receives a packet carrying a valid Binding Acknowledgement, the mobile node MUST examine the Status field as follows:

- If the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUST update the corresponding entry in its Binding Update List to indicate that the Binding Update has been acknowledged; the mobile node MUST then stop retransmitting the Binding Update. **In addition, if the value specified in the Lifetime field in the Binding Acknowledgement is less than the Lifetime value sent in the Binding Update being acknowledged, the mobile node MUST subtract the difference between these two Lifetime values from the remaining lifetime for the binding as maintained in the corresponding Binding Update List entry (with a minimum value for the Binding Update List entry lifetime of 0). That is, if the Lifetime value sent in the Binding Update was L_update, the Lifetime value received in the Binding Acknowledgement was L_ack, and the current remaining lifetime of the Binding Update List entry is L_remain, then the new value for the remaining lifetime of the Binding Update List entry should be**

  max((L_remain - (L_update - L_ack)), 0)

  where max(X, Y) is the maximum of X and Y. The effect of this step is to correctly manage the mobile node's view of the binding's remaining lifetime (as maintained in the corresponding Binding Update List entry) so that it correctly counts down from the Lifetime value given in the Binding Acknowledgement, but with the timer countdown beginning at the time that the Binding Update was sent.

  Mobile nodes SHOULD send a new Binding Update well before the expiration of this period in order to extend the lifetime. This helps to avoid disruptions in communications which might otherwise be caused by network delays or clock drift.

- Additionally, if the Status field value is 1 (accepted but prefix discovery necessary), the mobile node SHOULD send a Mobile Prefix Solicitation message to update its information about the available prefixes.

- If the Status field indicates that the Binding Update was rejected (the Status field is greater than or equal to 128), then the mobile node can take steps to correct the cause of the error and retransmit the Binding Update (with a new Sequence Number value), subject to the rate limiting restriction specified in Section 11.8. If this is not done or it fails, then the mobile node SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination.

Identifier: RQ_001_1768
RFC Clause: 11.7.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
Mobile nodes SHOULD send a new Binding Update well before the expiration of this period in order to extend the lifetime.

RFC Text:
When a mobile node receives a packet carrying a valid Binding Acknowledgement, the mobile node MUST examine the Status field as follows:

o If the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUST update the corresponding entry in its Binding Update List to indicate that the Binding Update has been acknowledged; the mobile node MUST then stop retransmitting the Binding Update. In addition, if the value specified in the Lifetime field in the Binding Acknowledgement is less than the Lifetime value sent in the Binding Update being acknowledged, the mobile node MUST subtract the difference between these two Lifetime values from the remaining lifetime for the binding as maintained in the corresponding Binding Update List entry (with a minimum value for the Binding Update List entry lifetime of 0). That is, if the Lifetime value sent in the Binding Update was L_update, the Lifetime value received in the Binding Acknowledgement was L_ack, and the current remaining lifetime of the Binding Update List entry is L_remain, then the new value for the remaining lifetime of the Binding Update List entry should be

max((L_remain - (L_update - L_ack)), 0)

where max(X, Y) is the maximum of X and Y. The effect of this step is to correctly manage the mobile node's view of the binding's remaining lifetime (as maintained in the corresponding Binding Update List entry) so that it correctly counts down from the Lifetime value given in the Binding Acknowledgement, but with the timer countdown beginning at the time that the Binding Update was sent.

Mobile nodes SHOULD send a new Binding Update well before the expiration of this period in order to extend the lifetime. This helps to avoid disruptions in communications which might otherwise be caused by network delays or clock drift.

o Additionally, if the Status field value is 1 (accepted but prefix discovery necessary), the mobile node SHOULD send a Mobile Prefix Solicitation message to update its information about the available prefixes.

o If the Status field indicates that the Binding Update was rejected (the Status field is greater than or equal to 128), then the mobile node can take steps to correct the cause of the error and retransmit the Binding Update (with a new Sequence Number value), subject to the rate limiting restriction specified in Section 11.8. If this is not done or it fails, then the mobile node SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination.

Identifier: RQ_001_1769
RFC Clause: 11.7.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet carrying a valid Binding Acknowledgement, if the Status field value is 1 (accepted but prefix discovery necessary), the mobile node SHOULD send a Mobile Prefix Solicitation message to update its information about the available prefixes.

RFC Text:
When a mobile node receives a packet carrying a valid Binding Acknowledgement, the mobile node MUST examine the Status field as follows:

o If the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUST update the corresponding entry in its Binding Update List to indicate that the Binding Update has been acknowledged; the mobile node MUST then stop retransmitting the Binding Update. In addition, if the value specified in the Lifetime field in the Binding Acknowledgement is less than the Lifetime value sent in the Binding Update being acknowledged, the mobile node MUST subtract the difference between these two Lifetime values from the remaining lifetime for the binding as maintained in the corresponding Binding Update List entry (with a minimum value for the Binding Update List entry lifetime of 0). That is, if the Lifetime value sent in the Binding Update was L_update, the Lifetime value received in the Binding Acknowledgement was L_ack, and the current remaining lifetime of the Binding Update List entry is L_remain, then the new value for the remaining lifetime of the Binding Update List entry should be

max((L_remain - (L_update - L_ack)), 0)

where max(X, Y) is the maximum of X and Y. The effect of this step is to correctly manage the mobile node's view of the binding's remaining lifetime (as maintained in the corresponding Binding Update List entry) so that it correctly counts down from the Lifetime value given in the Binding Acknowledgement, but with the timer countdown beginning at the time that the Binding Update was sent.

Mobile nodes SHOULD send a new Binding Update well before the expiration of this period in order to extend the lifetime. This helps to avoid disruptions in communications which might otherwise be caused by network delays or clock drift.

o Additionally, if the Status field value is 1 (accepted but prefix discovery necessary), the mobile node SHOULD send a Mobile Prefix Solicitation message to update its information about the available prefixes.

o If the Status field indicates that the Binding Update was rejected (the Status field is greater than or equal to 128), then the mobile node can take steps to correct the cause of the error and retransmit the Binding Update (with a new Sequence Number value), subject to the rate limiting restriction specified in Section 11.8. If this is not done or it fails, then the mobile node SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination.

Identifier: RQ_001_1770
RFC Clause: 11.7.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet carrying a valid Binding Acknowledgement, if the Status field indicates that the Binding Update was rejected (the Status field is greater than or equal to 128), then the mobile node can take steps to correct the cause of the error and retransmit the Binding Update (with a new Sequence Number value), subject to the rate limiting restriction (specified in RFC3775 Section 11.8). If this is not done or it fails, then the mobile node SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination.

RFC Text:
When a mobile node receives a packet carrying a valid Binding Acknowledgement, the mobile node MUST examine the Status field as follows:

o If the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUST update the corresponding entry in its Binding Update List to indicate that the Binding Update has been acknowledged; the mobile node MUST then stop retransmitting the Binding Update. In addition, if the value specified in the Lifetime field in the Binding Acknowledgement is less than the Lifetime value sent in the Binding Update being acknowledged, the mobile node MUST subtract the difference between these two Lifetime values from the remaining lifetime for the binding as maintained in the corresponding Binding Update List entry (with a minimum value for the Binding Update List entry lifetime of 0). That is, if the Lifetime value sent in the Binding Update was L_update, the Lifetime value received in the Binding Acknowledgement was L_ack, and the current remaining lifetime of the Binding Update List entry is L_remain, then the new value for the remaining lifetime of the Binding Update List entry should be

max((L_remain - (L_update - L_ack)), 0)

where max(X, Y) is the maximum of X and Y. The effect of this step is to correctly manage the mobile node's view of the binding's remaining lifetime (as maintained in the corresponding Binding Update List entry) so that it correctly counts down from the Lifetime value given in the Binding Acknowledgement, but with the timer countdown beginning at the time that the Binding Update was sent.

Mobile nodes SHOULD send a new Binding Update well before the expiration of this period in order to extend the lifetime. This helps to avoid disruptions in communications which might otherwise be caused by network delays or clock drift.

o Additionally, if the Status field value is 1 (accepted but prefix discovery necessary), the mobile node SHOULD send a Mobile Prefix Solicitation message to update its information about the available prefixes.

o If the Status field indicates that the Binding Update was rejected (the Status field is greater than or equal to 128), then the mobile node can take steps to correct the cause of the error and retransmit the Binding Update (with a new Sequence Number value), subject to the rate limiting restriction specified in Section 11.8. If this is not done or it fails, then the mobile node SHOULD record in its Binding Update List that future Binding Updates SHOULD NOT be sent to this destination.

Identifier: RQ_001_1771
RFC Clause: 11.7.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Binding Refresh Advice mobility option within the Binding Acknowledgement MUST be ignored if the acknowledgement came from a correspondent node.

If it came from the home agent, the mobile node uses the Refresh Interval field in the option as a suggestion that it SHOULD attempt to refresh its home registration at the indicated shorter interval.

RFC Text:
The treatment of a Binding Refresh Advice mobility option within the Binding Acknowledgement depends on where the acknowledgement came from. This option MUST be ignored if the acknowledgement came from a correspondent node. If it came from the home agent, the mobile node uses the Refresh Interval field in the option as a suggestion that it SHOULD attempt to refresh its home registration at the indicated shorter interval.

Identifier: RQ_001_1772
RFC Clause: 11.7.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Binding Refresh Advice mobility option within the Binding Acknowledgement came from the home agent, the mobile node uses the Refresh Interval field in the option as a suggestion that it SHOULD attempt to refresh its home registration at the indicated shorter interval.

RFC Text:
The treatment of a Binding Refresh Advice mobility option within the Binding Acknowledgement depends on where the acknowledgement came from. This option MUST be ignored if the acknowledgement came from a correspondent node. **If it came from the home agent, the mobile node uses the Refresh Interval field in the option as a suggestion that it SHOULD attempt to refresh its home registration at the indicated shorter interval.**

Identifier: RQ_001_1773
RFC Clause: 11.7.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Binding Refresh Advice mobility option within the Binding Acknowledgement came from the home agent, the mobile node examines the value of the Key Management Mobility Capability (K) bit. If this bit is not set, the mobile node SHOULD discard key management protocol connections, if any, to the home agent.

RFC Text:
If the acknowledgement came from the home agent, the mobile node examines the value of the Key Management Mobility Capability (K) bit. If this bit is not set, the mobile node SHOULD discard key management protocol connections, if any, to the home agent. The mobile node MAY also initiate a new key management connection.

Identifier: RQ_001_1774
RFC Clause: 11.7.3
Type: Optional
Applies to: Mobile_Node

Requirement:
If the Binding Refresh Advice mobility option within the Binding Acknowledgement came from the home agent, the mobile node examines the value of the Key Management Mobility Capability (K) bit. If this bit is not set, the mobile node . The mobile node MAY also initiate a new key management connection.

RFC Text:
If the acknowledgement came from the home agent, the mobile node examines the value of the Key Management Mobility Capability (K) bit. If this bit is not set, the mobile node SHOULD discard key management protocol connections, if any, to the home agent. **The mobile node MAY also initiate a new key management connection.**

Identifier: RQ_001_1775
RFC Clause: 11.7.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Binding Refresh Advice mobility option within the Binding Acknowledgement came from the home agent, the mobile node examines the value of the Key Management Mobility Capability (K) bit, if this bit is set, the mobile node SHOULD move its own endpoint in the key management protocol connections to the home agent, if any. The mobile node's new endpoint should be the new care-of address.

RFC Text:
If this bit is set, the mobile node SHOULD move its own endpoint in the key management protocol connections to the home agent, if any. The mobile node's new endpoint should be the new care-of address. For an IKE phase 1 connection, this means that packets sent to this address with the original ISAKMP cookies are accepted.

Identifier: RQ_001_1776
RFC Clause: 11.7.4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet containing a Binding Refresh Request message, the mobile node has a Binding Update List entry for the source of the Binding Refresh Request, and the mobile node wants to retain its binding cache entry at the correspondent node, then the mobile node should start a return routability procedure.

RFC Text:
When a mobile node receives a packet containing a Binding Refresh Request message, the mobile node has a Binding Update List entry for the source of the Binding Refresh Request, and the mobile node wants to retain its binding cache entry at the correspondent node, then the mobile node should start a return routability procedure. If the mobile node wants to have its binding cache entry removed, it can either ignore the Binding Refresh Request and wait for the binding to time out, or at any time, it can delete its binding from a correspondent node with an explicit binding update with a zero lifetime and the care-of address set to the home address. If the mobile node does not know if it needs the binding cache entry, it can make the decision in an implementation dependent manner, such as based on available resources.

Identifier: RQ_001_1777
RFC Clause: 11.7.4
Type: Optional
Applies to: Mobile_Node

Requirement:
When a mobile node receives a packet containing a Binding Refresh Request message, if the mobile node wants to have its binding cache entry removed, it can either ignore the Binding Refresh Request and wait for the binding to time out, or at any time, it can delete its binding from a correspondent node with an explicit binding update with a zero lifetime and the care-of address set to the home address. If the mobile node does not know if it needs the binding cache entry, it can make the decision in an implementation dependent manner, such as based on available resources.

RFC Text:
When a mobile node receives a packet containing a Binding Refresh Request message, the mobile node has a Binding Update List entry for the source of the Binding Refresh Request, and the mobile node wants to retain its binding cache entry at the correspondent node, then the mobile node should start a return routability procedure. **If the mobile node wants to have its binding cache entry removed, it can either ignore the Binding Refresh Request and wait for the binding to time out, or at any time, it can delete its binding from a correspondent node with an explicit binding update with a zero lifetime and the care-of address set to the home address. If the mobile node does not know if it needs the binding cache entry, it can make the decision in an implementation dependent manner, such as based on available resources.**

Identifier: RQ_001_1778
RFC Clause: 11.7.4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the return routability procedure completes successfully, a Binding Update message SHOULD be sent. The Lifetime field in this Binding Update SHOULD be set to a new lifetime, extending any current lifetime remaining from a previous Binding Update sent to this node (as indicated in any existing Binding Update List entry for this node), and the lifetime SHOULD again be less than or equal to the remaining lifetime of the home registration and the care-of address specified for the binding.

RFC Text:
If the return routability procedure completes successfully, a Binding Update message SHOULD be sent, as described in Section 11.7.2. The Lifetime field in this Binding Update SHOULD be set to a new lifetime, extending any current lifetime remaining from a previous Binding Update sent to this node (as indicated in any existing Binding Update List entry for this node), and the lifetime SHOULD again be less than or equal to the remaining lifetime of the home registration and the care-of address specified for the binding. When sending this Binding Update, the mobile node MUST update its Binding Update List in the same way as for any other Binding Update sent by the mobile node.

Identifier: RQ_001_1779
RFC Clause: 11.7.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When the return routability procedure completes successfully resulting in the sending of a Binding Update, the mobile node MUST update its Binding Update List in the same way as for any other Binding Update sent by the mobile node.

RFC Text:
If the return routability procedure completes successfully, a Binding Update message SHOULD be sent, as described in Section 11.7.2. The Lifetime field in this Binding Update SHOULD be set to a new lifetime, extending any current lifetime remaining from a previous Binding Update sent to this node (as indicated in any existing Binding Update List entry for this node), and the lifetime SHOULD again be less than or equal to the remaining lifetime of the home registration and the care-of address specified for the binding. **When sending this Binding Update, the mobile node MUST update its Binding Update List in the same way as for any other Binding Update sent by the mobile node.**

Identifier: RQ_001_1780
RFC Clause: 11.8
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the mobile node is sending a Mobile Prefix Solicitation, it SHOULD use an initial retransmission interval of INITIAL_SOLICIT_TIMER.

RFC Text:
When the mobile node sends a Mobile Prefix Solicitation, Home Test Init, Care-of Test Init or Binding Update for which it expects a response, the mobile node has to determine a value for the initial retransmission timer:

- **If the mobile node is sending a Mobile Prefix Solicitation, it SHOULD use an initial retransmission interval of INITIAL_SOLICIT_TIMER (see Section 12).**

- If the mobile node is sending a Binding Update and does not have an existing binding at the home agent, it SHOULD use InitialBindackTimeoutFirstReg (see Section 13) as a value for the initial retransmission timer. This long retransmission interval will allow the home agent to complete the Duplicate Address Detection procedure mandated in this case, as detailed in Section 11.7.1.

- Otherwise, the mobile node should use the specified value of INITIAL_BINDACK_TIMEOUT for the initial retransmission timer.

Identifier: RQ_001_1781
RFC Clause: 11.8
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the mobile node is sending a Binding Update and does not have an existing binding at the home agent, it SHOULD use InitialBindackTimeoutFirstReg as a value for the initial retransmission timer.

RFC Text:
When the mobile node sends a Mobile Prefix Solicitation, Home Test Init, Care-of Test Init or Binding Update for which it expects a response, the mobile node has to determine a value for the initial retransmission timer:

- If the mobile node is sending a Mobile Prefix Solicitation, it SHOULD use an initial retransmission interval of INITIAL_SOLICIT_TIMER (see Section 12).

- **If the mobile node is sending a Binding Update and does not have an existing binding at the home agent, it SHOULD use InitialBindackTimeoutFirstReg (see Section 13) as a value for the initial retransmission timer. This long retransmission interval will allow the home agent to complete the Duplicate Address Detection procedure mandated in this case, as detailed in Section 11.7.1.**

- Otherwise, the mobile node should use the specified value of INITIAL_BINDACK_TIMEOUT for the initial retransmission timer.

Identifier: RQ_001_1782
RFC Clause: 11.8
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When the mobile node sends a Mobile Prefix Solicitation, Home Test Init, Care-of Test Init or Binding Update for which it expects a response, the mobile node has to determine a value for the initial retransmission timer, by defualt the mobile node should use the specified value of INITIAL_BINDACK_TIMEOUT for the initial retransmission timer.

RFC Text:
When the mobile node sends a Mobile Prefix Solicitation, Home Test Init, Care-of Test Init or Binding Update for which it expects a response, the mobile node has to determine a value for the initial retransmission timer:

- o If the mobile node is sending a Mobile Prefix Solicitation, it SHOULD use an initial retransmission interval of INITIAL_SOLICIT_TIMER (see Section 12).

- o If the mobile node is sending a Binding Update and does not have an existing binding at the home agent, it SHOULD use InitialBindackTimeoutFirstReg (see Section 13) as a value for the initial retransmission timer. This long retransmission interval will allow the home agent to complete the Duplicate Address Detection procedure mandated in this case, as detailed in Section 11.7.1.

- **o Otherwise, the mobile node should use the specified value of INITIAL_BINDACK_TIMEOUT for the initial retransmission timer**.

Identifier: RQ_001_1783
RFC Clause: 11.8
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the mobile node fails to receive a valid matching response within the selected initial retransmission interval, the mobile node SHOULD retransmit the message until a response is received.

RFC Text:
If the mobile node fails to receive a valid matching response within the selected initial retransmission interval, the mobile node SHOULD retransmit the message until a response is received.

Identifier: RQ_001_1784
RFC Clause: 11.8
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The retransmissions by the mobile node MUST use an exponential back- off process in which the timeout period is doubled upon each retransmission, until either the node receives a response or the timeout period reaches the value MAX_BINDACK_TIMEOUT.

RFC Text:
The retransmissions by the mobile node MUST use an exponential back- off process in which the timeout period is doubled upon each retransmission, until either the node receives a response or the timeout period reaches the value MAX_BINDACK_TIMEOUT. The mobile node MAY continue to send these messages at this slower rate indefinitely.

Identifier: RQ_001_1785
RFC Clause: 11.8
Type: Optional
Applies to: Mobile_Node

Requirement:
Once the timeout period reaches the value MAX_BINDACK_TIMEOUT, the mobile node MAY continue to send retransmission messages at this rate indefinitely.

RFC Text:
The retransmissions by the mobile node MUST use an exponential back- off process in which the timeout period is doubled upon each retransmission, until either the node receives a response or the timeout period reaches the value MAX_BINDACK_TIMEOUT. **The mobile node MAY continue to send these messages at this slower rate indefinitely.**

Identifier: RQ_001_1786
RFC Clause: 11.8
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The mobile node SHOULD start a separate back-off process for different message types, different home addresses and different care-of addresses.

RFC Text:
The mobile node SHOULD start a separate back-off process for different message types, different home addresses and different care-of addresses. However, in addition an overall rate limitation applies for messages sent to a particular correspondent node. This ensures that the correspondent node has a sufficient amount of time to respond when bindings for multiple home addresses are registered, for instance. The mobile node MUST NOT send Mobility Header messages of a particular type to a particular correspondent node more than MAX_UPDATE_RATE times within a second.

Identifier: RQ_001_1787
RFC Clause: 11.8
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The mobile node MUST NOT send Mobility Header messages of a particular type to a particular correspondent node more than MAX_UPDATE_RATE times within a second.

RFC Text:
The mobile node SHOULD start a separate back-off process for different message types, different home addresses and different care-of addresses. However, in addition an overall rate limitation applies for messages sent to a particular correspondent node. This ensures that the correspondent node has a sufficient amount of time to respond when bindings for multiple home addresses are registered, for instance. **The mobile node MUST NOT send Mobility Header messages of a particular type to a particular correspondent node more than MAX_UPDATE_RATE times within a second.**

Identifier: RQ_001_1788
RFC Clause: 11.8
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Retransmitted Binding Updates MUST use a Sequence Number value greater than that used for the previous transmission of this Binding Update.

RFC Text:
Retransmitted Binding Updates MUST use a Sequence Number value greater than that used for the previous transmission of this Binding Update. Retransmitted Home Test Init and Care-of Test Init messages MUST use new cookie values.

Identifier: RQ_001_1789
RFC Clause: 11.8
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Retransmitted Home Test Init and Care-of Test Init messages MUST use new cookie values.

RFC Text:
Retransmitted Binding Updates MUST use a Sequence Number value greater than that used for the previous transmission of this Binding Update. **Retransmitted Home Test Init and Care-of Test Init messages MUST use new cookie values.**

Identifier: RQ_001_1790
RFC Clause: 12
Type: Mandatory
Applies to: Node

Requirement:
Prtocols must comply with the following constratints:

DHAAD_RETRIES	4 retransmissions
INITIAL_BINDACK_TIMEOUT	1 second
INITIAL_DHAAD_TIMEOUT	3 seconds
INITIAL_SOLICIT_TIMER	3 seconds
MAX_BINDACK_TIMEOUT	32 seconds
MAX_NONCE_LIFETIME	240 seconds
MAX_TOKEN_LIFETIME	210 seconds
MAX_RR_BINDING_LIFETIME	420 seconds
MAX_UPDATE_RATE	3 times
PREFIX_ADV_RETRIES	3 retransmissions
PREFIX_ADV_TIMEOUT	3 seconds

RFC Text:

DHAAD_RETRIES	**4 retransmissions**
INITIAL_BINDACK_TIMEOUT	**1 second**
INITIAL_DHAAD_TIMEOUT	**3 seconds**
INITIAL_SOLICIT_TIMER	**3 seconds**
MAX_BINDACK_TIMEOUT	**32 seconds**
MAX_NONCE_LIFETIME	**240 seconds**
MAX_TOKEN_LIFETIME	**210 seconds**
MAX_RR_BINDING_LIFETIME	**420 seconds**
MAX_UPDATE_RATE	**3 times**
PREFIX_ADV_RETRIES	**3 retransmissions**
PREFIX_ADV_TIMEOUT	**3 seconds**

Identifier: RQ_001_1791
RFC Clause: 13
Type: Mandatory
Applies to: Node

Requirement:
Protocols must comply with the following configuration variables:

MaxMobPfxAdvInterval	Default: 86,400 seconds
MinDelayBetweenRAs	Default: 3 seconds, Min: 0.03 seconds
MinMobPfxAdvInterval	Default: 600 seconds
InitialBindackTimeoutFirstReg	Default: 1.5 seconds

RFC Text:

MaxMobPfxAdvInterval	**Default: 86,400 seconds**
MinDelayBetweenRAs	**Default: 3 seconds, Min: 0.03 seconds**
MinMobPfxAdvInterval	**Default: 600 seconds**
InitialBindackTimeoutFirstReg	**Default: 1.5 seconds**

Identifier: RQ_001_1792
RFC Clause: 13
Type: Mandatory
Applies to: Home_Agent

Requirement:
Home agents MUST allow the following variables to be configured by system management:

MaxMobPfxAdvInterval
MinDelayBetweenRAs
MinMobPfxAdvInterval

RFC Text:
Home agents MUST allow the first three variables to be configured by system management, and mobile nodes MUST allow the last variable to be configured by system management.

Identifier: RQ_001_1793
RFC Clause: 13
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Mobile nodes MUST allow the following variables to be configured by system management:

InitialBindackTimeoutFirstReg

RFC Text:
Home agents MUST allow the first three variables to be configured by system management, and **mobile nodes MUST allow the last variable to be configured by system management.**

Identifier: RQ_001_1794
RFC Clause: 13
Type: Mandatory
Applies to: Node

Requirement:
The default value for InitialBindackTimeoutFirstReg has been calculated as 1.5 times the default value of RetransTimer times the default value of DupAddrDetectTransmits.

RFC Text:
The default value for InitialBindackTimeoutFirstReg has been calculated as 1.5 times the default value of RetransTimer [12] times the default value of DupAddrDetectTransmits [13].

Identifier: RQ_001_1795
RFC Clause: 13
Type: Mandatory
Applies to: Node

Requirement:
The value MinDelayBetweenRAs overrides the value of the protocol constant MIN_DELAY_BETWEEN_RAS, as specified in RFC 2461.

RFC Text:
The value MinDelayBetweenRAs overrides the value of the protocol constant MIN_DELAY_BETWEEN_RAS, as specified in RFC 2461 [12]. This variable SHOULD be set to MinRtrAdvInterval, if MinRtrAdvInterval is less than 3 seconds.

Identifier: RQ_001_1796
RFC Clause: 13
Type: Recommendation
Applies to: Node

Requirement:
The value MinDelayBetweenRA SHOULD be set to MinRtrAdvInterval, if MinRtrAdvInterval is less than 3 seconds.

RFC Text:
The value MinDelayBetweenRAs overrides the value of the protocol constant MIN_DELAY_BETWEEN_RAS, as specified in RFC 2461 [12]. **This variable SHOULD be set to MinRtrAdvInterval, if MinRtrAdvInterval is less than 3 seconds.**

Identifier: RQ_001_1797
RFC Clause: 5.2.7
Type: Optional
Applies to: Mobile_Node

Requirement:
When a Mobile Node receives an error code (either 136, 137, or 138) in the Binding Acknowledgement; the Mobile Node can then retry the return routability procedure.

RFC Text:
Due to resource limitations, rapid deletion of bindings, or reboots the correspondent node may not in all cases recognize the nonces that the tokens were based on. If a nonce index is unrecognized, the correspondent node replies with an error code in the Binding Acknowledgement (either 136, 137, or 138 as discussed in Section 6.1.8). **The mobile node can then retry the return routability procedure.**

Identifier: RQ_001_1798
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
The presence of "mobility options" are indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. **The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options.** These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1798
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
The presence of "mobility options" are indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. **The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options.** These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1798
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The presence of "mobility options" are indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. **The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options.** These options include padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8. The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1799
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Padding option is used to ensure that all options are aligned on an 8- octet boundary and that the total length of the Mobility Header is divisible by 8.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include **padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8.** The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1799
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Padding option is used to ensure that all options are aligned on an 8- octet boundary and that the total length of the Mobility Header is divisible by 8.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include **padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8.** The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1799
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Padding option is used to ensure that all options are aligned on an 8- octet boundary and that the total length of the Mobility Header is divisible by 8.

RFC Text:
A variable length field containing the data specific to the indicated Mobility Header type.

Mobile IPv6 also defines a number of "mobility options" for use within these messages; if included, any options MUST appear after the fixed portion of the message data specified in this document. The presence of such options will be indicated by the Header Len field within the message. When the Header Len value is greater than the length required for the message specified here, the remaining octets are interpreted as mobility options. These options include **padding options that can be used to ensure that other options are aligned properly, and that the total length of the message is divisible by 8.** The encoding and format of defined options are described in Section 6.2.

Alignment requirements for the Mobility Header are the same as for any IPv6 protocol Header. That is, they MUST be aligned on an 8- octet boundary.

Identifier: RQ_001_1800
RFC Clause: 6.1.7
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Binding Update Message, the care-of address MUST be a unicast routable address.

RFC Text:
The care-of address is specified either by the Source Address field in the IPv6 header or by the Alternate Care-of Address option, if present. **The care-of address MUST be a unicast routable address**. IPv6 Source Address MUST be a topologically correct source address. Binding Updates for a care-of address which is not a unicast routable address MUST be silently discarded.

Identifier: RQ_001_1801
RFC Clause: 6.7
Type: Optional
Applies to: Mobile_Node

Requirement:
The Mobile Prefix Solicitation messages may have options.

RFC Text:
The Mobile Prefix Solicitation messages may have options. These options MUST use the option format defined in RFC 2461. This document does not define any option types for the Mobile Prefix Solicitation message, but future documents may define new options. Home agents MUST silently ignore any options they do not recognize and continue processing the message.

Identifier: RQ_001_1802
RFC Clause: 7.5
Type: Optional
Applies to: Mobility_aware_Router

Requirement:
On an implementation where unsolicited multicast Router Advertisements can be disabled on specific interfaces, the MinRtrAdvInterval and MaxRtrAdvInterval can then be set to some high values.

RFC Text:
Note that multicast Router Advertisements are not always required in certain wireless networks that have limited bandwidth. Mobility detection or link changes in such networks may be done at lower layers. Router advertisements in such networks SHOULD be sent only when solicited. In such networks it SHOULD be possible to disable unsolicited multicast Router Advertisements on specific interfaces. **The MinRtrAdvInterval and MaxRtrAdvInterval in such a case can be set to some high values**.

Identifier: RQ_001_1803
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST also check that the source address in the tunneled packets corresponds to the currently registered location of the mobile node.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o Every home agent MUST be able to encapsulate [15] such intercepted packets in order to tunnel them to the primary care-of address for the mobile node indicated in its binding in the home agent's Binding Cache (Section 10.4.2).

o Every home agent MUST support decapsulating [15] reverse tunneled packets sent to it from a mobile node's home address. **Every home agent MUST also check that the source address in the tunneled packets corresponds to the currently registered location of the mobile node** (Section 10.4.5).

o ...

Identifier: RQ_001_1804
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
Every home agent MUST be able to participate in dynamic home agent address discovery.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o **Every home agent** MUST be able to accept packets addressed to the Mobile IPv6 Home-Agents anycast address [16] for the subnet on which it is serving as a home agent, and **MUST be able to participate in dynamic home agent address discovery** (Section 10.5).

o ...

Identifier: RQ_001_1805
RFC Clause: 8.4
Type: Optional
Applies to: Home_Agent

Requirement:
Every home agent SHOULD respond to Mobile Prefix Solicitations.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o **Every home agent** SHOULD support sending ICMP Mobile Prefix Advertisements (Section 6.8), and **SHOULD respond to Mobile Prefix Solicitations** (Section 6.7). If supported, this behavior MUST be configurable, so that home agents can be configured to avoid sending such Prefix Advertisements according to the needs of the network administration in the home domain.

o ...

Identifier: RQ_001_1806
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
If a home agent is able to send ICMP Mobile Prefix Advertisements, this behavior MUST be configurable (enable/disable).

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o **Every home agent SHOULD support sending ICMP Mobile Prefix Advertisements** (Section 6.8), and SHOULD respond to Mobile Prefix Solicitations (Section 6.7). **If supported, this behavior MUST be configurable**, so that home agents can be configured to avoid sending such Prefix Advertisements according to the needs of the network administration in the home domain.

o ...

Identifier: RQ_001_1807
RFC Clause: 8.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
A Home Agent that support the multicast group membership control protocols MUST be capable of using it to determine which multicast data packets to forward via the tunnel to the mobile node.

RFC Text:
In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. The following additional requirements apply to all IPv6 routers that serve as a home agent:

o ...

o **Every home agent SHOULD support the multicast group membership control protocols** as described in Section 10.4.3. **If this support is provided, the home agent MUST be capable of using it to determine which multicast data packets to forward via the tunnel to the mobile node.**
o ...

Identifier: RQ_001_1808
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST support care-of address formation.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o **The node MUST support movement detection, care-of address formation, and returning home** (Section 11.5).

o ...

Identifier: RQ_001_1809
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All IPv6 nodes capable of functioning as mobile nodes MUST support the returning home procedure.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o The node MUST support movement detection, care-of address formation, and returning home (Section 11.5).

o ...

Identifier: RQ_001_1810
RFC Clause: 8.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If a Mobile Node supports the multicast address listener part of a multicast group membership protocol, the mobile node MUST then be able to receive tunneled multicast packets from the home agent.

RFC Text:
Finally, the following requirements apply to all IPv6 nodes capable of functioning as mobile nodes:

o ...

o **The node MAY support the multicast address listener part of a multicast group membership protocol** as described in Section 11.3.4. **If this support is provided, the mobile node MUST be able to receive tunneled multicast packets from the home agent**.

o ...

Identifier: RQ_001_1811
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Before accepting a Binding Update, the receiving node MUST validate that the Sequence Number field in the Binding Update is greater than the Sequence Number received in the previous valid Binding Update for this home address, if any.

RFC Text:
Before accepting a Binding Update, the receiving node MUST validate the Binding Update according to the following tests:

o The packet MUST contain a unicast routable home address, either in the Home Address option or in the Source Address, if the Home Address option is not present.

o The Sequence Number field in the Binding Update is greater than the Sequence Number received in the previous valid Binding Update for this home address, if any.

Identifier: RQ_001_1811
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Before accepting a Binding Update, the receiving node MUST validate that the Sequence Number field in the Binding Update is greater than the Sequence Number received in the previous valid Binding Update for this home address, if any.

RFC Text:
Before accepting a Binding Update, the receiving node MUST validate the Binding Update according to the following tests:

o The packet MUST contain a unicast routable home address, either in the Home Address option or in the Source Address, if the Home Address option is not present.

o The Sequence Number field in the Binding Update is greater than the Sequence Number received in the previous valid Binding Update for this home address, if any.

Identifier: RQ_001_1812
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
A home agent serving a mobile node MUST schedule the delivery of the new prefix information to that mobile node when the valid or preferred lifetime is reconfigured or changes for any reason other than advancing real time.

RFC Text:
A home agent serving a mobile node will schedule the delivery of the new prefix information to that mobile node when any of the following conditions occur:

MUST}}:

- The state of the flags changes for the prefix of the mobile node's registered home address.
- **The valid or preferred lifetime is reconfigured or changes for any reason other than advancing real time.**
- The mobile node requests the information with a Mobile Prefix Solicitation (see Section 11.4.2).

SHOULD:

- A new prefix is added to the home subnet interface(s) of the home agent.

MAY:

- The valid or preferred lifetime or the state of the flags changes for a prefix which is not used in any Binding Cache entry for this mobile node.

Identifier: RQ_001_1813
RFC Clause: 10.6.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
A home agent serving a mobile node MUST schedule the delivery of the new prefix information to that mobile node when the mobile node requests the information with a Mobile Prefix Solicitation.

RFC Text:
A home agent serving a mobile node will schedule the delivery of the new prefix information to that mobile node when any of the following conditions occur:

MUST:

- The state of the flags changes for the prefix of the mobile node's registered home address.
- The valid or preferred lifetime is reconfigured or changes for any reason other than advancing real time.
- **The mobile node requests the information with a Mobile Prefix Solicitatio**n (see Section 11.4.2).

SHOULD:

- A new prefix is added to the home subnet interface(s) of the home agent.

MAY:

- The valid or preferred lifetime or the state of the flags changes for a prefix which is not used in any Binding Cache entry for this mobile node.

Identifier: RQ_001_1814
RFC Clause: 11.7.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Mobile Node only knows one Home Agent and reaches the MAX_BINDACK_TIMEOUT retransmission timeout period, the mobile node SHOULD continue to periodically retransmit the Binding Update at this rate until acknowledged (or until it begins attempting to register a different primary care-of address).

RFC Text:
The Acknowledge (A) bit in the Binding Update requests the home agent to return a Binding Acknowledgement in response to this Binding Update. As described in Section 6.1.8, the mobile node SHOULD retransmit this Binding Update to its home agent until it receives a matching Binding Acknowledgement. **Once reaching a retransmission timeout period of MAX_BINDACK_TIMEOUT,** the mobile node SHOULD restart the process of delivering the Binding Update, but trying instead the next home agent returned during dynamic home agent address discovery (see Section 11.4.1). **If there was only one home agent, the mobile node instead SHOULD continue to periodically retransmit the Binding Update at this rate until acknowledged (or until it begins attempting to register a different primary care-of address).** See Section 11.8 for information about retransmitting Binding Updates.

Identifier: RQ_001_1815
RFC Clause: 11.7.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a Mobile Node is sending a Binding Update to a correspondent node, requesting the deletion of any existing Binding Cache entry it has for the Mobile Node, and the Mobile Node is away from home: the Mobile Node MUST set the care-of address to its current care-of address.

RFC Text:
If the Binding Update is sent to the correspondent node, requesting the deletion of any existing Binding Cache entry it has for the mobile node, the care-of address is set to the mobile node's home address and the Lifetime field set to zero. In this case, generation of the binding management key depends exclusively on the home keygen token (Section 5.2.5). The care-of nonce index SHOULD be set to zero in this case. In keeping with the Binding Update creation rules below, **the care-of address MUST be set to** the home address if the mobile node is at home, or to **the current care-of address if it is away from home.**

Identifier: RQ_001_1816
RFC Clause: 5
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
Binding Updates between Mobile Node and Correspondent node MUST be protected by the use of the Binding Authorization Data option.

RFC Text:
Binding Updates are protected by the use of IPsec extension headers, or by the use of the Binding Authorization Data option. This option employs a binding management key, Kbm, which can be established through the return routability procedure. Mobile prefix discovery is protected through the use of IPsec extension headers. Mechanisms related to transporting payload packets - such as the Home Address destination option and type 2 routing header - have been specified in a manner which restricts their use in attacks.

Identifier: RQ_001_1816
RFC Clause: 5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Binding Updates between Mobile Node and Correspondent node MUST be protected by the use of the Binding Authorization Data option.

RFC Text:
Binding Updates are protected by the use of IPsec extension headers, or by the use of the Binding Authorization Data option. This option employs a binding management key, Kbm, which can be established through the return routability procedure. Mobile prefix discovery is protected through the use of IPsec extension headers. Mechanisms related to transporting payload packets - such as the Home Address destination option and type 2 routing header - have been specified in a manner which restricts their use in attacks.

Identifier: RQ_001_1817
RFC Clause: 9.5.1
Type: Mandatory
Applies to: Correspondent_Node

Requirement:
If the Correspondant node validates a Binding Update where:

- the Lifetime specified in the Binding Update is nonzero
- the specified care-of address is not equal to the home address for the binding
- the Home Registration (H) bit is not set in the Binding Update

then this is a request to cache a binding for the home address and is processed according to the procedure specified in in Section 9.5.2.

RFC Text:
If the Binding Update is valid according to the tests above, then the Binding Update is processed further as follows:

o The Sequence Number value received from a mobile node in a Binding Update is stored by the receiving node in its Binding Cache entry for the given home address.

o If the Lifetime specified in the Binding Update is nonzero and the specified care-of address is not equal to the home address for the binding, then this is a request to cache a binding for the home address. If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.1; otherwise, it is processed according to the procedure specified in Section 9.5.2.

o If the Lifetime specified in the Binding Update is zero or the specified care-of address matches the home address for the binding, then this is a request to delete the cached binding for the home address. In this case, the Binding Update MUST include a valid home nonce index, and the care-of nonce index MUST be ignored by the correspondent node. The generation of the binding management key depends then exclusively on the home keygen token (Section 5.2.5). If the Home Registration (H) bit is set in the Binding Update, the Binding Update is processed according to the procedure specified in Section 10.3.2; otherwise, it is processed according to the procedure specified in Section 9.5.3.

Identifier: RQ_001_1818
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
In processing the Binding Update, a Home Address destination option MUST be present in the message.

RFC Text:
To begin processing the Binding Update, the home agent MUST perform the following sequence of tests:

o If the node implements only correspondent node functionality, or has not been configured to act as a home agent, then the node MUST reject the Binding Update. The node MUST also return a Binding Acknowledgement to the mobile node, in which the Status field is set to 131 (home registration not supported).

o Else, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (not home subnet).

o Else, if the home agent chooses to reject the Binding Update for any other reason (e.g., insufficient resources to serve another mobile node as a home agent), then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to an appropriate value to indicate the reason for the rejection.

o A Home Address destination option MUST be present in the message. It MUST be validated as described in Section 9.3.1 with the following additional rule. The Binding Cache entry existence test MUST NOT be done for IPsec packets when the Home Address option contains an address for which the receiving node could act as a home agent.

Identifier: RQ_001_1819
RFC Clause: 11.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If there is no binding yet with the correspondent node the Reverse Tunneling mechanism SHALL be used to tunnel the packets via the home agent.

RFC Text:
Reverse Tunneling

This is the mechanism which tunnels the packets via the home agent. It is not as efficient as the above mechanism, but is needed if there is no binding yet with the correspondent node.

This mechanism is used for packets that have the mobile node's home address as the Source Address in the IPv6 header, or with multicast control protocol packets as described in Section 11.3.4.
Specifically:

* The packet is sent to the home agent using IPv6 encapsulation 15].

* The Source Address in the tunnel packet is the primary care-of address as registered with the home agent.

* The Destination Address in the tunnel packet is the home agent's address.

Then, the home agent will pass the encapsulated packet to the correspondent node.

Identifier: RQ_001_1820
RFC Clause: 11.3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
On receipt of a valid packet from the mobile node using the Reverse Tunneling mechanism, the home agent will pass the encapsulated packet to the correspondent node.

RFC Text:
Reverse Tunneling

This is the mechanism which tunnels the packets via the home agent. It is not as efficient as the above mechanism, but is needed if there is no binding yet with the correspondent node.

This mechanism is used for packets that have the mobile node's home address as the Source Address in the IPv6 header, or with multicast control protocol packets as described in Section 11.3.4.
Specifically:

* The packet is sent to the home agent using IPv6 encapsulation 15].

* The Source Address in the tunnel packet is the primary care-of address as registered with the home agent.

* **The Destination Address in the tunnel packet is the home agent's address.**

Then, the home agent will pass the encapsulated packet to the correspondent node.

Identifier: RQ_001_1821
RFC Clause: 11.5.1
Type: Optional
Applies to: Mobile_Node

Requirement:
If Router Advertisements that the mobile node receives include an Advertisement Interval option, the mobile node may use its Advertisement Interval field as an indication of the frequency with which it should expect to continue to receive future Advertisements from that router. If this amount of time elapses without the mobile node receiving any Advertisement from this router, the mobile node can be sure that at least one Advertisement sent by the router has been lost. The mobile node can then implement its own policy to determine how many lost Advertisements from its current default router constitute an L3 handover indication.

RFC Text:
In addition, the mobile node should consider the following events as indications that an L3 handover may have occurred. Upon receiving such indications, the mobile node needs to perform Router Discovery to discover routers and prefixes on the new link, as described in Section 6.3.7 of RFC 2461 [12].

- **If Router Advertisements that the mobile node receives include an Advertisement Interval option, the mobile node may use its Advertisement Interval field as an indication of the frequency with which it should expect to continue to receive future Advertisements from that router. This field specifies the minimum rate (the maximum amount of time between successive Advertisements) that the mobile node should expect. If this amount of time elapses without the mobile node receiving any Advertisement from this router, the mobile node can be sure that at least one Advertisement sent by the router has been lost. The mobile node can then implement its own policy to determine how many lost Advertisements from its current default router constitute an L3 handover indication.**

- **Nei**ghbor Unreachability Detection determines that the default router is no longer reachable.

- With some types of networks, notification that an L2 handover has occurred might be obtained from lower layer protocols or device driver software within the mobile node. While further details around handling L2 indications as movement hints is an item for further study, at the time of writing this specification the following is considered reasonable:

  An L2 handover indication may or may not imply L2 movement and L2 movement may or may not imply L3 movement; the correlations might be a function of the type of L2 but might also be a function of actual deployment of the wireless topology.

  Unless it is well-known that an L2 handover indication is likely to imply L3 movement, instead of immediately multicasting a router solicitation it may be better to attempt to verify whether the default router is still bi-directionally reachable. This can be accomplished by sending a unicast Neighbor Solicitation and waiting for a Neighbor Advertisement with the solicited flag set. Note that this is similar to Neighbor Unreachability detection but it does not have the same state machine, such as the STALE state.

  If the default router does not respond to the Neighbor Solicitation it makes sense to proceed to multicasting a Router Solicitation.

Identifier: RQ_001_1822
RFC Clause: 11.5.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If Neighbor Unreachability Detection determines that the default router is no longer reachable the mobile node should consider this as an indications that an L3 handover may have occurred .

RFC Text:
In addition, the mobile node should consider the following events as indications that an L3 handover may have occurred. Upon receiving such indications, the mobile node needs to perform Router Discovery to discover routers and prefixes on the new link, as described in Section 6.3.7 of RFC 2461 [12].

o If Router Advertisements that the mobile node receives include an Advertisement Interval option, the mobile node may use its Advertisement Interval field as an indication of the frequency with which it should expect to continue to receive future Advertisements from that router. This field specifies the minimum rate (the maximum amount of time between successive Advertisements) that the mobile node should expect. If this amount of time elapses without the mobile node receiving any Advertisement from this router, the mobile node can be sure that at least one Advertisement sent by the router has been lost. The mobile node can then implement its own policy to determine how many lost Advertisements from its current default router constitute an L3 handover indication.

o Neighbor Unreachability Detection determines that the default router is no longer reachable.

o With some types of networks, notification that an L2 handover has occurred might be obtained from lower layer protocols or device driver software within the mobile node. While further details around handling L2 indications as movement hints is an item for further study, at the time of writing this specification the following is considered reasonable:

An L2 handover indication may or may not imply L2 movement and L2 movement may or may not imply L3 movement; the correlations might be a function of the type of L2 but might also be a function of actual deployment of the wireless topology.

Unless it is well-known that an L2 handover indication is likely to imply L3 movement, instead of immediately multicasting a router solicitation it may be better to attempt to verify whether the default router is still bi-directionally reachable. This can be accomplished by sending a unicast Neighbor Solicitation and waiting for a Neighbor Advertisement with the solicited flag set. Note that this is similar to Neighbor Unreachability detection but it does not have the same state machine, such as the STALE state.

If the default router does not respond to the Neighbor Solicitation it makes sense to proceed to multicasting a Router Solicitation.

Identifier: RQ_001_1823
RFC Clause: 11.5.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
In the event of detecting a layer 2 handover, unless it is well-known that an L2 handover indication is likely to imply L3 movement, instead of immediately multicasting a router solicitation it may be better to attempt to verify whether the default router is still bi-directionally reachable. This can be accomplished by sending a unicast Neighbor Solicitation and waiting for a Neighbor Advertisement with the solicited flag set. If the default router does not respond to the Neighbor Solicitation it makes sense to proceed to multicasting a Router Solicitation.
`

RFC Text:
In addition, the mobile node should consider the following events as indications that an L3 handover may have occurred. Upon receiving such indications, the mobile node needs to perform Router Discovery to discover routers and prefixes on the new link, as described in Section 6.3.7 of RFC 2461 [12].

o If Router Advertisements that the mobile node receives include an Advertisement Interval option, the mobile node may use its Advertisement Interval field as an indication of the frequency with which it should expect to continue to receive future Advertisements from that router. This field specifies the minimum rate (the maximum amount of time between successive Advertisements) that the mobile node should expect. If this amount of time elapses without the mobile node receiving any Advertisement from this router, the mobile node can be sure that at least one Advertisement sent by the router has been lost. The mobile node can then implement its own policy to determine how many lost Advertisements from its current default router constitute an L3 handover indication.

o Neighbor Unreachability Detection determines that the default router is no longer reachable.

o With some types of networks, notification that an L2 handover has occurred might be obtained from lower layer protocols or device driver software within the mobile node. While further details around handling L2 indications as movement hints is an item for further study, at the time of writing this specification the following is considered reasonable:

An L2 handover indication may or may not imply L2 movement and L2 movement may or may not imply L3 movement; the correlations might be a function of the type of L2 but might also be a function of actual deployment of the wireless topology.

Unless it is well-known that an L2 handover indication is likely to imply L3 movement, instead of immediately multicasting a router solicitation it may be better to attempt to verify whether the default router is still bi-directionally reachable. This can be accomplished by sending a unicast Neighbor Solicitation and waiting for a Neighbor Advertisement with the solicited flag set. Note that this is similar to Neighbor Unreachability detection but it does not have the same state machine, such as the STALE state.

If the default router does not respond to the Neighbor Solicitation it makes sense to proceed to multicasting a Router Solicitation.

Identifier: RQ_001_1824
RFC Clause: 11.5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When the mobile node detects an L3 handover, it SHALL:

- perform Duplicate Address Detection on its link-local address,
- select a new default router as a consequence of Router Discovery,
- and then perform Prefix Discovery with that new router to form new care-of address(es) as described in Section 11.5.2.
- register its new primary care-of address with its home agent as described in Section 11.7.1.
- and after updating its home registration, the mobile node SHALLthen update associated mobility bindings in correspondent nodes that it is performing route optimization with as specified in Section 11.7.2.

RFC Text:
When the mobile node detects an L3 handover, it performs Duplicate Address Detection [13] on its link-local address, selects a new default router as a consequence of Router Discovery, and then performs Prefix Discovery with that new router to form new care-of address(es) as described in Section 11.5.2. It then registers its new primary care-of address with its home agent as described in Section 11.7.1. After updating its home registration, the mobile node then updates associated mobility bindings in correspondent nodes that it is performing route optimization with as specified in Section 11.7.2.

Identifier: RQ_001_1825
RFC Clause: 10.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In processing the Binding Update, a Home Address destination option MUST be validated as described in Section 9.3.1 with the following additional rule. The Binding Cache entry existence test MUST NOT be done for IPsec packets when the Home Address option contains an address for which the receiving node could act as a home agent.

RFC Text:
To begin processing the Binding Update, the home agent MUST perform the following sequence of tests:

- If the node implements only correspondent node functionality, or has not been configured to act as a home agent, then the node MUST reject the Binding Update. The node MUST also return a Binding Acknowledgement to the mobile node, in which the Status field is set to 131 (home registration not supported).

- Else, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (not home subnet).

- Else, if the home agent chooses to reject the Binding Update for any other reason (e.g., insufficient resources to serve another mobile node as a home agent), then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to an appropriate value to indicate the reason for the rejection.

- **A Home Address destination option** MUST be present in the message. **It MUST be validated as described in Section 9.3.1 with the following additional rule. The Binding Cache entry existence test MUST NOT be done for IPsec packets when the Home Address option contains an address for which the receiving node could act as a home agent.**

Identifier: RQ_001_1826
RFC Clause:
Type: Mandatory
Applies to: Home_Agent

Requirement:
If home agent accepts the Binding Update, it MUST then update its Binding Cache entry for this mobile node if such an entry already exists.

RFC Text:
If home agent accepts the Binding Update, it MUST then create a new entry in its Binding Cache for this mobile node or **update its existing Binding Cache entry, if such an entry already exists**. The Home Address field as received in the Home Address option provides the home address of the mobile node.

4.2 Requirements extracted from RFC3776

Identifier: RQ_001_2001
RFC Clause: 3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When the mobile node is away from its home, the Binding Updates sent by it to the home agent MUST support at least the following headers in the following order:

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header in transport mode
Mobility header
   Binding Update
      Alternate Care-of Address option (care-of address)
```

RFC Text:
When the mobile node is away from its home, the BUs sent by it to the home agent MUST support at least the following headers in the following order:

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header in transport mode
Mobility header
   Binding Update
      Alternate Care-of Address option (care-of address)
```

Note that the Alternate Care-of Address option is used to ensure that the care-of address is protected by ESP. The home agent considers the address within this option as the current care-of address for the mobile node. The home address is not protected by ESP directly, but the use of a specific home address with a specific security association is required by policy.

Identifier: RQ_001_2002
RFC Clause: 3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

The Binding Acknowledgements sent back to the mobile node when it is away from home MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header in transport mode
Mobility header
   Binding Acknowledgement
```

RFC Text:

The Binding Acknowledgements sent back to the mobile node when it is away from home MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header in transport mode
Mobility header
   Binding Acknowledgement
```

Identifier: RQ_001_2003
RFC Clause: 3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:

When the mobile node is at home the Binding Updates MUST support at least the following headers in the following order:

```
IPv6 header (source = home address,
             destination = home agent)
ESP header in transport mode
Mobility header
   Binding Update
```

RFC Text:

When the mobile node is at home, the above rules are different as the mobile node can use its home address as a source address. This typically happens for the de-registration Binding Update when the mobile is returning home. In this situation, the Binding Updates MUST support at least the following headers in the following order:

```
IPv6 header (source = home address,
             destination = home agent)
ESP header in transport mode
Mobility header
   Binding Update
```

Identifier: RQ_001_2004
RFC Clause: 3.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

The Binding Acknowledgement messages sent to the home address MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = home address)
ESP header in transport mode
Mobility header
   Binding Acknowledgement
```

RFC Text:

The Binding Acknowledgement messages sent to the home address MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = home address)
ESP header in transport mode
Mobility header
   Binding Acknowledgement
```

Identifier: RQ_001_2005
RFC Clause: 3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

When the Home Test Init messages tunneled to the home agent are protected by IPsec, they MUST support at least the following headers in the following order:

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header in tunnel mode
IPv6 header (source = home address,
             destination = correspondent node)
Mobility Header
   Home Test Init
```

RFC Text:

When the Home Test Init messages tunneled to the home agent are protected by IPsec, they MUST support at least the following headers in the following order:

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header in tunnel mode
IPv6 header (source = home address,
             destination = correspondent node)
Mobility Header
   Home Test Init
```

This format assumes that the mobile node's current care-of address is used as the outer header destination address in the security association. As discussed in Section 4.3, this requires the home agent to update the destination address when the mobile node moves. Policy entries and security association selectors stay the same, however, as the inner packets do not change upon movements.

Identifier: RQ_001_2006
RFC Clause: 3.2
Type: Mandatory
Applies to: Home_Agent

Requirement:

When the Home Test messages tunneled from the home agent are protected by IPsec, they MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header in tunnel mode
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test
```

RFC Text:

Similarly, when the Home Test messages tunneled from the home agent are protected by IPsec, they MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header in tunnel mode
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test
```

Identifier: RQ_001_2007
RFC Clause: 3.3
Type: Mandatory
Applies to: Home_Agent

Requirement:

If IPsec is used to protect prefix discovery, requests for prefixes from the mobile node to the home agent MUST support at least the following headers in the following order.

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header in transport mode
ICMPv6
   Mobile Prefix Solicitation
```

RFC Text:

If IPsec is used to protect prefix discovery, requests for prefixes from the mobile node to the home agent MUST support at least the following headers in the following order.

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header in transport mode
ICMPv6
   Mobile Prefix Solicitation
```

Identifier: RQ_001_2008
RFC Clause: 3.3
Type: Mandatory
Applies to: Home_Agent

Requirement:

If IPsec is used, solicited and unsolicited prefix information advertisements from the home agent to the mobile node MUST support at least the following headers in the following order.

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header in transport mode
ICMPv6
   Mobile Prefix Advertisement
```

RFC Text:

Again **if IPsec is used, solicited and unsolicited prefix information advertisements from the home agent to the mobile node MUST support at least the following headers in the following order.**

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header in transport mode
ICMPv6
   Mobile Prefix Advertisement
```

Identifier: RQ_001_2009
RFC Clause: 3.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:

If IPsec is used to protect payload packets tunneled to the home agent from the mobile node, we use a format similar to the one in Section 3.2. However, instead of the MobilityHeader, these packets may contain any legal IPv6 protocol(s):

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header in tunnel mode
IPv6 header (source = home address,
             destination = correspondent node)
Any protocol
```

RFC Text:

If IPsec is used to protect payload packets tunneled to the home agent from the mobile node, we use a format similar to the one in Section 3.2. However, instead of the MobilityHeader, these packets may contain any legal IPv6 protocol(s):

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header in tunnel mode
IPv6 header (source = home address,
             destination = correspondent node)
Any protocol
```

Identifier: RQ_001_2010
RFC Clause: 3.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
When the payload packets are tunneled from the home agent to the mobile node with ESP encapsulation, they MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header in tunnel mode
IPv6 header (source = correspondent node,
             destination = home address)
Any protocol
```

RFC Text:
Similarly, when the payload packets are tunneled from the home agent to the mobile node with ESP encapsulation, they MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header in tunnel mode
IPv6 header (source = correspondent node,
             destination = home address)
Any protocol
```

Identifier: RQ_001_2011
RFC Clause: 4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Manual configuration of IPsec security associations MUST be supported.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- **Manual configuration of IPsec security associations MUST be supported.** The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2011
RFC Clause: 4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Manual configuration of IPsec security associations MUST be supported.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- **Manual configuration of IPsec security associations MUST be supported.** The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2012
RFC Clause: 4.1
Type: Optional
Applies to: Home_Agent

Requirement:
Automatic key management with IKE MAY be supported.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- **Automatic key management with IKE [4] MAY be supported**. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2012
RFC Clause: 4.1
Type: Optional
Applies to: Mobile_Node

Requirement:
Automatic key management with IKE MAY be supported.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- **Automatic key management with IKE [4] MAY be supported**. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2013
RFC Clause: 4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Transport Mode ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be used.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- **ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used**.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2013
RFC Clause: 4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Transport Mode ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be used.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- **ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used**.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2014
RFC Clause: 4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
Tunnel Mode ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- **ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported** and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2014
RFC Clause: 4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Tunnel Mode ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- **ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported** and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2015
RFC Clause: 4.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
Tunnel Mode ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent SHOULD be used.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- **ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent** MUST be supported and **SHOULD be used.**

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2015
RFC Clause: 4.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:

Tunnel Mode ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent SHOULD be used.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- **ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent** MUST be supported and **SHOULD be used.**

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2016
RFC Clause: 4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

Transport Mode ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- **ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported** and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2016
RFC Clause: 4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Transport Mode ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- **ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported** and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2017
RFC Clause: 4.1
Type: Recommendation
Applies to: Home_Agent

Requirement:
Transport Mode ESP encapsulation of the ICMPv6 messages related to prefix discovery SHOULD be used.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- **ESP encapsulation of the ICMPv6 messages related to prefix discovery** MUST be supported and **SHOULD be used.**

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2017
RFC Clause: 4.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:

Transport Mode ESP encapsulation of the ICMPv6 messages related to prefix discovery SHOULD be used.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- **ESP encapsulation of the ICMPv6 messages related to prefix discovery** MUST be supported and **SHOULD be used.**

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2018
RFC Clause: 4.1
Type: Optional
Applies to: Home_Agent

Requirement:
ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- **ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used**.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2018
RFC Clause: 4.1
Type: Optional
Applies to: Mobile_Node

Requirement:
ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- **ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used**.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2019
RFC Clause: 4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:
If multicast group membership control protocols are supported, payload data protection MUST be supported for those protocols.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- **If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.**

Identifier: RQ_001_2019
RFC Clause: 4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If multicast group membership control protocols are supported, payload data protection MUST be supported for those protocols.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- **If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.**

Identifier: RQ_001_2020
RFC Clause: 4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
When a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option SHALL be considered as the source address of the packet.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.**

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2020
RFC Clause: 4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option SHALL be considered as the source address of the packet.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.**

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2021
RFC Clause: 4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
A home address within a Type 2 Routing header destined to the receiving node SHALL BE considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- **Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.**

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2021
RFC Clause: 4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
A home address within a Type 2 Routing header destined to the receiving node SHALL BE considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- **Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.**

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2022
RFC Clause: 4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- **When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent.** This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2022
RFC Clause: 4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- **When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent.** This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2023
RFC Clause: 4.2
Type: Optional
Applies to: Home_Agent

Requirement:
The authentication of mobile nodes MAY be based either on machine or user credentials.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- **The authentication of mobile nodes MAY be based either on machine or user credentials.** Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2023
RFC Clause: 4.2
Type: Optional
Applies to: Mobile_Node

Requirement:
The authentication of mobile nodes MAY be based either on machine or user credentials.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- **The authentication of mobile nodes MAY be based either on machine or user credentials.** Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2025
RFC Clause: 4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent are made inactive. If the corresponding security associations were created dynamically using IKE, they are automatically deleted when they expire.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- **When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (**for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. **If the security associations were created dynamically using IKE, they are automatically deleted when they expire.** If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2025
RFC Clause: 4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent are made inactive. If the corresponding security associations were created dynamically using IKE, they are automatically deleted when they expire.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- **When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (**for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. **If the security associations were created dynamically using IKE, they are automatically deleted when they expire.** If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2026
RFC Clause: 4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent are made inactive. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- **When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (**for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expir**e. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again.** The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2026
RFC Clause: 4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent are made inactive. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- **When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (**for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expir**e. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again.** The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

Identifier: RQ_001_2027
RFC Clause: 4.2
Type: Recommendation
Applies to: Home_Agent

Requirement:
When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent are made inactive. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- **When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (**for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. **The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.**

Identifier: RQ_001_2027
RFC Clause: 4.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent are made inactive. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- **When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (**for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. **The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.**

Identifier: RQ_001_2028
RFC Clause: 4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The mobile node MUST use the Home Address destination option in Binding Updates and Mobile Prefix Solicitations, sent to the home agent from a care-of address.

RFC Text:
The following rules apply to mobile nodes:

- **The mobile node MUST use the Home Address destination option in Binding Updates and Mobile Prefix Solicitations, sent to the home agent from a care-of address.**

- When the mobile node receives a changed set of prefixes from the home agent during prefix discovery, there is a need to configure new security policy entries, and there may be a need to configure new security associations. It is outside the scope of this specification to discuss automatic methods for this.

Identifier: RQ_001_2029
RFC Clause: 4.2
Type: Mandatory
Applies to: Home_Agent

Requirement:
The home agent MUST use the Type 2 Routing header in Binding Acknowledgements and Mobile Prefix Advertisements sent to the mobile node, again due to the need to have the home address visible when the policy checks are made

RFC Text:
The following rules apply to home agents:

- **The home agent MUST use the Type 2 Routing header in Binding Acknowledgements and Mobile Prefix Advertisements sent to the mobile node, again due to the need to have the home address visible when the policy checks are made.**

- It is necessary to avoid the possibility that a mobile node could use its security association to send a Binding Update on behalf of another mobile node using the same home agent. In order to do this, the security policy database entries MUST unequivocally identify a single security association for protecting Binding Updates between any given home address and home agent when manually keyed IPsec security associations are used. When dynamic keying is used, the security policy database entries MUST unequivocally identify the IKE phase 1 credentials which can be used to authorize the creation of security associations for protecting Binding Updates for a particular home address. How these mappings are maintained is outside the scope of this specification, but they may be maintained, for instance, as a locally administered table in the home agent. If the phase 1 identity is a Fully Qualified Domain Name (FQDN), secure forms of DNS may also be used.

- When the set of prefixes advertised by the home agent changes, there is a need to configure new security policy entries, and there may be a need to configure new security associations. It is outside the scope of this specification to discuss automatic methods for this, if new home addresses are required.

Identifier: RQ_001_2030
RFC Clause: 4.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support the Encapsulating Security Payload (ESP) header in transport mode.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support** and SHOULD use **the Encapsulating Security Payload (ESP) [3] header in transport mode** and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2030
RFC Clause: 4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support the Encapsulating Security Payload (ESP) header in transport mode.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support** and SHOULD use **the Encapsulating Security Payload (ESP) [3] header in transport mode** and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2031
RFC Clause: 4.3
Type: Recommendation
Applies to: Home_Agent

Requirement:
When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents** MUST support and **SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode** and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2031
RFC Clause: 4.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents** MUST support and **SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode** and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2032
RFC Clause: 4.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents** MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and **MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.**

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2032
RFC Clause: 4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents** MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and **MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.**

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2033
RFC Clause: 4.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
Provide mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401, RFC 2402, and RFC 2406.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

o When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

o Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.

Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2033
RFC Clause: 4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Provide mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401, RFC 2402, and RFC 2406.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

o When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

o Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.

Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2034
RFC Clause: 4.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
Tunnel mode IPsec ESP MUST be supported for the protection of packets belonging to the return routability procedure[Home Test Init, Home Test, Care-of Test Init and Care-of Test messages]

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- **Tunnel mode IPsec ESP MUST be support**ed and SHOULD be used **for the protection of packets belonging to the return routability procedure.** A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2034
RFC Clause: 4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Tunnel mode IPsec ESP MUST be supported for the protection of packets belonging to the return routability procedure[Home Test Init, Home Test, Care-of Test Init and Care-of Test messages]

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- **Tunnel mode IPsec ESP MUST be support**ed and SHOULD be used **for the protection of packets belonging to the return routability procedure.** A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2035
RFC Clause: 4.3
Type: Recommendation
Applies to: Home_Agent

Requirement:
Tunnel mode IPsec ESP SHOULD be used for the protection of packets belonging to the return routability procedure.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- **Tunnel mode IPsec ESP** MUST be supported and **SHOULD be used for the protection of packets belonging to the return routability procedure.** A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2035
RFC Clause: 4.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
Tunnel mode IPsec ESP SHOULD be used for the protection of packets belonging to the return routability procedure.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- **Tunnel mode IPsec ESP** MUST be supported and **SHOULD be used for the protection of packets belonging to the return routability procedure.** A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2036
RFC Clause: 4.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
When tunnel mode IPsec ESP is used for the protection of packets belonging to the return routability procedure, a non-null encryption transform and a non-null authentication algorithm MUST be applied.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- **Tunnel mode IPsec ESP** MUST be supported and SHOULD be used **for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.**

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2036
RFC Clause: 4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When tunnel mode IPsec ESP is used for the protection of packets belonging to the return routability procedure, a non-null encryption transform and a non-null authentication algorithm MUST be applied.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

- **Tunnel mode IPsec ESP** MUST be supported and SHOULD be used **for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.**

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

Identifier: RQ_001_2037
RFC Clause: 4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When ESP is used to protect Binding Updates, Mobile IPv6 implementations MUST use the Alternate Care-of Address mobility option in Binding Updates sent by mobile nodes while away from home.

RFC Text:
The following rules apply to mobile nodes:

- **When ESP is used to protect Binding Updates**, there is no protection for the care-of address which appears in the IPv6 header outside the area protected by ESP. It is important for the home agent to verify that the care-of address has not been tampered with. As a result, the attacker would have redirected the mobile node's traffic to another address. In order to prevent this, **Mobile IPv6 implementations MUST use the Alternate Care-of Address mobility option in Binding Updates sent by mobile nodes while away from home.** The exception to this is when the mobile node returns home and sends a Binding Update to the home agent in order to de-register. In this case no Alternate Care-of Address option is needed, as described in Section 3.1.

  When IPsec is used to protect return routability signaling or payload packets, the mobile node MUST set the source address it uses for the outgoing tunnel packets to the current primary care-of address. The mobile node starts to use a new primary care-of address immediately after sending a Binding Update to the home agent to register this new address. Similarly, it starts to use the new address as the required destination address of tunneled packets received from the home agent.

Identifier: RQ_001_2038
RFC Clause: 4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When IPsec is used to protect return routability signaling or payload packets, the mobile node MUST set the source address it uses for the outgoing tunnel packets to the current primary care-of address.

RFC Text:
The following rules apply to mobile nodes:

- When ESP is used to protect Binding Updates, there is no protection for the care-of address which appears in the IPv6 header outside the area protected by ESP. It is important for the home agent to verify that the care-of address has not been tampered with. As a result, the attacker would have redirected the mobile node's traffic to another address. In order to prevent this, Mobile IPv6 implementations MUST use the Alternate Care-of Address mobility option in Binding Updates sent by mobile nodes while away from home. The exception to this is when the mobile node returns home and sends a Binding Update to the home agent in order to de-register. In this case no Alternate Care-of Address option is needed, as described in Section 3.1.

  When IPsec is used to protect return routability signaling or payload packets, the mobile node MUST set the source address it uses for the outgoing tunnel packets to the current primary care-of address. The mobile node starts to use a new primary care-of address immediately after sending a Binding Update to the home agent to register this new address. Similarly, it starts to use the new address as the required destination address of tunneled packets received from the home agent.

Identifier: RQ_001_2039
RFC Clause: 4.3
Type: Mandatory
Applies to: Home_Agent

Requirement:
When IPsec is used to protect return routability signaling or payload packets, IPsec security associations are needed to provide this protection. When the care-of address for the mobile node changes as a result of an accepted Binding Update, special treatment is needed for the next packets sent using these security associations. The home agent MUST set the new care-of address as the destination address of these packets.

RFC Text:
The following rules apply to home agents:

> o **When IPsec is used to protect return routability signaling or payload packets, IPsec security associations are needed to provide this protection. When the care-of address for the mobile node changes as a result of an accepted Binding Update, special treatment is needed for the next packets sent using these security associations. The home agent MUST set the new care-of address as the destination address of these packets,** as if the outer header destination address in the security association had changed. Similarly, the home agent starts to expect the new source address in the tunnel packets received from the mobile node.
>
> Such address changes can be implemented, for instance, through an API from the Mobile IPv6 implementation to the IPsec implementation. It should be noted that the use of such an API and the address changes MUST only be done based on the Binding Updates received by the home agent and protected by the use of IPsec. Address modifications based on other sources, such as Binding Updates to the correspondent nodes protected by return routability, or open access to an API from any application may result in security vulnerabilities.

Identifier: RQ_001_2040
RFC Clause: 4.3
Type: Recommendation
Applies to: Home_Agent

Requirement:
Address changes MUST only be done based on the Binding Updates received by the home agent and protected by the use of IPsec.

RFC Text:
The following rules apply to home agents:

> o When IPsec is used to protect return routability signaling or payload packets, IPsec security associations are needed to provide this protection. When the care-of address for the mobile node changes as a result of an accepted Binding Update, special treatment is needed for the next packets sent using these security associations. The home agent MUST set the new care-of address as the destination address of these packets, as if the outer header destination address in the security association had changed. Similarly, the home agent starts to expect the new source address in the tunnel packets received from the mobile node.
>
> Such address changes can be implemented, for instance, through an API from the Mobile IPv6 implementation to the IPsec implementation. It should be noted that the use of such an API and the **address changes MUST only be done based on the Binding Updates received by the home agent and protected by the use of IPsec.** Address modifications based on other sources, such as Binding Updates to the correspondent nodes protected by return routability, or open access to an API from any application may result in security vulnerabilities.

Identifier: RQ_001_2041
RFC Clause: 4.4
Type: Mandatory
Applies to: Home_Agent

Requirement:
If anti-replay protection is required, dynamic keying MUST be used.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **If anti-replay protection is required, dynamic keying MUST be used.** IPsec can provide anti-replay protection only if dynamic keying is used (which may not always be the case). IPsec also does not guarantee correct ordering of packets, only that they have not been replayed. Because of this, sequence numbers within the Mobile IPv6 messages are used to ensure correct ordering. However, if the 16 bit Mobile IPv6 sequence number space is cycled through, or the home agent reboots and loses its state regarding the sequence numbers, replay and reordering attacks become possible. The use of dynamic keying, IPsec anti-replay protection, and the Mobile IPv6 sequence numbers can together prevent such attacks.

- If IKE version 1 is used with preshared secrets in main mode, it determines the shared secret to use from the IP address of the peer. With Mobile IPv6, however, this may be a care-of address and does not indicate which mobile node attempts to contact the home agent. Therefore, if preshared secret authentication is used in IKEv1 between the mobile node and the home agent then aggressive mode MUST be used. Note also that care needs to be taken with phase 1 identity selection. Where the ID_IPV6_ADDR Identity Payloads is used, unambiguous mapping of identities to keys is not possible. (The next version of IKE may not have these limitations.)

Identifier: RQ_001_2041
RFC Clause: 4.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If anti-replay protection is required, dynamic keying MUST be used.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- **If anti-replay protection is required, dynamic keying MUST be used.** IPsec can provide anti-replay protection only if dynamic keying is used (which may not always be the case). IPsec also does not guarantee correct ordering of packets, only that they have not been replayed. Because of this, sequence numbers within the Mobile IPv6 messages are used to ensure correct ordering. However, if the 16 bit Mobile IPv6 sequence number space is cycled through, or the home agent reboots and loses its state regarding the sequence numbers, replay and reordering attacks become possible. The use of dynamic keying, IPsec anti-replay protection, and the Mobile IPv6 sequence numbers can together prevent such attacks.

- If IKE version 1 is used with preshared secrets in main mode, it determines the shared secret to use from the IP address of the peer. With Mobile IPv6, however, this may be a care-of address and does not indicate which mobile node attempts to contact the home agent. Therefore, if preshared secret authentication is used in IKEv1 between the mobile node and the home agent then aggressive mode MUST be used. Note also that care needs to be taken with phase 1 identity selection. Where the ID_IPV6_ADDR Identity Payloads is used, unambiguous mapping of identities to keys is not possible. (The next version of IKE may not have these limitations.)

Identifier: RQ_001_2042
RFC Clause: 4.4
Type: Mandatory
Applies to: Home_Agent

Requirement:

If preshared secret authentication is used in IKEv1 between the mobile node and the home agent then aggressive mode MUST be used.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- If anti-replay protection is required, dynamic keying MUST be used. IPsec can provide anti-replay protection only if dynamic keying is used (which may not always be the case). IPsec also does not guarantee correct ordering of packets, only that they have not been replayed. Because of this, sequence numbers within the Mobile IPv6 messages are used to ensure correct ordering. However, if the 16 bit Mobile IPv6 sequence number space is cycled through, or the home agent reboots and loses its state regarding the sequence numbers, replay and reordering attacks become possible. The use of dynamic keying, IPsec anti-replay protection, and the Mobile IPv6 sequence numbers can together prevent such attacks.

- If IKE version 1 is used with preshared secrets in main mode, it determines the shared secret to use from the IP address of the peer. With Mobile IPv6, however, this may be a care-of address and does not indicate which mobile node attempts to contact the home agent. Therefore, **if preshared secret authentication is used in IKEv1 between the mobile node and the home agent then aggressive mode MUST be used. N**ote also that care needs to be taken with phase 1 identity selection. Where the ID_IPV6_ADDR Identity Payloads is used, unambiguous mapping of identities to keys is not possible. (The next version of IKE may not have these limitations.)

Identifier: RQ_001_2042
RFC Clause: 4.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If preshared secret authentication is used in IKEv1 between the mobile node and the home agent then aggressive mode MUST be used.

RFC Text:
The following requirements apply to both home agents and mobile nodes:

- If anti-replay protection is required, dynamic keying MUST be used. IPsec can provide anti-replay protection only if dynamic keying is used (which may not always be the case). IPsec also does not guarantee correct ordering of packets, only that they have not been replayed. Because of this, sequence numbers within the Mobile IPv6 messages are used to ensure correct ordering. However, if the 16 bit Mobile IPv6 sequence number space is cycled through, or the home agent reboots and loses its state regarding the sequence numbers, replay and reordering attacks become possible. The use of dynamic keying, IPsec anti-replay protection, and the Mobile IPv6 sequence numbers can together prevent such attacks.

- If IKE version 1 is used with preshared secrets in main mode, it determines the shared secret to use from the IP address of the peer. With Mobile IPv6, however, this may be a care-of address and does not indicate which mobile node attempts to contact the home agent. Therefore, **if preshared secret authentication is used in IKEv1 between the mobile node and the home agent then aggressive mode MUST be used. N**ote also that care needs to be taken with phase 1 identity selection. Where the ID_IPV6_ADDR Identity Payloads is used, unambiguous mapping of identities to keys is not possible. (The next version of IKE may not have these limitations.)

Identifier: RQ_001_2043
RFC Clause: 4.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If dynamic keying is used, the key management protocol MUST use the care-of address as the source address in the protocol exchanges with the mobile node's home agent.

RFC Text:
The following rules apply to mobile nodes:

- In addition to the rules above, **if dynamic keying is used, the key management protocol MUST use the care-of address as the source address in the protocol exchanges with the mobile node's home agent.**
- However, the IPsec security associations with the mobile node's home agent use home addresses. That is, the IPsec security associations MUST be requested from the key management protocol using the home address of the mobile node as the client identity.

  The security associations for protecting Binding Updates and Acknowledgements are requested for the Mobility header protocol in transport mode and for specific IP addresses as endpoints. No other selectors are used. Similarly, the security associations for protecting prefix discovery are requested for the ICMPv6 protocol and the specific IP addresses, again without other selectors. Security associations for payload and return routability protection are requested for a specific tunnel interface and either the payload protocol or the Mobility header protocol, in tunnel mode. In this case one requested endpoint is an IP address and the other one is a wildcard, and there are no other selectors.

- If the mobile node has used IKE version 1 to establish security associations with its home agent, it should follow the procedures discussed in Section 11.7.1 and 11.7.3 of the base specification [7] to determine whether the IKE endpoints can be moved or if IKE phase 1 has to be re-established.

Identifier: RQ_001_2044
RFC Clause: 4.4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the mobile node has used IKE version 1 to establish security associations with its home agent, it should follow the procedures discussed in Section 11.7.1 and 11.7.3 of RFC3775 to determine whether the IKE endpoints can be moved or if IKE phase 1 has to be re-established.

RFC Text:
The following rules apply to mobile nodes:

- In addition to the rules above, if dynamic keying is used, the key management protocol MUST use the care-of address as the source address in the protocol exchanges with the mobile node's home agent.
- However, the IPsec security associations with the mobile node's home agent use home addresses. That is, the IPsec security associations MUST be requested from the key management protocol using the home address of the mobile node as the client identity.

  The security associations for protecting Binding Updates and Acknowledgements are requested for the Mobility header protocol in transport mode and for specific IP addresses as endpoints. No other selectors are used. Similarly, the security associations for protecting prefix discovery are requested for the ICMPv6 protocol and the specific IP addresses, again without other selectors. Security associations for payload and return routability protection are requested for a specific tunnel interface and either the payload protocol or the Mobility header protocol, in tunnel mode. In this case one requested endpoint is an IP address and the other one is a wildcard, and there are no other selectors.

- **If the mobile node has used IKE version 1 to establish security associations with its home agent, it should follow the procedures discussed in Section 11.7.1 and 11.7.3 of the base specification [7] to determine whether the IKE endpoints can be moved or if IKE phase 1 has to be re-established.**

Identifier: RQ_001_2045
RFC Clause: 4.4
Type: Recommendation
Applies to: Home_Agent

Requirement:
If the home agent has used IKE version 1 to establish security associations with the mobile node, it should follow the procedures discussed in Section 10.3.1 and 10.3.2 of RFC3775 to determine whether the IKE endpoints can be moved or if IKE phase 1 has to be re-established.

RFC Text:
The following rules apply to home agents:

- **If the home agent has used IKE version 1 to establish security associations with the mobile node, it should follow the procedures discussed in Section 10.3.1 and 10.3.2 of the base specification [7] to determine whether the IKE endpoints can be moved or if IKE phase 1 has to be re-established.**

Identifier: RQ_001_2046
RFC Clause: 4.1
Type: Mandatory
Applies to: Home_Agent

Requirement:

If stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

RFC Text:

The following requirements apply to both home agents and mobile nodes:

- Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

Identifier: RQ_001_2046
RFC Clause: 4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

RFC Text:

```
The following requirements apply to both home agents and mobile nodes:

   o  Manual configuration of IPsec security associations MUST be
      supported.  The configuration of the keys is expected to take
      place out-of-band, for instance at the time the mobile node is
      configured to use its home agent.

   o  Automatic key management with IKE [4] MAY be supported.  Only
      IKEv1 is discussed in this document.  Other automatic key
      management mechanisms exist and will appear beyond IKEv1, but this
      document does not address the issues related to them.

   o  ESP encapsulation of Binding Updates and Acknowledgements between
      the mobile node and home agent MUST be supported and MUST be used.

   o  ESP encapsulation of the Home Test Init and Home Test messages
      tunneled between the mobile node and home agent MUST be supported
      and SHOULD be used.

   o  ESP encapsulation of the ICMPv6 messages related to prefix
      discovery MUST be supported and SHOULD be used.

   o  ESP encapsulation of the payload packets tunneled between the
      mobile node and home agent MAY be supported and used.

   o  If multicast group membership control protocols or stateful
      address autoconfiguration protocols are supported, payload data
      protection MUST be supported for those protocols.
```

4.3 Requirements extracted from RFC4068

Identifier: RQ_001_3001
RFC Clause: 3.1
Type: Mandatory
Applies to: Router

Requirement:
All implementations MUST support the Fast Handover mechanism specified in this document to avoid potential address conflicts.

RFC Text:
Through the RtSolPr and PrRtAdv messages, the MN also formulates a prospective new CoA (NCoA) when it is still present on the PAR's link. Hence, the latency due to new prefix discovery subsequent to handover is eliminated. Furthermore, this prospective address can be used immediately after attaching to the new subnet link (i.e., NAR's link) when the MN has received a "Fast Binding Acknowledgment (FBack)" message prior to its movement. If it moves without receiving an FBack, the MN can still start using NCoA after announcing its attachment through a "Fast Neighbor Advertisement (FNA)" message. NAR responds to FNA if the tentative address is already in use thereby reducing NCoA configuration latency. Under some limited conditions in which the probability of address collision is considered insignificant, it may be possible to use NCoA immediately after attaching to the new link. **Even so, all implementations MUST support** and SHOULD use **the mechanism specified in this document to avoid potential address conflicts.**

Identifier: RQ_001_3001
RFC Clause: 3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All implementations MUST support the Fast Handover mechanism specified in this document to avoid potential address conflicts.

RFC Text:
Through the RtSolPr and PrRtAdv messages, the MN also formulates a prospective new CoA (NCoA) when it is still present on the PAR's link. Hence, the latency due to new prefix discovery subsequent to handover is eliminated. Furthermore, this prospective address can be used immediately after attaching to the new subnet link (i.e., NAR's link) when the MN has received a "Fast Binding Acknowledgment (FBack)" message prior to its movement. If it moves without receiving an FBack, the MN can still start using NCoA after announcing its attachment through a "Fast Neighbor Advertisement (FNA)" message. NAR responds to FNA if the tentative address is already in use thereby reducing NCoA configuration latency. Under some limited conditions in which the probability of address collision is considered insignificant, it may be possible to use NCoA immediately after attaching to the new link. **Even so, all implementations MUST support** and SHOULD use **the mechanism specified in this document to avoid potential address conflicts.**

Identifier: RQ_001_3002
RFC Clause: 3.1
Type: Recommendation
Applies to: Router

Requirement:
All implementations SHOULD use the Fast Handover mechanism specified in this document to avoid potential address conflicts.

RFC Text:
Through the RtSolPr and PrRtAdv messages, the MN also formulates a prospective new CoA (NCoA) when it is still present on the PAR's link. Hence, the latency due to new prefix discovery subsequent to handover is eliminated. Furthermore, this prospective address can be used immediately after attaching to the new subnet link (i.e., NAR's link) when the MN has received a "Fast Binding Acknowledgment (FBack)" message prior to its movement. If it moves without receiving an FBack, the MN can still start using NCoA after announcing its attachment through a "Fast Neighbor Advertisement (FNA)" message. NAR responds to FNA if the tentative address is already in use thereby reducing NCoA configuration latency. Under some limited conditions in which the probability of address collision is considered insignificant, it may be possible to use NCoA immediately after attaching to the new link. **Even so, all implementations** MUST support and **SHOULD use the mechanism specified in this document to avoid potential address conflicts.**

Identifier: RQ_001_3002
RFC Clause: 3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
All implementations SHOULD use the Fast Handover mechanism specified in this document to avoid potential address conflicts.

RFC Text:
Through the RtSolPr and PrRtAdv messages, the MN also formulates a prospective new CoA (NCoA) when it is still present on the PAR's link. Hence, the latency due to new prefix discovery subsequent to handover is eliminated. Furthermore, this prospective address can be used immediately after attaching to the new subnet link (i.e., NAR's link) when the MN has received a "Fast Binding Acknowledgment (FBack)" message prior to its movement. If it moves without receiving an FBack, the MN can still start using NCoA after announcing its attachment through a "Fast Neighbor Advertisement (FNA)" message. NAR responds to FNA if the tentative address is already in use thereby reducing NCoA configuration latency. Under some limited conditions in which the probability of address collision is considered insignificant, it may be possible to use NCoA immediately after attaching to the new link. **Even so, all implementations** MUST support and **SHOULD use the mechanism specified in this document to avoid potential address conflicts.**

Identifier: RQ_001_3003
RFC Clause: 3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
To reduce the Binding Update latency, the protocol specifies a tunnel between the Previous CoA (PCoA) and the New CoA (NCoA). When feasible, the Mobile Node (MN) SHOULD send a Fast Binding Update (FBU) from the Previous Access Router's (PAR's) link. Otherwise, it should be sent immediately after attachment to New Access Router (NAR) has been detected.

RFC Text:
To reduce the Binding Update latency, the protocol specifies a tunnel between the Previous CoA (PCoA) and the NCoA. An MN sends a "Fast Binding Update" message to its Previous Access Router to establish this tunnel. When feasible, the MN SHOULD send an FBU from PAR's link. Otherwise, it should be sent immediately after attachment to NAR has been detected. Subsequent sections describe the protocol mechanics. As a result, PAR begins tunneling packets arriving for PCoA to NCoA. Such a tunnel remains active until the MN completes the Binding Update with its correspondents. In the opposite direction, the MN SHOULD reverse tunnel packets to PAR until it completes the Binding Update. PAR SHOULD forward the inner packet in the tunnel to its destination (i.e., to the MN's correspondent). Such a reverse tunnel ensures that packets containing PCoA as a source IP address are not dropped due to ingress filtering. Readers may observe that even though the MN is IP-capable on the new link, it cannot use NCoA directly with its correspondents without the correspondents first establishing a binding cache entry (for NCoA). Forwarding support for PCoA is provided through a reverse tunnel between the MN and the PAR.

Identifier: RQ_001_3004
RFC Clause: 3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The Mobile Node (MN) SHOULD reverse tunnel packets to the Previous Access Router (PAR) until it completes the Binding Update.

RFC Text:
To reduce the Binding Update latency, the protocol specifies a tunnel between the Previous CoA (PCoA) and the NCoA. An MN sends a "Fast Binding Update" message to its Previous Access Router to establish this tunnel. When feasible, the MN SHOULD send an FBU from PAR's link. Otherwise, it should be sent immediately after attachment to NAR has been detected. Subsequent sections describe the protocol mechanics. As a result, PAR begins tunneling packets arriving for PCoA to NCoA. Such a tunnel remains active until the MN completes the Binding Update with its correspondents. **In the opposite direction, the MN SHOULD reverse tunnel packets to PAR until it completes the Binding Update.** PAR SHOULD forward the inner packet in the tunnel to its destination (i.e., to the MN's correspondent). Such a reverse tunnel ensures that packets containing PCoA as a source IP address are not dropped due to ingress filtering. Readers may observe that even though the MN is IP-capable on the new link, it cannot use NCoA directly with its correspondents without the correspondents first establishing a binding cache entry (for NCoA). Forwarding support for PCoA is provided through a reverse tunnel between the MN and the PAR.

Identifier: RQ_001_3005
RFC Clause: 3.1
Type: Recommendation
Applies to: Router

Requirement:
On receipt of reverse tunnel packets from the Mobile Node (MN), the Previous Access Router (PAR) SHOULD forward the inner packet in the tunnel to its destination (i.e., to the MN's correspondent).

RFC Text:
To reduce the Binding Update latency, the protocol specifies a tunnel between the Previous CoA (PCoA) and the NCoA. An MN sends a "Fast Binding Update" message to its Previous Access Router to establish this tunnel. When feasible, the MN SHOULD send an FBU from PAR's link. Otherwise, it should be sent immediately after attachment to NAR has been detected. Subsequent sections describe the protocol mechanics. As a result, PAR begins tunneling packets arriving for PCoA to NCoA. Such a tunnel remains active until the MN completes the Binding Update with its correspondents. In the opposite direction, the MN SHOULD reverse tunnel packets to PAR until it completes the Binding Update. **PAR SHOULD forward the inner packet in the tunnel to its destination (i.e., to the MN's correspondent)**. Such a reverse tunnel ensures that packets containing PCoA as a source IP address are not dropped due to ingress filtering. Readers may observe that even though the MN is IP-capable on the new link, it cannot use NCoA directly with its correspondents without the correspondents first establishing a binding cache entry (for NCoA). Forwarding support for PCoA is provided through a reverse tunnel between the MN and the PAR.

Identifier: RQ_001_3006
RFC Clause: 3.1
Type: Mandatory
Applies to: Router

Requirement:
The "Handover Initiate (HI)" and "Handover Acknowledge (HAck)" messages MUST be supported.

RFC Text:
The protocol also provides the following important functionalities. The access routers can exchange messages to confirm that a proposed NCoA is acceptable. For instance, when an MN sends an FBU from PAR's link, FBack can be delivered after the NAR considers the NCoA acceptable for use. This is especially useful when addresses are assigned by the access router. The NAR can also rely on its trust relationship with PAR before providing forwarding support for the MN. That is, it may create a forwarding entry for the NCoA subject to "approval" from PAR which it trusts. Finally, the access routers could transfer network-resident contexts, such as access control, QoS, and header compression, in conjunction with handover. **For these operations, the protocol provides "Handover Initiate (HI)" and "Handover Acknowledge (HAck)" messages. Both of these messages MUST be supported** and SHOULD be used. The access routers MUST have necessary security association established by means outside the scope of this document.

Identifier: RQ_001_3006
RFC Clause: 3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The "Handover Initiate (HI)" and "Handover Acknowledge (HAck)" messages MUST be supported.

RFC Text:
The protocol also provides the following important functionalities. The access routers can exchange messages to confirm that a proposed NCoA is acceptable. For instance, when an MN sends an FBU from PAR's link, FBack can be delivered after the NAR considers the NCoA acceptable for use. This is especially useful when addresses are assigned by the access router. The NAR can also rely on its trust relationship with PAR before providing forwarding support for the MN. That is, it may create a forwarding entry for the NCoA subject to "approval" from PAR which it trusts. Finally, the access routers could transfer network-resident contexts, such as access control, QoS, and header compression, in conjunction with handover. **For these operations, the protocol provides "Handover Initiate (HI)" and "Handover Acknowledge (HAck)" messages. Both of these messages MUST be supported** and SHOULD be used. The access routers MUST have necessary security association established by means outside the scope of this document.

Identifier: RQ_001_3007
RFC Clause: 3.1
Type: Recommendation
Applies to: Router

Requirement:
The "Handover Initiate (HI)" and "Handover Acknowledge (HAck)" messages SHOULD be used.

RFC Text:
The protocol also provides the following important functionalities. The access routers can exchange messages to confirm that a proposed NCoA is acceptable. For instance, when an MN sends an FBU from PAR's link, FBack can be delivered after the NAR considers the NCoA acceptable for use. This is especially useful when addresses are assigned by the access router. The NAR can also rely on its trust relationship with PAR before providing forwarding support for the MN. That is, it may create a forwarding entry for the NCoA subject to "approval" from PAR which it trusts. Finally, the access routers could transfer network-resident contexts, such as access control, QoS, and header compression, in conjunction with handover. **For these operations, the protocol provides "Handover Initiate (HI)" and "Handover Acknowledge (HAck)" messages. Both of these messages** MUST be supported and **SHOULD be used**. The access routers MUST have necessary security association established by means outside the scope of this document.

Identifier: RQ_001_3007
RFC Clause: 3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The "Handover Initiate (HI)" and "Handover Acknowledge (HAck)" messages SHOULD be used.

RFC Text:
The protocol also provides the following important functionalities. The access routers can exchange messages to confirm that a proposed NCoA is acceptable. For instance, when an MN sends an FBU from PAR's link, FBack can be delivered after the NAR considers the NCoA acceptable for use. This is especially useful when addresses are assigned by the access router. The NAR can also rely on its trust relationship with PAR before providing forwarding support for the MN. That is, it may create a forwarding entry for the NCoA subject to "approval" from PAR which it trusts. Finally, the access routers could transfer network-resident contexts, such as access control, QoS, and header compression, in conjunction with handover. **For these operations, the protocol provides "Handover Initiate (HI)" and "Handover Acknowledge (HAck)" messages. Both of these messages** MUST be supported and **SHOULD be used**. The access routers MUST have necessary security association established by means outside the scope of this document.

Identifier: RQ_001_3008
RFC Clause: 3.2
Type: Mandatory
Applies to: Router

Requirement:
To ensure that the New CoA (NCoA) used in Fast Binding Update (FBU) does not conflict with an address already in use by some other node on the link, FBU encapsulation within Fast Neighbor Advertisement (FNA) MUST be implemented when the FBU is sent from the New Access Router's (NAR) link.

RFC Text:
With the information provided in the PrRtAdv message, the MN formulates a prospective NCoA and sends an FBU message when a link-specific handover event occurs. The purpose of the FBU is to authorize PAR to bind PCoA to NCoA, so that arriving packets can be tunneled to the new location of the MN. Whenever feasible, the FBU SHOULD be sent from PAR's link. For instance, an internal link-specific trigger could enable FBU transmission from the previous link. When it is not feasible, the FBU is sent from the new link. **Care MUST be taken to ensure that the NCoA used in FBU does not conflict with an address already in use by some other node on the link. For this, FBU encapsulation within FNA MUST be implemented** and SHOULD be used (see below) **when the FBU is sent from NAR's link.**

Identifier: RQ_001_3008
RFC Clause: 3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
To ensure that the New CoA (NCoA) used in Fast Binding Update (FBU) does not conflict with an address already in use by some other node on the link, FBU encapsulation within Fast Neighbor Advertisement (FNA) MUST be implemented when the FBU is sent from the New Access Router's (NAR) link.

RFC Text:
With the information provided in the PrRtAdv message, the MN formulates a prospective NCoA and sends an FBU message when a link-specific handover event occurs. The purpose of the FBU is to authorize PAR to bind PCoA to NCoA, so that arriving packets can be tunneled to the new location of the MN. Whenever feasible, the FBU SHOULD be sent from PAR's link. For instance, an internal link-specific trigger could enable FBU transmission from the previous link. When it is not feasible, the FBU is sent from the new link. **Care MUST be taken to ensure that the NCoA used in FBU does not conflict with an address already in use by some other node on the link. For this, FBU encapsulation within FNA MUST be implemented** and SHOULD be used (see below) **when the FBU is sent from NAR's link.**

Identifier: RQ_001_3009
RFC Clause: 3.2
Type: Recommendation
Applies to: Router

Requirement:
To ensure that the New CoA (NCoA) used in Fast Binding Update (FBU) does not conflict with an address already in use by some other node on the link, FBU encapsulation within Fast Neighbor Advertisement (FNA) SHOULD be used when the FBU is sent from the New Access Router's (NAR) link.

RFC Text:
With the information provided in the PrRtAdv message, the MN formulates a prospective NCoA and sends an FBU message when a link-specific handover event occurs. The purpose of the FBU is to authorize PAR to bind PCoA to NCoA, so that arriving packets can be tunneled to the new location of the MN. Whenever feasible, the FBU SHOULD be sent from PAR's link. For instance, an internal link-specific trigger could enable FBU transmission from the previous link. When it is not feasible, the FBU is sent from the new link. **Care MUST be taken to ensure that the NCoA used in FBU does not conflict with an address already in use by some other node on the link. For this, FBU encapsulation within FNA** MUST be implemented and **SHOULD be used (see below) when the FBU is sent from NAR's link.**

Identifier: RQ_001_3009
RFC Clause: 3.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
To ensure that the New CoA (NCoA) used in Fast Binding Update (FBU) does not conflict with an address already in use by some other node on the link, FBU encapsulation within Fast Neighbor Advertisement (FNA) SHOULD be used when the FBU is sent from the New Access Router's (NAR) link.

RFC Text:
With the information provided in the PrRtAdv message, the MN formulates a prospective NCoA and sends an FBU message when a link-specific handover event occurs. The purpose of the FBU is to authorize PAR to bind PCoA to NCoA, so that arriving packets can be tunneled to the new location of the MN. Whenever feasible, the FBU SHOULD be sent from PAR's link. For instance, an internal link-specific trigger could enable FBU transmission from the previous link. When it is not feasible, the FBU is sent from the new link. **Care MUST be taken to ensure that the NCoA used in FBU does not conflict with an address already in use by some other node on the link. For this, FBU encapsulation within FNA** MUST be implemented and **SHOULD be used (see below) when the FBU is sent from NAR's link.**

Identifier: RQ_001_3010
RFC Clause: 3.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the The Mobile Node (MN) receives a Fast Binding Acknowledgment (FBack) on the previous link.The Mobile Node (MN) SHOULD send Fast Neighbor Advertisement (FNA) immediately after attaching to New Access Router (NAR), so that arriving and buffered packets can be forwarded to the MN right away.

RFC Text:
Depending on whether an FBack is received on the previous link (which clearly depends on whether the FBU was sent in the first place), there are two modes of operation.

1. **The MN receives an FBack on the previous link. This means that packet tunneling is already in progress by the time the MN handovers to NAR. The MN SHOULD send FNA immediately after attaching to NAR, so that arriving and buffered packets can be forwarded to the MN right away.**

   Before sending an FBack to an MN, PAR can determine whether the NCoA is acceptable to the NAR through the exchange of HI and HAck messages. When assigned addressing (i.e., addresses are assigned by the router) is used, the proposed NCoA in the FBU is carried in HI, and the NAR MAY assign the proposed NCoA. Such an assigned NCoA MUST be returned in HAck, and the PAR MUST in turn provide the assigned NCoA in the FBack. If there is an assigned NCoA returned in the FBack, the MN MUST use the assigned address (and not the proposed address in the FBU) upon attaching to NAR.

2. The MN does not receive the FBack on the previous link because the MN has not sent the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack. Without receiving an FBack in the latter case, the MN cannot ascertain whether PAR has successfully processed the FBU. Hence, it (re)sends an FBU as soon as it attaches to NAR. To enable NAR

   to forward packets immediately (when FBU has been processed) and to allow NAR to verify whether NCoA is acceptable, the MN SHOULD encapsulate the FBU in the FNA. If NAR detects that NCoA is in use when processing the FNA, for instance while creating a neighbor entry, it MUST discard the inner FBU packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option in which NAR MAY include an alternate IP address for the MN to use. This discarding avoids the rare and undesirable outcome that results from address collision. Detailed FNA processing rules are specified in Section 6.3.3.

The scenario in which an MN sends an FBU and receives an FBack on PAR's link is illustrated in Figure 2. For convenience, this scenario is characterized as "predictive" mode of operation. The scenario in which the MN sends an FBU from NAR's link is illustrated in Figure 3. For convenience, this scenario is characterized as a "reactive" mode of operation. Note that the reactive mode also includes the case in which an FBU has been sent from PAR's link but an FBack has not been received yet.

Finally, the PrRtAdv message may be sent unsolicited (i.e., without the MN first sending a RtSolPr). This mode is described in Section 3.3.

Identifier: RQ_001_3011
RFC Clause: 3.2
Type: Optional
Applies to: Router

Requirement:
When assigned addressing is used, the proposed New CoA (NCoA) in the Fast Binding Update (FBU) is carried in Handover Initiate (HI), and the New Access Router (NAR) MAY assign the proposed NCoA.

RFC Text:
Depending on whether an FBack is received on the previous link (which clearly depends on whether the FBU was sent in the first place), there are two modes of operation.

1. The MN receives an FBack on the previous link. This means that packet tunneling is already in progress by the time the MN handovers to NAR. The MN SHOULD send FNA immediately after attaching to NAR, so that arriving and buffered packets can be forwarded to the MN right away.

   Before sending an FBack to an MN, PAR can determine whether the NCoA is acceptable to the NAR through the exchange of HI and HAck messages. **When assigned addressing (i.e., addresses are assigned by the router) is used, the proposed NCoA in the FBU is carried in HI, and the NAR MAY assign the proposed NCoA.** Such an assigned NCoA MUST be returned in HAck, and the PAR MUST in turn provide the assigned NCoA in the FBack. If there is an assigned NCoA returned in the FBack, the MN MUST use the assigned address (and not the proposed address in the FBU) upon attaching to NAR.

2. The MN does not receive the FBack on the previous link because the MN has not sent the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack. Without receiving an FBack in the latter case, the MN cannot ascertain whether PAR has successfully processed the FBU. Hence, it (re)sends an FBU as soon as it attaches to NAR. To enable NAR to forward packets immediately (when FBU has been processed) and to allow NAR to verify whether NCoA is acceptable, the MN SHOULD encapsulate the FBU in the FNA. If NAR detects that NCoA is in use when processing the FNA, for instance while creating a neighbor entry, it MUST discard the inner FBU packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option in which NAR MAY include an alternate IP address for the MN to use. This discarding avoids the rare and undesirable outcome that results from address collision. Detailed FNA processing rules are specified in Section 6.3.3.

Identifier: RQ_001_3012
RFC Clause: 3.2
Type: Mandatory
Applies to: Router

Requirement:
When the New Access Router (NAR) assigns the proposed New CoA (NCoA), this NCoA MUST be returned in Handover Acknowledge (HAck).

RFC Text:
Depending on whether an FBack is received on the previous link (which clearly depends on whether the FBU was sent in the first place), there are two modes of operation.

1. The MN receives an FBack on the previous link. This means that packet tunneling is already in progress by the time the MN handovers to NAR. The MN SHOULD send FNA immediately after attaching to NAR, so that arriving and buffered packets can be forwarded to the MN right away.

   Before sending an FBack to an MN, PAR can determine whether the NCoA is acceptable to the NAR through the exchange of HI and HAck messages. **When assigned addressing (i.e., addresses are assigned by the router) is used, the proposed NCoA in the FBU is carried in HI, and the NAR MAY assign the proposed NCoA. Such an assigned NCoA MUST be returned in HAck,** and the PAR MUST in turn provide the assigned NCoA in the FBack. If there is an assigned NCoA returned in the FBack, the MN MUST use the assigned address (and not the proposed address in the FBU) upon attaching to NAR.

2. The MN does not receive the FBack on the previous link because the MN has not sent the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack. Without receiving an FBack in the latter case, the MN cannot ascertain whether PAR has successfully processed the FBU. Hence, it (re)sends an FBU as soon as it attaches to NAR. To enable NAR to forward packets immediately (when FBU has been processed) and to allow NAR to verify whether NCoA is acceptable, the MN SHOULD encapsulate the FBU in the FNA. If NAR detects that NCoA is in use when processing the FNA, for instance while creating a neighbor entry, it MUST discard the inner FBU packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option in which NAR MAY include an alternate IP address for the MN to use. This discarding avoids the rare and undesirable outcome that results from address collision. Detailed FNA processing rules are specified in Section 6.3.3.

Identifier: RQ_001_3013
RFC Clause: 3.2
Type: Mandatory
Applies to: Router

Requirement:

When the New Access Router (NAR) assigns the proposed New CoA (NCoA) and this NCoA is returned in Handover Acknowledge (HAck), the Previous Access Router (PAR) MUST in turn provide the assigned NCoA in the Fast Binding Acknowledgment (FBack).

RFC Text:

Depending on whether an FBack is received on the previous link (which clearly depends on whether the FBU was sent in the first place), there are two modes of operation.

1. The MN receives an FBack on the previous link. This means that packet tunneling is already in progress by the time the MN handovers to NAR. The MN SHOULD send FNA immediately after attaching to NAR, so that arriving and buffered packets can be forwarded to the MN right away.

   Before sending an FBack to an MN, PAR can determine whether the NCoA is acceptable to the NAR through the exchange of HI and HAck messages. **When assigned addressing (i.e., addresses are assigned by the router) is used, the proposed NCoA in the FBU is carried in HI, and the NAR MAY assign the proposed NCoA. Such an assigned NCoA MUST be returned in HAck, and the PAR MUST in turn provide the assigned NCoA in the FBack.** If there is an assigned NCoA returned in the FBack, the MN MUST use the assigned address (and not the proposed address in the FBU) upon attaching to NAR.

2. The MN does not receive the FBack on the previous link because the MN has not sent the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack. Without receiving an FBack in the latter case, the MN cannot ascertain whether PAR has successfully processed the FBU. Hence, it (re)sends an FBU as soon as it attaches to NAR. To enable NAR to forward packets immediately (when FBU has been processed) and to allow NAR to verify whether NCoA is acceptable, the MN SHOULD encapsulate the FBU in the FNA. If NAR detects that NCoA is in use when processing the FNA, for instance while creating a neighbor entry, it MUST discard the inner FBU packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option in which NAR MAY include an alternate IP address for the MN to use. This discarding avoids the rare and undesirable outcome that results from address collision. Detailed FNA processing rules are specified in Section 6.3.3.

Identifier: RQ_001_3014
RFC Clause: 3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If there is an assigned New CoA (NCoA) returned in the Fast Binding Acknowledgment (FBack), the Mobile Node (MN) MUST use the assigned address (and not the proposed address in the FBU) upon attaching to the New Access Router (NAR).

RFC Text:
Depending on whether an FBack is received on the previous link (which clearly depends on whether the FBU was sent in the first place), there are two modes of operation.

1. The MN receives an FBack on the previous link. This means that packet tunneling is already in progress by the time the MN handovers to NAR. The MN SHOULD send FNA immediately after attaching to NAR, so that arriving and buffered packets can be forwarded to the MN right away.

   Before sending an FBack to an MN, PAR can determine whether the NCoA is acceptable to the NAR through the exchange of HI and HAck messages. When assigned addressing (i.e., addresses are assigned by the router) is used, the proposed NCoA in the FBU is carried in HI, and the NAR MAY assign the proposed NCoA. Such an assigned NCoA MUST be returned in HAck, and the PAR MUST in turn provide the assigned NCoA in the FBack. **If there is an assigned NCoA returned in the FBack, the MN MUST use the assigned address (and not the proposed address in the FBU) upon attaching to NAR.**

2. The MN does not receive the FBack on the previous link because the MN has not sent the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack. Without receiving an FBack in the latter case, the MN cannot ascertain whether PAR has successfully processed the FBU. Hence, it (re)sends an FBU as soon as it attaches to NAR. To enable NAR to forward packets immediately (when FBU has been processed) and to allow NAR to verify whether NCoA is acceptable, the MN SHOULD encapsulate the FBU in the FNA. If NAR detects that NCoA is in use when processing the FNA, for instance while creating a neighbor entry, it MUST discard the inner FBU packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option in which NAR MAY include an alternate IP address for the MN to use. This discarding avoids the rare and undesirable outcome that results from address collision. Detailed FNA processing rules are specified in Section 6.3.3.

Identifier: RQ_001_3015
RFC Clause: 3.2
Type: Mandatory
Applies to: Router

Requirement:

If New Access Router (NAR) detects that New CoA (NCoA) is in use when processing the Fast Neighbor Advertisement (FNA), it MUST discard the inner Fast Binding Update (FBU) packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option.

RFC Text:

Depending on whether an FBack is received on the previous link (which clearly depends on whether the FBU was sent in the first place), there are two modes of operation.

1. The MN receives an FBack on the previous link. This means that packet tunneling is already in progress by the time the MN handovers to NAR. The MN SHOULD send FNA immediately after attaching to NAR, so that arriving and buffered packets can be forwarded to the MN right away.

   Before sending an FBack to an MN, PAR can determine whether the NCoA is acceptable to the NAR through the exchange of HI and HAck messages. When assigned addressing (i.e., addresses are assigned by the router) is used, the proposed NCoA in the FBU is carried in HI, and the NAR MAY assign the proposed NCoA. Such an assigned NCoA MUST be returned in HAck, and the PAR MUST in turn provide the assigned NCoA in the FBack. If there is an assigned NCoA returned in the FBack, the MN MUST use the assigned address (and not the proposed address in the FBU) upon attaching to NAR.

2. The MN does not receive the FBack on the previous link because the MN has not sent the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack. Without receiving an FBack in the latter case, the MN cannot ascertain whether PAR has successfully processed the FBU. Hence, it (re)sends an FBU as soon as it attaches to NAR. To enable NAR to forward packets immediately (when FBU has been processed) and to allow NAR to verify whether NCoA is acceptable, the MN SHOULD encapsulate the FBU in the FNA. **If NAR detects that NCoA is in use when processing the FNA, for instance while creating a neighbor entry, it MUST discard the inner FBU packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option** in which NAR MAY include an alternate IP address for the MN to use. This discarding avoids the rare and undesirable outcome that results from address collision. Detailed FNA processing rules are specified in Section 6.3.3.

Identifier: RQ_001_3016
RFC Clause: 3.2
Type: Optional
Applies to: Router

Requirement:
If the New Access Router (NAR) detects that New CoA (NCoA) is in use when processing the Fast Neighbor Advertisement (FNA), it discards the inner Fast Binding Update (FBU) packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option in which the New Access Router (NAR) MAY include an alternate IP address for the Mobile Node (MN) to use.

RFC Text:
Depending on whether an FBack is received on the previous link (which clearly depends on whether the FBU was sent in the first place), there are two modes of operation.

1. The MN receives an FBack on the previous link. This means that packet tunneling is already in progress by the time the MN handovers to NAR. The MN SHOULD send FNA immediately after attaching to NAR, so that arriving and buffered packets can be forwarded to the MN right away.

   Before sending an FBack to an MN, PAR can determine whether the NCoA is acceptable to the NAR through the exchange of HI and HAck messages. When assigned addressing (i.e., addresses are assigned by the router) is used, the proposed NCoA in the FBU is carried in HI, and the NAR MAY assign the proposed NCoA. Such an assigned NCoA MUST be returned in HAck, and the PAR MUST in turn provide the assigned NCoA in the FBack. If there is an assigned NCoA returned in the FBack, the MN MUST use the assigned address (and not the proposed address in the FBU) upon attaching to NAR.

2. The MN does not receive the FBack on the previous link because the MN has not sent the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack. Without receiving an FBack in the latter case, the MN cannot ascertain whether PAR has successfully processed the FBU. Hence, it (re)sends an FBU as soon as it attaches to NAR. To enable NAR to forward packets immediately (when FBU has been processed) and to allow NAR to verify whether NCoA is acceptable, the MN SHOULD encapsulate the FBU in the FNA. **If NAR detects that NCoA is in use when processing the FNA, for instance while creating a neighbor entry, it MUST discard the inner FBU packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option in which NAR MAY include an alternate IP address for the MN to use.** This discarding avoids the rare and undesirable outcome that results from address collision. Detailed FNA processing rules are specified in Section 6.3.3.

Identifier: RQ_001_3017
RFC Clause: 3.2
Type: Optional
Applies to: Router

Requirement:
The Proxy Router Advertisement (PrRtAdv) message may be sent unsolicited.

RFC Text:
Finally, the PrRtAdv message may be sent unsolicited (i.e., without the MN first sending a RtSolPr). This mode is described in Section 3.3.

Identifier: RQ_001_3018
RFC Clause: 3.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In some wireless technologies, the Previous Access Router (PAR) can send an unsolicited Proxy Router Advertisement (PrRtAdv) containing the link layer address, IP address, and subnet prefixes of the New Access Router (NAR) when the network decides that a handover is imminent. Mobile Node (MN) MUST process this Proxy Router Advertisement (PrRtAdv) to configure a new care of address on the new subnet.

RFC Text:
In some wireless technologies, the handover control may reside in the network even though the decision to undergo handover may be mutually arrived at between the MN and the network. In these networks, the PAR can send an unsolicited PrRtAdv containing the link layer address, IP address, and subnet prefixes of the NAR when the network decides that a handover is imminent. The MN MUST process this PrRtAdv to configure a new care of address on the new subnet, and MUST send an FBU to PAR prior to switching to the new link. After transmitting PrRtAdv, the PAR MUST continue to forward packets to the MN on its current link until the FBU is received. The rest of the operation is the same as that described in Section 3.2.

Identifier: RQ_001_3019
RFC Clause: 3.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In some wireless technologies, the Previous Access Router (PAR) can send an unsolicited Proxy Router Advertisement (PrRtAdv) containing the link layer address, IP address, and subnet prefixes of the New Access Router (NAR) when the network decides that a handover is imminent. Mobile Node (MN) processes this Proxy Router Advertisement (PrRtAdv) to configure a new care of address on the new subnet and MUST send an Fast Binding Update (FBU) to Previous Access Router (PAR) prior to switching to the new link.

RFC Text:
In some wireless technologies, the handover control may reside in the network even though the decision to undergo handover may be mutually arrived at between the MN and the network. In these networks, the PAR can send an unsolicited PrRtAdv containing the link layer address, IP address, and subnet prefixes of the NAR when the network decides that a handover is imminent. The MN MUST process this PrRtAdv to configure a new care of address on the new subnet, and MUST send an FBU to PAR prior to switching to the new link. After transmitting PrRtAdv, the PAR MUST continue to forward packets to the MN on its current link until the FBU is received. The rest of the operation is the same as that described in Section 3.2.

Identifier: RQ_001_3020
RFC Clause: 3.3
Type: Mandatory
Applies to: Router

Requirement:
After transmitting Proxy Router Advertisement (PrRtAdv), the Previous Access Router (PAR) MUST continue to forward packets to the Mobile Node (MN) on its current link until the Fast Binding Update (FBU) is received.

RFC Text:
In some wireless technologies, the handover control may reside in the network even though the decision to undergo handover may be mutually arrived at between the MN and the network. In these networks, the PAR can send an unsolicited PrRtAdv containing the link layer address, IP address, and subnet prefixes of the NAR when the network decides that a handover is imminent. The MN MUST process this PrRtAdv to configure a new care of address on the new subnet, and MUST send an FBU to PAR prior to switching to the new link. **After transmitting PrRtAdv, the PAR MUST continue to forward packets to the MN on its current link until the FBU is received. The rest of the operation is the same as that described in Section 3.2.**

Identifier: RQ_001_3021
RFC Clause: 4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
Implementations SHOULD make use of "L2 triggers" whenever possible to initiate the sending of Router Solicitation for Proxy Advertisement (RtSolPr).

RFC Text:
After discovering one or more nearby access points, the MN sends RtSolPr to resolve access point identifiers to subnet router information. This is convenient to do after performing router discovery. However, the MN can send RtSolPr at any time, e.g., when one or more new access points are discovered. The MN can also send RtSolPr more than once during its attachment to PAR. The trigger for sending RtSolPr can originate from a link-specific event, such as the promise of a better signal strength from another access point coupled with fading signal quality with the current access point. Such events, often broadly referred to as "L2 triggers", are outside the scope of this document. Nevertheless, they serve as events that invoke this protocol. For instance, when a "link up" indication is obtained on the new link, protocol messages (e.g., FNA) can be immediately transmitted. **Implementations SHOULD make use of such triggers whenever possible.**

Identifier: RQ_001_3022
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
As a response to Router Solicitation for Proxy Advertisement (RtSolPr), If the Previous Access Router (PAR) does not have an entry corresponding to the new access point, the PAR sends a Proxy Router Advertisement (PrRtAdv) message that indicates it MUST respond indicating that the new access point is unknown and the Mobile Node (MN) MUST stop fast handover protocol operations on the current link.

RFC Text:
As a response to RtSolPr, PAR sends a PrRtAdv message that indicates one of the following possible conditions.

1. **If the PAR does not have an entry corresponding to the new access point, it MUST respond indicating that the new access point is unknown. The MN MUST stop fast handover protocol operations on the current link.** The MN MAY send an FBU from its new link.

2. If the new access point is connected to the PAR's current interface (to which MN is attached), the PAR MUST respond with a Code value indicating that the new access point is connected to the current interface, but not send any prefix information. This scenario could arise, for example, when several wireless access points are bridged into a wired network. No further protocol action is necessary.

3. If the new access point is known and the PAR has information about it, then PAR MUST respond indicating that the new access point is known and supply the [AP-ID, AR-Info] tuple. If the new access point is known, but does not support fast handover, the PAR MUST indicate this with Code 3 (See Section 6.1.2).

4. If a wildcard is supplied as an identifier for the new access point, the PAR SHOULD supply neighborhood [AP-ID, AR-Info] tuples that are subject to path MTU restrictions (i.e., provide any `n' tuples without exceeding the link MTU).

Identifier: RQ_001_3023
RFC Clause: 4
Type: Optional
Applies to: Mobile_Node

Requirement:

ON receipt of a PrRtAdv message indicating that the new access point is unknown and the Mobile Node (MN) MUST stop fast handover protocol operations on the current link, the Mobile Node (MN) MAY send a Fast Binding Update (FBU) from its new link.

RFC Text:

As a response to RtSolPr, PAR sends a PrRtAdv message that indicates one of the following possible conditions.

1. **If the PAR does not have an entry corresponding to the new access point, it MUST respond indicating that the new access point is unknown.** The MN MUST stop fast handover protocol operations on the current link. **The MN MAY send an FBU from its new link.**

2. If the new access point is connected to the PAR's current interface (to which MN is attached), the PAR MUST respond with a Code value indicating that the new access point is connected to the current interface, but not send any prefix information. This scenario could arise, for example, when several wireless access points are bridged into a wired network. No further protocol action is necessary.

3. If the new access point is known and the PAR has information about it, then PAR MUST respond indicating that the new access point is known and supply the [AP-ID, AR-Info] tuple. If the new access point is known, but does not support fast handover, the PAR MUST indicate this with Code 3 (See Section 6.1.2).

4. If a wildcard is supplied as an identifier for the new access point, the PAR SHOULD supply neighborhood [AP-ID, AR-Info] tuples that are subject to path MTU restrictions (i.e., provide any `n' tuples without exceeding the link MTU).

Identifier: RQ_001_3024
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:

As a response to Router Solicitation for Proxy Advertisement (RtSolPr), if the new access point is connected to the Previous Access Router's (PAR) current interface (to which Mobile Node (MN) is attached), the PAR responds with a Proxy Router Advertisement (PrRtAdv) message with a Code value indicating that the new access point is connected to the current interface, but does not send any prefix information.

RFC Text:

As a response to RtSolPr, PAR sends a PrRtAdv message that indicates one of the following possible conditions.

1. If the PAR does not have an entry corresponding to the new access point, it MUST respond indicating that the new access point is unknown. The MN MUST stop fast handover protocol operations on the current link. The MN MAY send an FBU from its new link.

2. **If the new access point is connected to the PAR's current interface (to which MN is attached), the PAR MUST respond with a Code value indicating that the new access point is connected to the current interface, but not send any prefix information. This scenario could arise, for example, when several wireless access points are bridged into a wired network. No further protocol action is necessary.**

3. If the new access point is known and the PAR has information about it, then PAR MUST respond indicating that the new access point is known and supply the [AP-ID, AR-Info] tuple. If the new access point is known, but does not support fast handover, the PAR MUST indicate this with Code 3 (See Section 6.1.2).

4. If a wildcard is supplied as an identifier for the new access point, the PAR SHOULD supply neighborhood [AP-ID, AR-Info] tuples that are subject to path MTU restrictions (i.e., provide any `n' tuples without exceeding the link MTU).

Identifier: RQ_001_3025
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:

As a response to the Router Solicitation for Proxy Advertisement (RtSolPr), if the new access point is known and the Previous Access Router (PAR) has information about it, then PAR MUST respond with a Proxy Router Advertisement (PrRtAdv) message indicating that the new access point is known and supply the [AP-ID, AR-Info] tuple.

RFC Text:

As a response to RtSolPr, PAR sends a PrRtAdv message that indicates one of the following possible conditions.

1. If the PAR does not have an entry corresponding to the new access point, it MUST respond indicating that the new access point is unknown. The MN MUST stop fast handover protocol operations on the current link. The MN MAY send an FBU from its new link.

2. If the new access point is connected to the PAR's current interface (to which MN is attached), the PAR MUST respond with a Code value indicating that the new access point is connected to the current interface, but not send any prefix information. This scenario could arise, for example, when several wireless access points are bridged into a wired network. No further protocol action is necessary.

3. **If the new access point is known and the PAR has information about it, then PAR MUST respond indicating that the new access point is known and supply the [AP-ID, AR-Info] tuple.** If the new access point is known, but does not support fast handover, the PAR MUST indicate this with Code 3 (See Section 6.1.2).

4. If a wildcard is supplied as an identifier for the new access point, the PAR SHOULD supply neighborhood [AP-ID, AR-Info] tuples that are subject to path MTU restrictions (i.e., provide any `n' tuples without exceeding the link MTU).

Identifier: RQ_001_3026
RFC Clause: 4
Type: Recommendation
Applies to: Router

Requirement:
As a response to Router Solicitation for Proxy Advertisement (RtSolPr), if a wildcard is supplied as an identifier for the new access point, then Previous Access Router (PAR) SHOULD respond with a Proxy Router Advertisement (PrRtAdv) message containing neighborhood [AP-ID, AR-Info] tuples that are subject to path MTU restrictions (i.e., provide any `n' tuples without exceeding the link MTU).

RFC Text:
As a response to RtSolPr, PAR sends a PrRtAdv message that indicates one of the following possible conditions.

1. If the PAR does not have an entry corresponding to the new access point, it MUST respond indicating that the new access point is unknown. The MN MUST stop fast handover protocol operations on the current link. The MN MAY send an FBU from its new link.

2. If the new access point is connected to the PAR's current interface (to which MN is attached), the PAR MUST respond with a Code value indicating that the new access point is connected to the current interface, but not send any prefix information. This scenario could arise, for example, when several wireless access points are bridged into a wired network. No further protocol action is necessary.

3. If the new access point is known and the PAR has information about it, then PAR MUST respond indicating that the new access point is known and supply the [AP-ID, AR-Info] tuple. If the new access point is known, but does not support fast handover, the PAR MUST indicate this with Code 3 (See Section 6.1.2).

4. **If a wildcard is supplied as an identifier for the new access point, the PAR SHOULD supply neighborhood [AP-ID, AR-Info] tuples that are subject to path MTU restrictions (i.e., provide any `n' tuples without exceeding the link MTU).**

Identifier: RQ_001_3027
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
Unless the parameters necessary for the MN to send packets immediately upon attaching to the NAR are supplied by the link layer handover mechanism itself, the Router Solicitation for Proxy Advertisement (RtSolPr) and Proxy Router Advertisement (PrRtAdv) messages MUST be implemented by an MN and an access router that supports fast handovers.

RFC Text:
The RtSolPr and PrRtAdv messages MUST be implemented by an MN and an access router that supports fast handovers. However, when the parameters necessary for the MN to send packets immediately upon attaching to the NAR are supplied by the link layer handover mechanism itself, use of above messages is optional on such links.

Identifier: RQ_001_3027
RFC Clause: 4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Unless the parameters necessary for the MN to send packets immediately upon attaching to the NAR are supplied by the link layer handover mechanism itself, the Router Solicitation for Proxy Advertisement (RtSolPr) and Proxy Router Advertisement (PrRtAdv) messages MUST be implemented by an MN and an access router that supports fast handovers.

RFC Text:
The RtSolPr and PrRtAdv messages MUST be implemented by an MN and an access router that supports fast handovers. However, when the parameters necessary for the MN to send packets immediately upon attaching to the NAR are supplied by the link layer handover mechanism itself, use of above messages is optional on such links.

Identifier: RQ_001_3028
RFC Clause: 4
Type: Optional
Applies to: Router

Requirement:
If the parameters necessary for the MN to send packets immediately upon attaching to the New Access Router (NAR) are supplied by the link layer handover mechanism itself, the use of Router Solicitation for Proxy Advertisement (RtSolPr) and Proxy Router Advertisement (PrRtAdv) messages is optional on such links.

RFC Text:
The RtSolPr and PrRtAdv messages MUST be implemented by an MN and an access router that supports fast handovers. However, when the parameters necessary for the MN to send packets immediately upon attaching to the NAR are supplied by the link layer handover mechanism itself, use of above messages is optional on such links.

Identifier: RQ_001_3028
RFC Clause: 4
Type: Optional
Applies to: Mobile_Node

Requirement:
If the parameters necessary for the MN to send packets immediately upon attaching to the New Access Router (NAR) are supplied by the link layer handover mechanism itself, the use of Router Solicitation for Proxy Advertisement (RtSolPr) and Proxy Router Advertisement (PrRtAdv) messages is optional on such links.

RFC Text:
The RtSolPr and PrRtAdv messages MUST be implemented by an MN and an access router that supports fast handovers. However, when the parameters necessary for the MN to send packets immediately upon attaching to the NAR are supplied by the link layer handover mechanism itself, use of above messages is optional on such links.

Identifier: RQ_001_3029
RFC Clause: 4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
After a Proxy Router Advertisement (PrRtAdv) message is processed, the Mobile Node (MN) SHOULD send the FBU from Previous Access Router's (PAR) link whenever "anticipation" of handover is feasible.

RFC Text:
After a PrRtAdv message is processed, the MN sends an FBU at a time determined by link-specific events, and includes the proposed NCoA. The MN SHOULD send the FBU from PAR's link whenever "anticipation" of handover is feasible. When anticipation is not feasible or when it has not received an FBack, the MN sends an FBU immediately after attaching to NAR's link. This FBU SHOULD be encapsulated in an FNA message. The encapsulation allows the NAR to discard the (inner) FBU packet if an address conflict is detected as a result of (outer) FNA packet processing (see FNA processing below). In response to the FBU, the PAR establishes a binding between PCoA ("Home Address") and NCoA, and sends the FBack to the MN. Prior to establishing this binding, PAR SHOULD send an HI message to NAR, and receive HAck in response. To determine the NAR's address for the HI message, the PAR can perform the longest prefix match of NCoA (in FBU) with the prefix list of neighboring access routers. When the source IP address of the FBU is PCoA, i.e., the FBU is sent from the PAR's link, and the HI message MUST have a Code value set to 0; see Section 6.2.1. When the source IP address of the FBU is not PCoA, i.e., the FBU is sent from the NAR's link, the HI message MUST have a Code value of 1; see Section 6.2.1.

Identifier: RQ_001_3030
RFC Clause: 4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When anticipation of handover is not feasible or when, after sending an Fast Binding Update (FBU) it has not received an Fast Binding Acknowledgment (FBack), the Mobile Node (MN) sends an FBU immediately after attaching to New Access Router's(NAR) Link. This FBU SHOULD be encapsulated in an FNA message.

RFC Text:
After a PrRtAdv message is processed, the MN sends an FBU at a time determined by link-specific events, and includes the proposed NCoA. The MN SHOULD send the FBU from PAR's link whenever "anticipation" of handover is feasible. **When anticipation is not feasible or when it has not received an FBack, the MN sends an FBU immediately after attaching to NAR's link. This FBU SHOULD be encapsulated in an FNA message**. The encapsulation allows the NAR to discard the (inner) FBU packet if an address conflict is detected as a result of (outer) FNA packet processing (see FNA processing below). In response to the FBU, the PAR establishes a binding between PCoA ("Home Address") and NCoA, and sends the FBack to the MN. Prior to establishing this binding, PAR SHOULD send an HI message to NAR, and receive HAck in response. To determine the NAR's address for the HI message, the PAR can perform the longest prefix match of NCoA (in FBU) with the prefix list of neighboring access routers. When the source IP address of the FBU is PCoA, i.e., the FBU is sent from the PAR's link, and the HI message MUST have a Code value set to 0; see Section 6.2.1. When the source IP address of the FBU is not PCoA, i.e., the FBU is sent from the NAR's link, the HI message MUST have a Code value of 1; see Section 6.2.1.

Identifier: RQ_001_3031
RFC Clause: 4
Type: Recommendation
Applies to: Router

Requirement:
In response to the FBU, the Previous Access Router (PAR) establishes a binding between Previous CoA (PCoA) ("Home Address") and New CoA (NCoA), and sends the Fast Binding Acknowledgment (FBack) to the Mobile Node (MN). Prior to establishing this binding, Previous Access Router (PAR) SHOULD send an Handover Initiate (HI) message to New Access Router (NAR), and receive Handover Acknowledge (HAck) in response.

RFC Text:
After a PrRtAdv message is processed, the MN sends an FBU at a time determined by link-specific events, and includes the proposed NCoA. The MN SHOULD send the FBU from PAR's link whenever "anticipation" of handover is feasible. When anticipation is not feasible or when it has not received an FBack, the MN sends an FBU immediately after attaching to NAR's link. This FBU SHOULD be encapsulated in an FNA message. The encapsulation allows the NAR to discard the (inner) FBU packet if an address conflict is detected as a result of (outer) FNA packet processing (see FNA processing below). **In response to the FBU, the PAR establishes a binding between PCoA ("Home Address") and NCoA, and sends the FBack to the MN. Prior to establishing this binding, PAR SHOULD send an HI message to NAR, and receive HAck in response**. To determine the NAR's address for the HI message, the PAR can perform the longest prefix match of NCoA (in FBU) with the prefix list of neighboring access routers. When the source IP address of the FBU is PCoA, i.e., the FBU is sent from the PAR's link, and the HI message MUST have a Code value set to 0; see Section 6.2.1. When the source IP address of the FBU is not PCoA, i.e., the FBU is sent from the NAR's link, the HI message MUST have a Code value of 1; see Section 6.2.1.

Identifier: RQ_001_3032
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
When the source IP address of the Fast Binding Update (FBU) is Previous CoA (PCoA), i.e., the FBU is sent from the Previous Access Router's (PAR) link, the HI message MUST have a Code value set to 0.

RFC Text:
After a PrRtAdv message is processed, the MN sends an FBU at a time determined by link-specific events, and includes the proposed NCoA. The MN SHOULD send the FBU from PAR's link whenever "anticipation" of handover is feasible. When anticipation is not feasible or when it has not received an FBack, the MN sends an FBU immediately after attaching to NAR's link. This FBU SHOULD be encapsulated in an FNA message. The encapsulation allows the NAR to discard the (inner) FBU packet if an address conflict is detected as a result of (outer) FNA packet processing (see FNA processing below). In response to the FBU, the PAR establishes a binding between PCoA ("Home Address") and NCoA, and sends the FBack to the MN. Prior to establishing this binding, PAR SHOULD send an HI message to NAR, and receive HAck in response. To determine the NAR's address for the HI message, the PAR can perform the longest prefix match of NCoA (in FBU) with the prefix list of neighboring access routers. **When the source IP address of the FBU is PCoA, i.e., the FBU is sent from the PAR's link, and the HI message MUST have a Code value set to 0; see Section 6.2.1.** When the source IP address of the FBU is not PCoA, i.e., the FBU is sent from the NAR's link, the HI message MUST have a Code value of 1; see Section 6.2.1.

Identifier: RQ_001_3033
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
When the source IP address of the Fast Binding Update (FBU) is not Previous CoA (PCoA), i.e., the FBU is sent from the NAR's link, the HI message MUST have a Code value of 1.

RFC Text:
After a PrRtAdv message is processed, the MN sends an FBU at a time determined by link-specific events, and includes the proposed NCoA. The MN SHOULD send the FBU from PAR's link whenever "anticipation" of handover is feasible. When anticipation is not feasible or when it has not received an FBack, the MN sends an FBU immediately after attaching to NAR's link. This FBU SHOULD be encapsulated in an FNA message. The encapsulation allows the NAR to discard the (inner) FBU packet if an address conflict is detected as a result of (outer) FNA packet processing (see FNA processing below). In response to the FBU, the PAR establishes a binding between PCoA ("Home Address") and NCoA, and sends the FBack to the MN. Prior to establishing this binding, PAR SHOULD send an HI message to NAR, and receive HAck in response. To determine the NAR's address for the HI message, the PAR can perform the longest prefix match of NCoA (in FBU) with the prefix list of neighboring access routers. When the source IP address of the FBU is PCoA, i.e., the FBU is sent from the PAR's link, and the HI message MUST have a Code value set to 0; see Section 6.2.1. **When the source IP address of the FBU is not PCoA, i.e., the FBU is sent from the NAR's link, the HI message MUST have a Code value of 1; see Section 6.2.1.**

Identifier: RQ_001_3034
RFC Clause: 4
Type: Optional
Applies to: Router

Requirement:
In response to a HI message with Code 0, if the New Access Router (NAR) creates a host route entry for Previous CoA (PCoA) in case NCoA cannot be accepted or assigned. The NAR MAY also set up a reverse tunnel to the PAR in this case.

RFC Text:
The HI message contains the PCoA, Link-Layer Address, and the NCoA of the MN. **In response to processing an HI message with Code 0, the NAR**

1. determines whether NCoA supplied in the HI message is a valid address for use. If it is, the NAR starts proxying [6] the address for PROXY_ND_LIFETIME during which the MN is expected to connect to the NAR. The NAR MAY use the Link-Layer Address to verify whether a corresponding IP address exists in its forwarding tables.

2. allocates NCoA for the MN when assigned addressing is used, creates a proxy neighbor cache entry, and begins defending it. The NAR MAY allocate the NCoA proposed in HI.

3. **MAY create a host route entry for PCoA in case NCoA cannot be accepted or assigned. This host route entry SHOULD be implemented such that until the MN's presence is detected, either through explicit announcement by the MN or by other means, arriving packets do not invoke neighbor discovery. The NAR MAY also set up a reverse tunnel to the PAR in this case.**

4. provides the status of the handover request in the Handover Acknowledge (HAck) message.

Identifier: RQ_001_3035
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
In response to a HI message with Code 0, the New Access Router (NAR) provides the status of the handover request in the Handover Acknowledge (HAck) message.

RFC Text:
The HI message contains the PCoA, Link-Layer Address, and the NCoA of the MN. **In response to processing an HI message with Code 0, the NAR**

1. determines whether NCoA supplied in the HI message is a valid address for use. If it is, the NAR starts proxying [6] the address for PROXY_ND_LIFETIME during which the MN is expected to connect to the NAR. The NAR MAY use the Link-Layer Address to verify whether a corresponding IP address exists in its forwarding tables.

2. allocates NCoA for the MN when assigned addressing is used, creates a proxy neighbor cache entry, and begins defending it. The NAR MAY allocate the NCoA proposed in HI.

3. MAY create a host route entry for PCoA in case NCoA cannot be accepted or assigned. This host route entry SHOULD be implemented such that until the MN's presence is detected, either through explicit announcement by the MN or by other means, arriving packets do not invoke neighbor discovery. The NAR MAY also set up a reverse tunnel to the PAR in this case.

4. provides the status of the handover request in the Handover Acknowledge (HAck) message.

Identifier: RQ_001_3036
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
If HAck contains an assigned NCoA, the FBack MUST include it,

RFC Text:
If HAck contains an assigned NCoA, the FBack MUST include it, and the MN MUST use the address provided in the FBack. The PAR MAY send the FBack to the previous link to facilitate faster reception in the event that the MN is still present. The result of the FBU and FBack processing is that PAR begins tunneling the MN's packets to NCoA. If the MN does not receive an FBack message even after retransmitting the FBU for FBU_RETRIES, it MUST assume that fast handover support is not available and stop the protocol operation.

Identifier: RQ_001_3037
RFC Clause: 4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If HAck contains an assigned NCoA, the Mobile Node (MN) MUST use the address provided in the FBack.

RFC Text:
If HAck contains an assigned NCoA, the FBack MUST include it, **and the MN MUST use the address provided in the FBack.** The PAR MAY send the FBack to the previous link to facilitate faster reception in the event that the MN is still present. The result of the FBU and FBack processing is that PAR begins tunneling the MN's packets to NCoA. If the MN does not receive an FBack message even after retransmitting the FBU for FBU_RETRIES, it MUST assume that fast handover support is not available and stop the protocol operation.

Identifier: RQ_001_3038
RFC Clause: 4
Type: Optional
Applies to: Router

Requirement:
If HAck contains an assigned NCoA, the PAR MAY send the FBack to the previous link to facilitate faster reception in the event that the MN is still present.

RFC Text:
If HAck contains an assigned NCoA, the FBack MUST include it, and the MN MUST use the address provided in the FBack. **The PAR MAY send the FBack to the previous link to facilitate faster reception in the event that the MN is still present**. The result of the FBU and FBack processing is that PAR begins tunneling the MN's packets to NCoA. If the MN does not receive an FBack message even after retransmitting the FBU for FBU_RETRIES, it MUST assume that fast handover support is not available and stop the protocol operation.

Identifier: RQ_001_3039
RFC Clause: 4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the Mobile Node (MN) does not receive an FBack message even after retransmitting the Fast Binding Update (FBU) for FBU_RETRIES, it MUST assume that fast handover support is not available and stop the protocol operation.

RFC Text:
If HAck contains an assigned NCoA, the FBack MUST include it, and the MN MUST use the address provided in the FBack. The PAR MAY send the FBack to the previous link to facilitate faster reception in the event that the MN is still present. The result of the FBU and FBack processing is that PAR begins tunneling the MN's packets to NCoA. **If the MN does not receive an FBack message even after retransmitting the FBU for FBU_RETRIES, it MUST assume that fast handover support is not available and stop the protocol operation.**

Identifier: RQ_001_3040
RFC Clause: 4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When the Mobile Node (MN) establishes link connectivity with the NAR, it SHOULD send a Fast Neighbor Advertisement (FNA) message.

RFC Text:
When the MN establishes link connectivity with the NAR, it SHOULD send a Fast Neighbor Advertisement (FNA) message (see 6.3.3). If the MN has not received an FBack by the time the FNA is being sent, it SHOULD encapsulate the FBU in the FNA and send them together.

Identifier: RQ_001_3041
RFC Clause: 4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Mobile Node (MN) has not received an FBack by the time the FNA is being sent, it SHOULD encapsulate the Fast Binding Update (FBU) in the FNA and send them together

RFC Text:
When the MN establishes link connectivity with the NAR, it SHOULD send a Fast Neighbor Advertisement (FNA) message (see 6.3.3). **If the MN has not received an FBack by the time the FNA is being sent, it SHOULD encapsulate the FBU in the FNA and send them together**.

Identifier: RQ_001_3042
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
When the NCoA corresponding to the FNA message is acceptable, the NAR MUST forward any buffered packets.

RFC Text:
When the NCoA corresponding to the FNA message is acceptable, the NAR MUST

1. delete its proxy neighbor cache entry, if any is present.

2. create a neighbor cache entry and set its state to REACHABLE without overwriting an existing entry for a different layer 2 address.

3. **forward any buffered packets**.

4. enable the host route entry for PCoA, if any is present.

Identifier: RQ_001_3043
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
When the NCoA corresponding to the FNA message is not acceptable, the NAR MUST send a Router Advertisement with the NAACK option.

RFC Text:
When the NCoA corresponding to the FNA message is not acceptable, the NAR MUST

1. discard the inner (FBU) packet.

2. **send a Router Advertisement with the NAACK option** in which it MAY include an alternate NCoA for use. This message MUST be sent to the source IP address present in the FNA using the same Layer 2 address present in the FNA.

Identifier: RQ_001_3044
RFC Clause: 4
Type: Optional
Applies to: Router

Requirement:
When the NCoA corresponding to the FNA message is not acceptable and the New Access Router (NAR) sends a Router Advertisement with the NAACK option, it MAY include an alternate NCoA for use.

RFC Text:
When the NCoA corresponding to the FNA message is not acceptable, the NAR MUST

1. discard the inner (FBU) packet.

2. **send a Router Advertisement with the NAACK option in which it MAY include an alternate NCoA for use.** This message MUST be sent to the source IP address present in the FNA using the same Layer 2 address present in the FNA.

Identifier: RQ_001_3045
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
When the NCoA corresponding to the FNA message is not acceptable and the New Access Router (NAR) sends a Router Advertisement with the NAACK option, this message MUST be sent to the source IP address present in the FNA using the same Layer 2 address present in the FNA.

RFC Text:
When the NCoA corresponding to the FNA message is not acceptable, the NAR MUST

1. discard the inner (FBU) packet.

2. **send a Router Advertisement with the NAACK option** in which it MAY include an alternate NCoA for use. **This message MUST be sent to the source IP address present in the FNA using the same Layer 2 address present in the FNA.**

Identifier: RQ_001_3046
RFC Clause: 4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the Mobile Node (MN) receives a Router Advertisement with a NAACK option, it MUST use the IP address, if any, provided in the NAACK option.

RFC Text:
If the MN receives a Router Advertisement with a NAACK option, it MUST use the IP address, if any, provided in the NAACK option. Otherwise, the MN should configure another NCoA. Subsequently, the MN SHOULD send an FBU using the new CoA. As a special case, the address supplied in NAACK could be PCoA itself, in which case the MN MUST NOT send any more FBUs.

Identifier: RQ_001_3047
RFC Clause: 4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Mobile Node (MN) receives a Router Advertisement with a NAACK option that does not provide an IP address, the MN should configure another NCoA.

RFC Text:
If the MN receives a Router Advertisement with a NAACK option, it MUST use the IP address, if any, provided in the NAACK option. Otherwise, the MN should configure another NCoA. Subsequently, the MN SHOULD send an FBU using the new CoA. As a special case, the address supplied in NAACK could be PCoA itself, in which case the MN MUST NOT send any more FBUs.

Identifier: RQ_001_3048
RFC Clause: 4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the Mobile Node (MN) receives a Router Advertisement with a NAACK option that does not provide an IP address, the MN configures another NCoA and SHOULD send an FBU using the new CoA.

RFC Text:
If the MN receives a Router Advertisement with a NAACK option, it MUST use the IP address, if any, provided in the NAACK option. Otherwise, the MN should configure another NCoA. Subsequently, the MN SHOULD send an FBU using the new CoA. As a special case, the address supplied in NAACK could be PCoA itself, in which case the MN MUST NOT send any more FBUs.

Identifier: RQ_001_3049
RFC Clause: 4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the Mobile Node (MN) receives a Router Advertisement with a NAACK option that contains the PCoA itself, the MN MUST NOT send any more FBUs.

RFC Text:
If the MN receives a Router Advertisement with a NAACK option, it MUST use the IP address, if any, provided in the NAACK option. Otherwise, the MN should configure another NCoA. Subsequently, the MN SHOULD send an FBU using the new CoA. As a special case, the address supplied in NAACK could be PCoA itself, in which case the MN MUST NOT send any more FBUs.

Identifier: RQ_001_3050
RFC Clause: 4
Type: Recommendation
Applies to: Mobile_Node

Requirement:
Once the Mobile Node (MN) has confirmed its NCoA, it SHOULD send a Neighbor Advertisement message.

RFC Text:
Once the MN has confirmed its NCoA, it SHOULD send a Neighbor Advertisement message. This message allows MN's neighbors to update their neighbor cache entries with the MN's addresses.

Identifier: RQ_001_3051
RFC Clause: 4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Mobile Node (MN) MUST configure the tunnel end-point address of the PAR using the 128 bit global address contained in the PAR'S router advertisements.

RFC Text:
Just as in Mobile IPv6, the PAR sets the 'R' bit in the Prefix Information option, and includes its 128 bit global address in the router advertisements. This allows the mobile nodes to learn the PAR's global IPv6 address. The MN reverse tunnels its packets to the same global address of PAR. The tunnel end-point addresses MUST be configured accordingly. When PAR receives a reverse tunneled packet, it MUST verify if a secure binding exists for the MN identified by PCoA in the tunneled packet, before forwarding the packet.

Identifier: RQ_001_3052
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
When PAR receives a reverse tunneled packet, it MUST verify if a secure binding exists for the Mobile Node (MN) identified by PCoA in the tunneled packet, before forwarding the packet.

RFC Text:
Just as in Mobile IPv6, the PAR sets the 'R' bit in the Prefix Information option, and includes its 128 bit global address in the router advertisements. This allows the mobile nodes to learn the PAR's global IPv6 address. The MN reverse tunnels its packets to the same global address of PAR. The tunnel end-point addresses MUST be configured accordingly. **When PAR receives a reverse tunneled packet, it MUST verify if a secure binding exists for the MN identified by PCoA in the tunneled packet, before forwarding the packet.**

Identifier: RQ_001_3053
RFC Clause: 5.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The MN expects a PrRtAdv in response to its RtSolPr message. If the MN does not receive a PrRtAdv message even after RTSOLPR_RETRIES, it MUST assume that PAR does not support the fast handover protocol and stop sending RtSolPr messages.

RFC Text:
The MN expects a PrRtAdv in response to its RtSolPr message. If the MN does not receive a PrRtAdv message even after RTSOLPR_RETRIES, it MUST assume that PAR does not support the fast handover protocol and stop sending RtSolPr messages.

Identifier: RQ_001_3054
RFC Clause: 5.2
Type: Mandatory
Applies to: Router

Requirement:
The PAR MUST use the NCoA present in the Fast Binding Update (FBU) in its HI message.

RFC Text:
Typically, the MN formulates its prospective NCoA using the information provided in a PrRtAdv message and sends the FBU. **The PAR MUST use the NCoA present in the FBU in its HI message**. The NAR MUST verify if the NCoA present in HI is already in use. In any case, NAR MUST respond to HI using a HAck, in which it may include another NCoA to use, especially when assigned address configuration is used. If there is a CoA present in HAck, the PAR MUST include it in the FBack message.

Identifier: RQ_001_3055
RFC Clause: 5.2
Type: Mandatory
Applies to: Router

Requirement:
The New Access Router (NAR) MUST respond to HI using a HAck.

RFC Text:
Typically, the MN formulates its prospective NCoA using the information provided in a PrRtAdv message and sends the FBU. The PAR MUST use the NCoA present in the FBU in its HI message. The NAR MUST verify if the NCoA present in HI is already in use. **In any case, NAR MUST respond to HI using a HAck, in which it may include another NCoA to use**, especially when assigned address configuration is used. If there is a CoA present in HAck, the PAR MUST include it in the FBack message.

Identifier: RQ_001_3056
RFC Clause: 5.2
Type: Mandatory
Applies to: Router

Requirement:
If there is a CoA present in HAck, the PAR MUST include it in the FBack message.

RFC Text:
Typically, the MN formulates its prospective NCoA using the information provided in a PrRtAdv message and sends the FBU. The PAR MUST use the NCoA present in the FBU in its HI message. The NAR MUST verify if the NCoA present in HI is already in use. In any case, NAR MUST respond to HI using a HAck, in which it may include another NCoA to use, especially when assigned address configuration is used. **If there is a CoA present in HAck, the PAR MUST include it in the FBack message.**

Identifier: RQ_001_3057
RFC Clause: 5.4
Type: Optional
Applies to: Router

Requirement:
If the NAR does not have the knowledge REQUIRED to assess whether the MN's address is a duplicate before the MN moves to the new subnet, it may indicate this:

- by not confirming the NCoA in the HAck message.
- in the NAACK option in response to the FNA message

RFC Text:
In some cases, the NAR may already have the knowledge REQUIRED to assess whether the MN's address is a duplicate before the MN moves to the new subnet. For example, the NAR can have a list of all nodes on its subnet, perhaps for access control, and by searching this list, it can confirm whether the MN's address is a duplicate. The result of this search is sent back to the PAR in the HAck message. **If such knowledge is not available at the NAR, it may indicate this by not confirming the NCoA in the HAck message. The NAR may also indicate this in the NAACK option in response to the FNA message. In such cases, the MN would have to follow the address configuration procedure according to [6] after attaching to the NAR.**

Identifier: RQ_001_3058
RFC Clause: 5.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
An MN returning to the PAR before updating the necessary bindings when present on the NAR MUST send a Fast Binding Update with the Home Address equal to the MN's PCoA and a lifetime of zero to the PAR.

RFC Text:
An MN returning to the PAR before updating the necessary bindings when present on the NAR MUST send a Fast Binding Update with the Home Address equal to the MN's PCoA and a lifetime of zero to the PAR. The MN should have a security association with the PAR since it performed a fast handover to the NAR. The PAR, upon receiving this Fast Binding Update, will check its set of outgoing (temporary fast handover) tunnels. If it finds a match, it SHOULD tear down that tunnel (i.e., stop forwarding packets for this MN and start delivering packets directly to the node instead). The MN SHOULD NOT attempt to use any of the fast handover mechanisms described in this specification and SHOULD revert back to standard Mobile IPv6.

Identifier: RQ_001_3059
RFC Clause: 5.5
Type: Recommendation
Applies to: Router

Requirement:
The PAR, upon receiving a Fast Binding Update, from a MN returning to the PAR, will check its set of outgoing (temporary fast handover) tunnels. If it finds a match, it SHOULD tear down that tunnel (i.e., stop forwarding packets for this MN and start delivering packets directly to the node instead).

RFC Text:
An MN returning to the PAR before updating the necessary bindings when present on the NAR MUST send a Fast Binding Update with the Home Address equal to the MN's PCoA and a lifetime of zero to the PAR. The MN should have a security association with the PAR since it performed a fast handover to the NAR. **The PAR, upon receiving this Fast Binding Update, will check its set of outgoing (temporary fast handover) tunnels. If it finds a match, it SHOULD tear down that tunnel (i.e., stop forwarding packets for this MN and start delivering packets directly to the node instead)**. The MN SHOULD NOT attempt to use any of the fast handover mechanisms described in this specification and SHOULD revert back to standard Mobile IPv6.

Identifier: RQ_001_3060
RFC Clause: 5.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
An MN returning to the PAR SHOULD NOT attempt to use any of the fast handover mechanisms described in this specification and SHOULD revert back to standard Mobile IPv6.

RFC Text:
An MN returning to the PAR before updating the necessary bindings when present on the NAR MUST send a Fast Binding Update with the Home Address equal to the MN's PCoA and a lifetime of zero to the PAR. The MN should have a security association with the PAR since it performed a fast handover to the NAR. The PAR, upon receiving this Fast Binding Update, will check its set of outgoing (temporary fast handover) tunnels. If it finds a match, it SHOULD tear down that tunnel (i.e., stop forwarding packets for this MN and start delivering packets directly to the node instead). **The MN SHOULD NOT attempt to use any of the fast handover mechanisms described in this specification and SHOULD revert back to standard Mobile IPv6.**

Identifier: RQ_001_3061
RFC Clause: 5.5
Type: Recommendation
Applies to: Router

Requirement:
The default lifetime of temporary tunnels, for the purpose of fast handovers, should be the same as the lifetime value in the Fast Binding Update (FBU) message.

RFC Text:
Temporary tunnels for the purpose of fast handovers should use short lifetimes (a small number of seconds or less). The lifetime of such tunnels should be enough to allow an MN to update all its active bindings. The default lifetime of the tunnel should be the same as the lifetime value in the FBU message.

Identifier: RQ_001_3061
RFC Clause: 5.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The default lifetime of temporary tunnels, for the purpose of fast handovers, should be the same as the lifetime value in the Fast Binding Update (FBU) message.

RFC Text:
Temporary tunnels for the purpose of fast handovers should use short lifetimes (a small number of seconds or less). The lifetime of such tunnels should be enough to allow an MN to update all its active bindings. The default lifetime of the tunnel should be the same as the lifetime value in the FBU message.

Identifier: RQ_001_3062
RFC Clause: 5.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the MN discovers itself on an unanticipated access router, a Fast Binding Update to the PAR SHOULD be sent.

RFC Text:
The effect of erroneous movement is typically limited to the loss of packets since routing can change and the PAR may forward packets toward another router before the MN actually connects to that router. **If the MN discovers itself on an unanticipated access router, a Fast Binding Update to the PAR SHOULD be sent**. Since Fast Binding Updates are authenticated, they supercede the existing binding and packets MUST be redirected to the newly confirmed location of the MN.

Identifier: RQ_001_3063
RFC Clause: 5.5
Type: Mandatory
Applies to: Router

Requirement:
If the MN discovers itself on an unanticipated access router and sends a Fast Binding Update to the PAR. Since Fast Binding Updates are authenticated, they supercede the existing binding and the PAR MUST redirect packets to the newly confirmed location of the MN.

RFC Text:
The effect of erroneous movement is typically limited to the loss of packets since routing can change and the PAR may forward packets toward another router before the MN actually connects to that router. If the MN discovers itself on an unanticipated access router, a Fast Binding Update to the PAR SHOULD be sent. **Since Fast Binding Updates are authenticated, they supercede the existing binding and packets MUST be redirected to the newly confirmed location of the MN.**

Identifier: RQ_001_3064
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
All Router Solicitation for Proxy Advertisement's Link-Layer Address options have the format defined for Link-Layer Address Option in 6.4.3.

RFC Text:
Mobile Nodes send Router Solicitation for Proxy Advertisement in order to prompt routers for Proxy Router Advertisements. **All the Link-Layer Address options have the format defined in 6.4.3.**

Identifier: RQ_001_3064
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
All Router Solicitation for Proxy Advertisement's Link-Layer Address options have the format defined for Link-Layer Address Option in 6.4.3.

RFC Text:
Mobile Nodes send Router Solicitation for Proxy Advertisement in order to prompt routers for Proxy Router Advertisements. **All the Link-Layer Address options have the format defined in 6.4.3.**

Identifier: RQ_001_3065
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Router Solicitation for Proxy Advertisement, the Source Address field shall contain An IP address assigned to the sending interface.

RFC Text:
IP Fields:

Source Address
An IP address assigned to the sending interface.

Destination Address
The address of the Access Router or the all routers multicast address.

Hop Limit 255. See RFC 2461.

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3065
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Router Solicitation for Proxy Advertisement, the Source Address field shall contain An IP address assigned to the sending interface.

RFC Text:
IP Fields:

Source Address
An IP address assigned to the sending interface.

Destination Address
The address of the Access Router or the all routers multicast address.

Hop Limit 255. See RFC 2461.

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3066
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Router Solicitation for Proxy Advertisement, the Destination Address field shall contain the address of the Access Router or the all routers multicast address.

RFC Text:
IP Fields:

Source Address
An IP address assigned to the sending interface.

Destination Address
The address of the Access Router or the all routers multicast address.

Hop Limit 255. See RFC 2461.

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3066
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Router Solicitation for Proxy Advertisement, the Destination Address field shall contain the address of the Access Router or the all routers multicast address.

RFC Text:
IP Fields:

Source Address
An IP address assigned to the sending interface.

Destination Address
The address of the Access Router or the all routers multicast address.

Hop Limit 255. See RFC 2461.

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3067
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Router Solicitation for Proxy Advertisement, the Hop Limit field shall be set to 255.

RFC Text:
IP Fields:

Source Address
An IP address assigned to the sending interface.

Destination Address
The address of the Access Router or the all routers multicast address.

Hop Limit **255.** See RFC 2461.

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3067
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Router Solicitation for Proxy Advertisement, the Hop Limit field shall be set to 255.

RFC Text:
IP Fields:

Source Address
An IP address assigned to the sending interface.

Destination Address
The address of the Access Router or the all routers multicast address.

Hop Limit **255.** See RFC 2461.

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3068
RFC Clause: 6.1.1
Type: Recommendation
Applies to: Router

Requirement:
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include the Authentication Extension Header in the Router Solicitation for Proxy Advertisement message,

RFC Text:
IP Fields:

Source Address
An IP address assigned to the sending interface.

Destination Address
The address of the Access Router or the all routers multicast address.

Hop Limit 255. See RFC 2461.

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3068
RFC Clause: 6.1.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:

If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include the Authentication Extension Header in the Router Solicitation for Proxy Advertisement message,

RFC Text:

IP Fields:

Source Address
An IP address assigned to the sending interface.

Destination Address
The address of the Access Router or the all routers multicast address.

Hop Limit 255. See RFC 2461.

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3069
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:

THe ICMP Router Solicitation for Proxy Advertisement message shall be structured as follows:

Bits	Field
1-8	Type
9-16	Code
17-32	Checksum
33-40	Subtype
41-48	Reserved
49-64	Identified
65- end	Options

RFC Text:

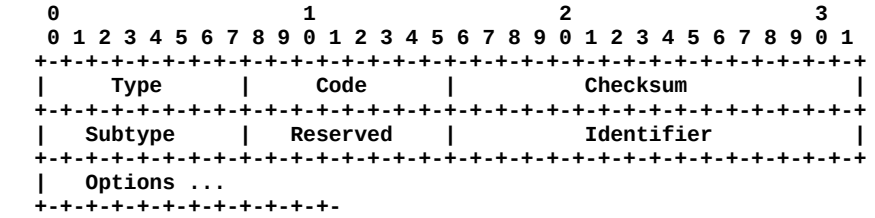


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See [4].
Code	0
Checksum	The ICMPv6 checksum.
Subtype	2
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3069
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:

THe ICMP Router Solicitation for Proxy Advertisement message shall be structured as follows:

Bits	Field
1-8	Type
9-16	Code
17-32	Checksum
33-40	Subtype
41-48	Reserved
49-64	Identified
65- end	Options

RFC Text:

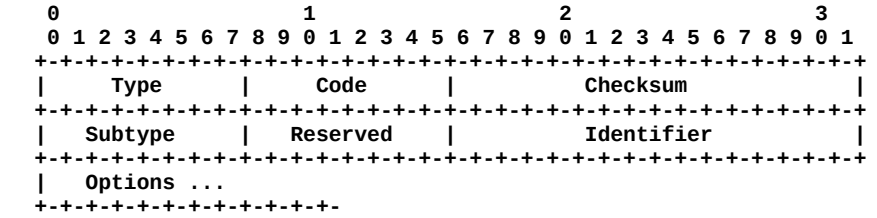


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See [4].
Code	0
Checksum	The ICMPv6 checksum.
Subtype	2
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3070
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message the Type field contains the Experimental Mobility Protocol Type which is 150.

RFC Text:

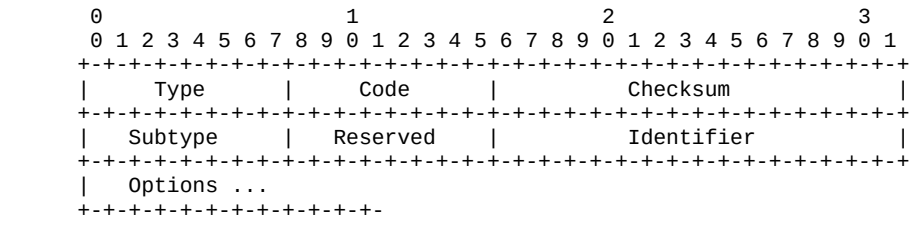


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	**The Experimental Mobility Protocol Type. See [4].**
Code	0
Checksum	The ICMPv6 checksum.
Subtype	2
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3070
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message the Type field contains the Experimental Mobility Protocol Type which is 150.

RFC Text:

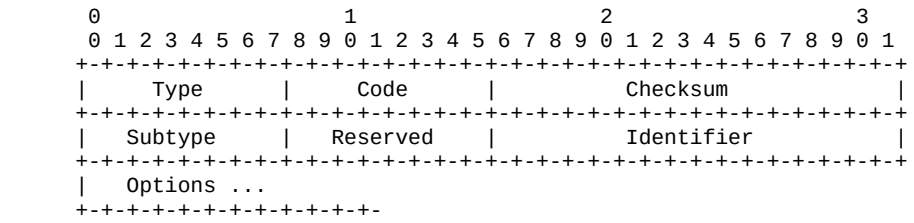


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	**The Experimental Mobility Protocol Type. See [4].**
Code	0
Checksum	The ICMPv6 checksum.
Subtype	2
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3071
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message the Code field contains the value 0.

RFC Text:

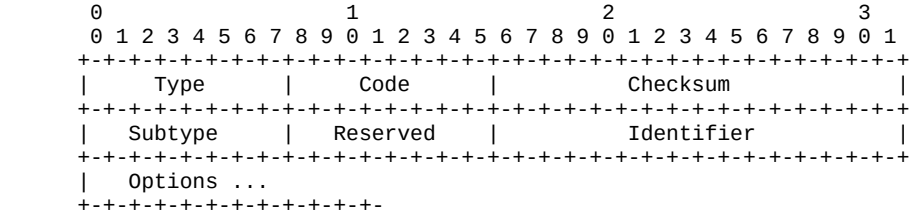


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type — The Experimental Mobility Protocol Type. See [4].

Code — **0**

Checksum — The ICMPv6 checksum.

Subtype — 2

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3071
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message the Code field contains the value 0.

RFC Text:

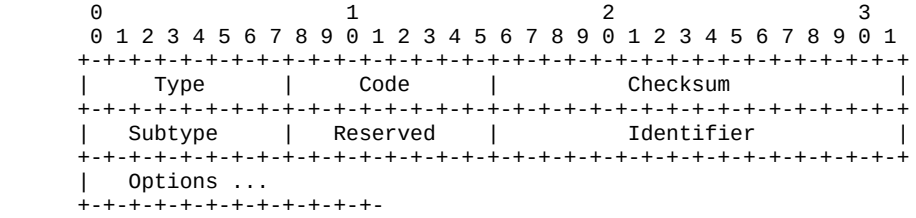


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See [4].
Code	**0**
Checksum	The ICMPv6 checksum.
Subtype	2
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3072
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message the Checksum contains the ICMPv6 checksum.

RFC Text:

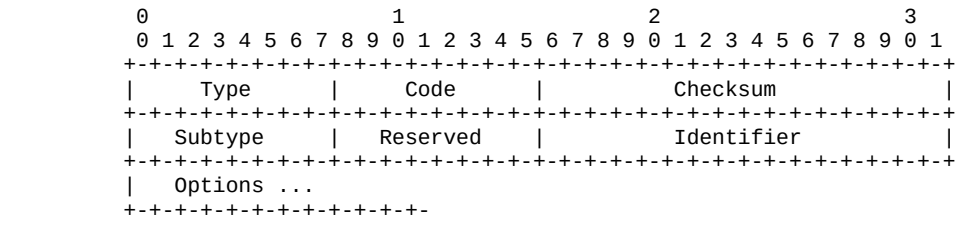


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type — The Experimental Mobility Protocol Type. See [4].

Code — 0

Checksum — The ICMPv6 checksum.

Subtype — 2

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3072
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message the Checksum contains the ICMPv6 checksum.

RFC Text:

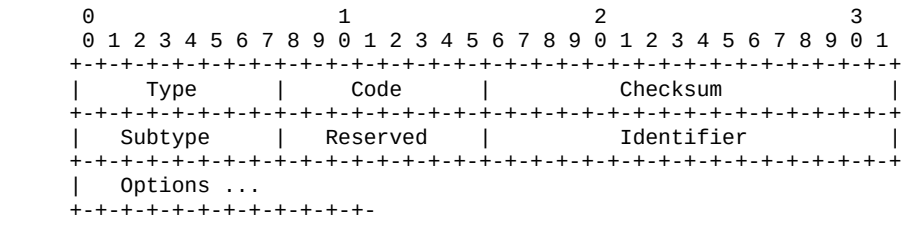


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See [4].
Code	0
Checksum	**The ICMPv6 checksum.**
Subtype	2
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3073
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message the Subtype field contains the value 2.

RFC Text:

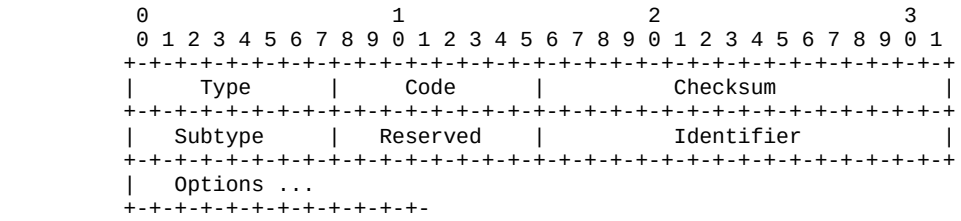


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See [4].
Code	0
Checksum	The ICMPv6 checksum.
Subtype	**2**
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3073
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message the Subtype field contains the value 2.

RFC Text:

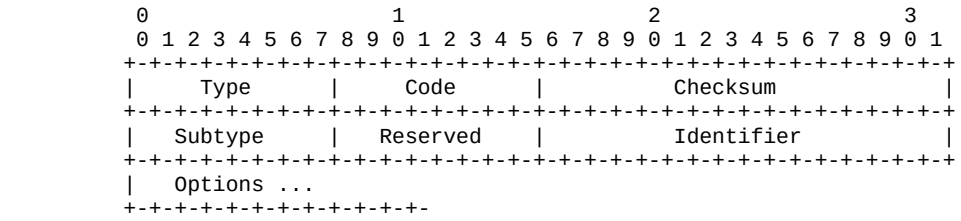


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See [4].
Code	0
Checksum	The ICMPv6 checksum.
Subtype	**2**
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3074
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message the Reserved field MUST be set to zero by the sender.

RFC Text:

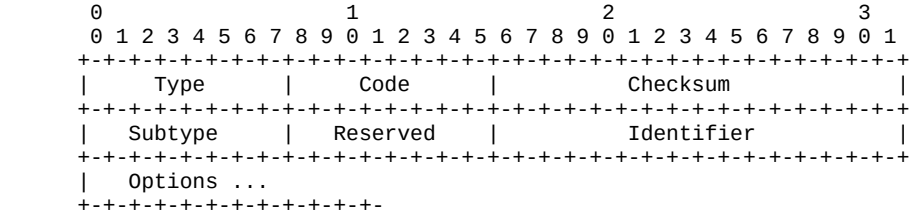


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See [4].
Code	0
Checksum	The ICMPv6 checksum.
Subtype	2
Reserved	**MUST be set to zero by the sender** and ignored by the receiver.
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3075
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message the Reserved field MUST be ignored by the receiver.

RFC Text:

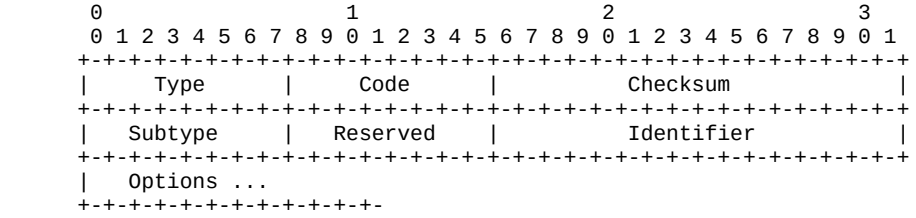


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See [4].
Code	0
Checksum	The ICMPv6 checksum.
Subtype	2
Reserved	**MUST be** set to zero by the sender and **ignored by the receiver.**
Identifier	MUST be set by the sender so that replies can be matched to this Solicitation.

Identifier: RQ_001_3076
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message the Identifier field MUST be set by the sender so that replies can be matched to this Solicitation.

RFC Text:

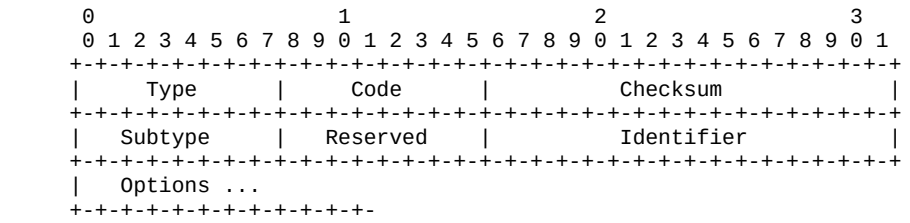


Figure 4: Router Solicitation for Proxy (RtSolPr) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See [4].
Code	0
Checksum	The ICMPv6 checksum.
Subtype	2
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	**MUST be set by the sender so that replies can be matched to this Solicitation**.

Identifier: RQ_001_3077
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message the Valid Options are:

- Source Link-Layer Address
- New Access Point Link-Layer Address

RFC Text:
Valid Options:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point for which the MN requests routing advertisement information. It MUST be included in all RtSolPr messages. More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.

Identifier: RQ_001_3077
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message the Valid Options are:

- Source Link-Layer Address
- New Access Point Link-Layer Address

RFC Text:
Valid Options:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point for which the MN requests routing advertisement information. It MUST be included in all RtSolPr messages. More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.

Identifier: RQ_001_3078
RFC Clause: 6.1.1
Type: Recommendation
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message in the Source Link-Layer Address Option, the Link-Layer Address of the sender, when known, SHOULD be included using the Link-Layer Address option.

RFC Text:
Valid Options:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point for which the MN requests routing advertisement information. It MUST be included in all RtSolPr messages. More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.

Identifier: RQ_001_3078
RFC Clause: 6.1.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message in the Source Link-Layer Address Option, the Link-Layer Address of the sender, when known, SHOULD be included using the Link-Layer Address option.

RFC Text:
Valid Options:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point for which the MN requests routing advertisement information. It MUST be included in all RtSolPr messages. More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.

Identifier: RQ_001_3079
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message in the New Access Point Link-Layer Address Option, the Link-Layer Address or identification of the access point for which the MN requests routing advertisement information MUST be included in all RtSolPr messages.

More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.

RFC Text:
Valid Options:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point for which the MN requests routing advertisement information. It MUST be included in all RtSolPr messages. More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.

Identifier: RQ_001_3079
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message in the New Access Point Link-Layer Address Option, the Link-Layer Address or identification of the access point for which the MN requests routing advertisement information MUST be included in all RtSolPr messages.

More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.

RFC Text:
Valid Options:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point for which the MN requests routing advertisement information. It MUST be included in all RtSolPr messages. More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.

Identifier: RQ_001_3080
RFC Clause: 6.1.1
Type: Optional
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message in the New Access Point Link-Layer Address Option:

- more than one such address or identifier can be present
- this field can also be a wildcard address with all bits set to zero.

RFC Text:
Valid Options:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point for which the MN requests routing advertisement information. It MUST be included in all RtSolPr messages. **More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.**

Identifier: RQ_001_3080
RFC Clause: 6.1.1
Type: Optional
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message in the New Access Point Link-Layer Address Option:

- more than one such address or identifier can be present
- this field can also be a wildcard address with all bits set to zero.

RFC Text:
Valid Options:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point for which the MN requests routing advertisement information. It MUST be included in all RtSolPr messages. **More than one such address or identifier can be present. This field can also be a wildcard address with all bits set to zero.**

Identifier: RQ_001_3081
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
Receivers MUST silently ignore any options that they do not recognize and continue processing the rest of the Router Solicitation for Proxy Advertisement message.

RFC Text:
Future versions of this protocol may define new option types. **Receivers MUST silently ignore any options that they do not recognize and continue processing the rest of the message.**

Identifier: RQ_001_3081
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Receivers MUST silently ignore any options that they do not recognize and continue processing the rest of the Router Solicitation for Proxy Advertisement message.

RFC Text:
Future versions of this protocol may define new option types. **Receivers MUST silently ignore any options that they do not recognize and continue processing the rest of the message.**

Identifier: RQ_001_3082
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Router

Requirement:
In the Router Solicitation for Proxy Advertisement message, when a wildcard is used for a New Access Point LLA, no other New Access Point LLA options MUST be present.

RFC Text:
When a wildcard is used for a New Access Point LLA, no other New Access Point LLA options MUST be present.

Identifier: RQ_001_3082
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Router Solicitation for Proxy Advertisement message, when a wildcard is used for a New Access Point LLA, no other New Access Point LLA options MUST be present.

RFC Text:
When a wildcard is used for a New Access Point LLA, no other New Access Point LLA options MUST be present.

Identifier: RQ_001_3083
RFC Clause: 6.1.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
A Proxy Router Advertisement (PrRtAdv) message should be received by the MN in response to a RtSolPr. If such a message is not received in a timely manner (no less than twice the typical round trip time (RTT) over the access link or 100 milliseconds if RTT is not known), it SHOULD resend the RtSolPr message.

RFC Text:
A Proxy Router Advertisement (PrRtAdv) message should be received by **the MN** in response to a RtSolPr. If such a message is not received in a timely manner (no less than twice the typical round trip time (RTT) over the access link or 100 milliseconds if RTT is not known), it **SHOULD resend the RtSolPr message.** Subsequent retransmissions can be up to RTSOLPR_RETRIES, but MUST use an exponential backoff in which the timeout period (i.e., 2xRTT or 100 milliseconds) is doubled prior to each instance of retransmission. If Proxy Router Advertisement is not received by the time the MN disconnects from the PAR, the MN SHOULD send an FBU immediately after configuring a new CoA.

Identifier: RQ_001_3084
RFC Clause: 6.1.1
Type: Optional
Applies to: Mobile_Node

Requirement:
Following its initial retransmission, subsequent retransmissions of the RtSolPr can be up to RTSOLPR_RETRIES.

RFC Text:
A Proxy Router Advertisement (PrRtAdv) message should be received by the MN in response to a RtSolPr. If such a message is not received in a timely manner (no less than twice the typical round trip time (RTT) over the access link or 100 milliseconds if RTT is not known), it SHOULD resend the RtSolPr message. **Subsequent retransmissions can be up to RTSOLPR_RETRIES**, but MUST use an exponential backoff in which the timeout period (i.e., 2xRTT or 100 milliseconds) is doubled prior to each instance of retransmission. If Proxy Router Advertisement is not received by the time the MN disconnects from the PAR, the MN SHOULD send an FBU immediately after configuring a new CoA.

Identifier: RQ_001_3085
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Following its initial retransmission, subsequent retransmissions of the RtSolPr MUST use an exponential backoff in which the timeout period (i.e., 2xRTT or 100 milliseconds) is doubled prior to each instance of retransmission.

RFC Text:
A Proxy Router Advertisement (PrRtAdv) message should be received by the MN in response to a RtSolPr. If such a message is not received in a timely manner (no less than twice the typical round trip time (RTT) over the access link or 100 milliseconds if RTT is not known), it SHOULD resend the RtSolPr message. **Subsequent retransmissions** can be up to RTSOLPR_RETRIES, but **MUST use an exponential backoff in which the timeout period (i.e., 2xRTT or 100 milliseconds) is doubled prior to each instance of retransmission.** If Proxy Router Advertisement is not received by the time the MN disconnects from the PAR, the MN SHOULD send an FBU immediately after configuring a new CoA.

Identifier: RQ_001_3086
RFC Clause: 6.1.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If a Proxy Router Advertisement is not received by the time the MN disconnects from the PAR, the MN SHOULD send an FBU immediately after configuring a new CoA.

RFC Text:
A Proxy Router Advertisement (PrRtAdv) message should be received by the MN in response to a RtSolPr. If such a message is not received in a timely manner (no less than twice the typical round trip time (RTT) over the access link or 100 milliseconds if RTT is not known), it SHOULD resend the RtSolPr message. Subsequent retransmissions can be up to RTSOLPR_RETRIES, but MUST use an exponential backoff in which the timeout period (i.e., 2xRTT or 100 milliseconds) is doubled prior to each instance of retransmission. **If Proxy Router Advertisement is not received by the time the MN disconnects from the PAR, the MN SHOULD send an FBU immediately after configuring a new CoA.**

Identifier: RQ_001_3087
RFC Clause: 6.1.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When RtSolPr messages are sent more than once, they MUST be rate limited with MAX_RTSOLPR_RATE per second.

RFC Text:
When RtSolPr messages are sent more than once, they MUST be rate limited with MAX_RTSOLPR_RATE per second. During each use of a RtSolPr, exponential backoff is used for retransmissions.

Identifier: RQ_001_3088
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Proxy Router Advertisement, the Source Address MUST be the Link-Local Address assigned to the interface from which this message is sent.

RFC Text:
IP Fields:

Source Address
MUST be the Link-Local Address assigned to the interface from which this message is sent.

Destination Address
The Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3088
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Proxy Router Advertisement, the Source Address MUST be the Link-Local Address assigned to the interface from which this message is sent.

RFC Text:
IP Fields:

Source Address
MUST be the Link-Local Address assigned to the interface from which this message is sent.

Destination Address
The Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3089
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Proxy Router Advertisement, the Destination Address MUST be the Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

RFC Text:
IP Fields:

Source Address
MUST be the Link-Local Address assigned to the interface from which this message is sent.

Destination Address
The Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3089
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Proxy Router Advertisement, the Destination Address MUST be the Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

RFC Text:
IP Fields:

Source Address
MUST be the Link-Local Address assigned to the interface from which this message is sent.

Destination Address
The Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3090
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Proxy Router Advertisement, the Hop Limit MUST be 255.

RFC Text:
IP Fields:

Source Address
MUST be the Link-Local Address assigned to the interface from which this message is sent.

Destination Address
The Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3090
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Proxy Router Advertisement, the Hop Limit MUST be 255.

RFC Text:
IP Fields:

Source Address
MUST be the Link-Local Address assigned to the interface from which this message is sent.

Destination Address
The Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3091
RFC Clause: 6.1.2
Type: Recommendation
Applies to: Router

Requirement:
In the IP Header for the Proxy Router Advertisement, if a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include the Authentication Header.

RFC Text:
IP Fields:

Source Address
MUST be the Link-Local Address assigned to the interface from which this message is sent.

Destination Address
The Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3091
RFC Clause: 6.1.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
In the IP Header for the Proxy Router Advertisement, if a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include the Authentication Header.

RFC Text:
IP Fields:

Source Address
MUST be the Link-Local Address assigned to the interface from which this message is sent.

Destination Address
The Source Address of an invoking Router Solicitation for a Proxy Advertisement or the address of the node the Access Router is instructing to handover.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, the sender SHOULD include this header. See RFC 2402 [5].

Identifier: RQ_001_3092
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message shall be structured as follows:

Bits	Field
1-8	Type
9-16	Code
17-32	Checksum
33-40	Subtype
41-48	Reserved
49-64	Identifier
65-end	Options

RFC Text:

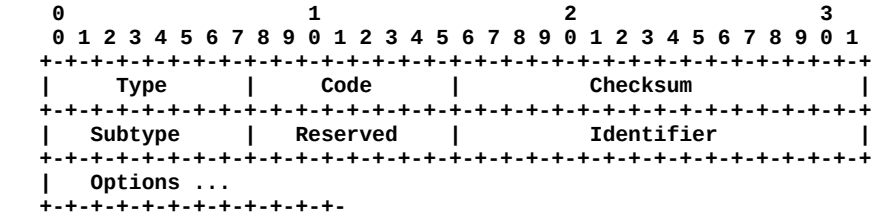


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0, 1, 2, 3 or 4. See below.

Checksum — The ICMPv6 checksum.

Subtype — 3

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3092
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message shall be structured as follows:

Bits	Field
1-8	Type
9-16	Code
17-32	Checksum
33-40	Subtype
41-48	Reserved
49-64	Identifier
65-end	Options

RFC Text:

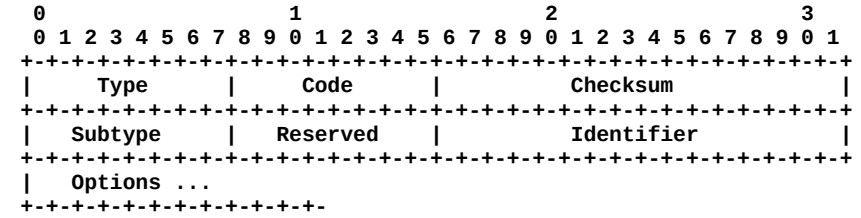


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0, 1, 2, 3 or 4. See below.

Checksum — The ICMPv6 checksum.

Subtype — 3

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3093
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Type field shall be the Experimental Mobility Protocol Type which is 150.

RFC Text:

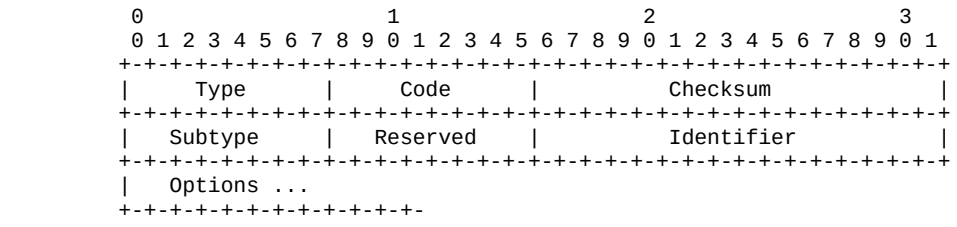


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type **The Experimental Mobility Protocol Type. See RFC 4065 [4].**

Code 0, 1, 2, 3 or 4. See below.

Checksum The ICMPv6 checksum.

Subtype 3

Reserved MUST be set to zero by the sender and ignored by the receiver.

Identifier Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3093
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Type field shall be the Experimental Mobility Protocol Type which is 150.

RFC Text:

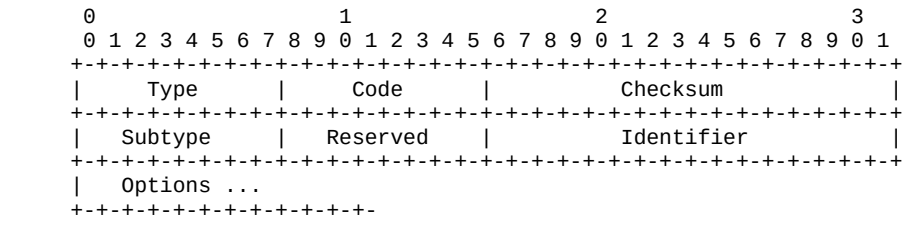


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type **The Experimental Mobility Protocol Type. See RFC 4065 [4].**

Code 0, 1, 2, 3 or 4. See below.

Checksum The ICMPv6 checksum.

Subtype 3

Reserved MUST be set to zero by the sender and ignored by the receiver.

Identifier Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3094
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Code Field shall be set to 0, 1, 2, 3 or 4.

RFC Text:

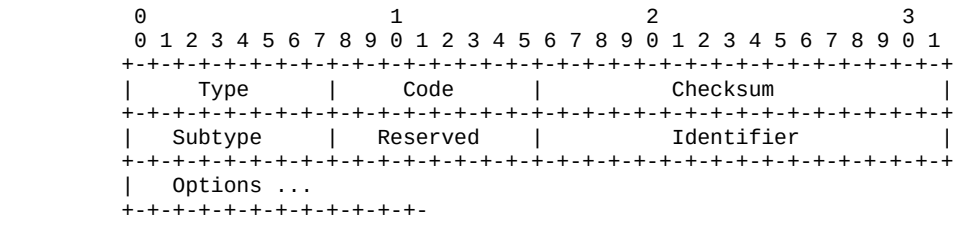


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0, 1, 2, 3 or 4. See below.

Checksum — The ICMPv6 checksum.

Subtype — 3

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3094
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Code Field shall be set to 0, 1, 2, 3 or 4.

RFC Text:

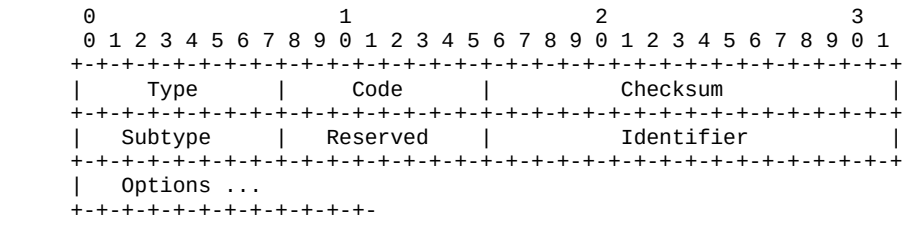


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0, 1, 2, 3 or 4. See below.

Checksum — The ICMPv6 checksum.

Subtype — 3

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3095
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Checksum Field shall contain the ICMPv6 checksum.

RFC Text:

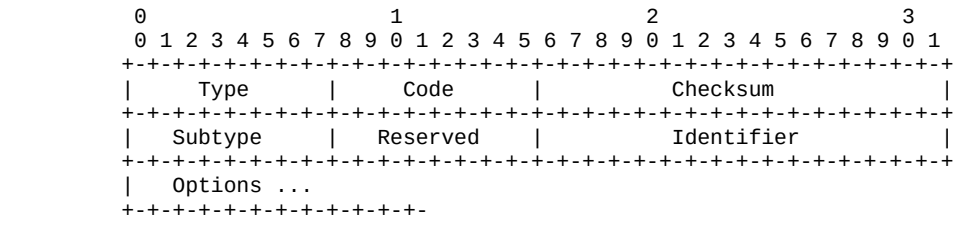


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0, 1, 2, 3 or 4. See below.

Checksum — The ICMPv6 checksum.

Subtype — 3

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3095
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Checksum Field shall contain the ICMPv6 checksum.

RFC Text:

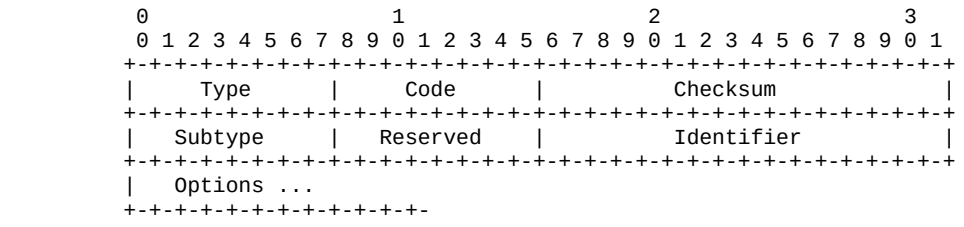


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0, 1, 2, 3 or 4. See below.

Checksum — The ICMPv6 checksum.

Subtype — 3

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3096
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Subtype Field shall be set to 3.

RFC Text:

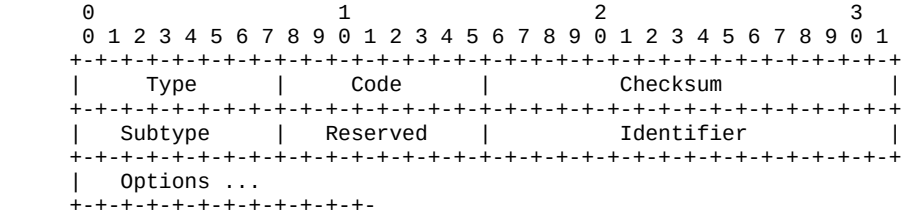


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0, 1, 2, 3 or 4. See below.
Checksum	The ICMPv6 checksum.
Subtype	**3**
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3096
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Subtype Field shall be set to 3.

RFC Text:

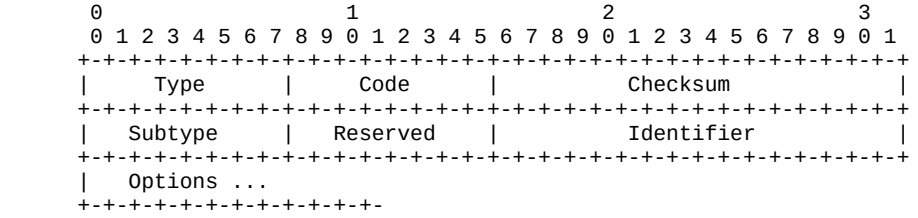


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0, 1, 2, 3 or 4. See below.
Checksum	The ICMPv6 checksum.
Subtype	**3**
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3097
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:

THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Reserved Field MUST be set to zero by the sender.

RFC Text:

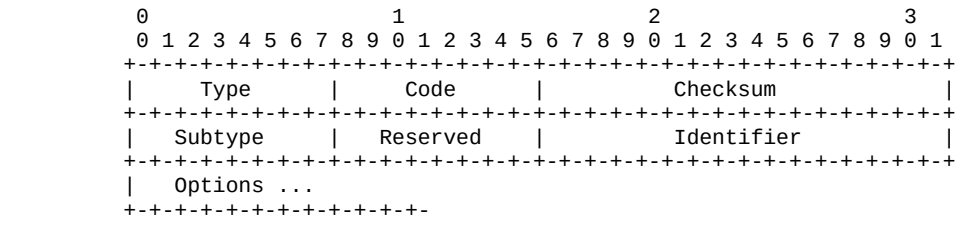


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0, 1, 2, 3 or 4. See below.
Checksum	The ICMPv6 checksum.
Subtype	3
Reserved	**MUST be set to zero by the sender** and ignored by the receiver.
Identifier	Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3098
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
THe ICMP Proxy Router Advertisement (PrRtAdv) Message the Reserved Field MUST be ignored by the receiver.

RFC Text:

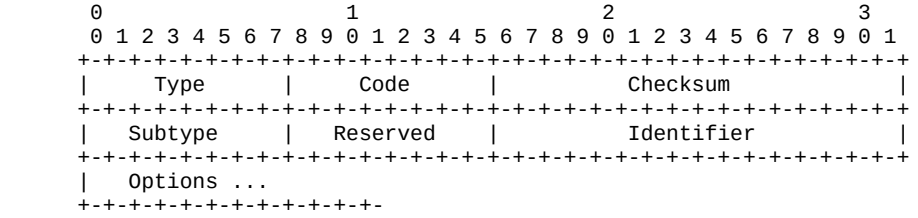


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0, 1, 2, 3 or 4. See below.
Checksum	The ICMPv6 checksum.
Subtype	3
Reserved	MUST be set to zero by the sender and **ignored by the receiver.**
Identifier	Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3099
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message the Identifier Field MUST be:

- Copied from the Router Solicitation for Proxy Advertisement
- or set to Zero if unsolicited.

RFC Text:

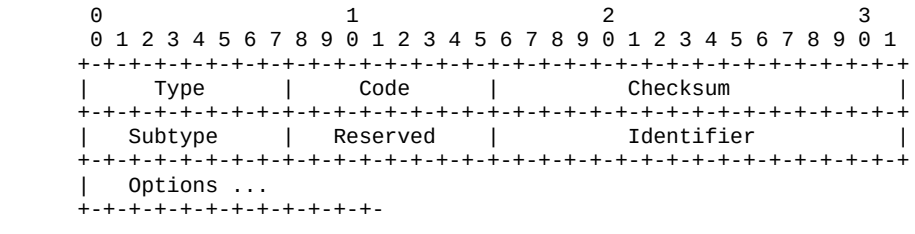


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0, 1, 2, 3 or 4. See below.

Checksum — The ICMPv6 checksum.

Subtype — 3

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Identifier: RQ_001_3099
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message the Identifier Field MUST be:

- Copied from the Router Solicitation for Proxy Advertisement
- or set to Zero if unsolicited.

RFC Text:

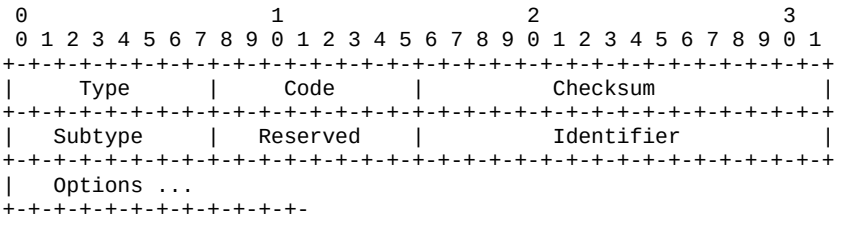


Figure 5: Proxy Router Advertisement (PrRtAdv) Message

ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0, 1, 2, 3 or 4. See below.
Checksum	The ICMPv6 checksum.
Subtype	3
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	**Copied from the Router Solicitation for Proxy Advertisement or set to Zero if unsolicited**.

Identifier: RQ_001_3100
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message the Valid Options, in the following order, are:

- Source Link-Layer Address
- New Access Point Link-Layer Address
- New Router's Link-Layer Address
- New Router's IP Address
- New Router Prefix Information Option.
- New CoA Option

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3100
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message the Valid Options, in the following order, are:

- Source Link-Layer Address
- New Access Point Link-Layer Address
- New Router's Link-Layer Address
- New Router's IP Address
- New Router Prefix Information Option.
- New CoA Option

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3101
RFC Clause: 6.1.2
Type: Recommendation
Applies to: Router

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the Source Link-Layer Address Option is present, when known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3101
RFC Clause: 6.1.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the Source Link-Layer Address Option is present, when known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3102
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the New Access Point Link-Layer Address Option is present, the Link-Layer Address or identification of the access point is copied from the RtSolPr message.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message.
This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3102
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the New Access Point Link-Layer Address Option is present, the Link-Layer Address or identification of the access point is copied from the RtSolPr message.

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message.
This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3103
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message the New Access Point Link-Layer Address Option MUST be present.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. **This option MUST be present.**

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3103
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message the New Access Point Link-Layer Address Option MUST be present.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. **This option MUST be present.**

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3104
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the New Router's Link-Layer Address Option is present, it contains the Link-Layer Address of the Access Router for which this message is proxied.

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3104
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the New Router's Link-Layer Address Option is present, it contains the Link-Layer Address of the Access Router for which this message is proxied.

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3105
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message the New Router's Link-Layer Address Option MUST be included when Code is 0 or 1.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. **This option MUST be included when Code is 0 or 1.**

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3105
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message the New Router's Link-Layer Address Option MUST be included when Code is 0 or 1.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. **This option MUST be included when Code is 0 or 1.**

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3106
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message the New Router's IP Address Option MUST be included when Code Field contains 0 or 1.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. **This option MUST be included when Code is 0 or 1.**

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3106
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message the New Router's IP Address Option MUST be included when Code Field contains 0 or 1.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. **This option MUST be included when Code is 0 or 1.**

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3107
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the New Router's IP Address Option is present it shall contain the IP address of the NAR.

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3107
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the New Router's IP Address Option is present it shall contain the IP address of the NAR.

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3108
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the New Router Prefix Information Option is present it specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3108
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message if the New Router Prefix Information Option is present it specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration.

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3109
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Router

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message, the New Router Prefix Information Option MUST be included when Code is 0 or 1 unless this prefix is the same as that used in the New Router's IP Address option in which case it need not be present.

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. **This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.**

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3109
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the ICMP Proxy Router Advertisement (PrRtAdv) Message, the New Router Prefix Information Option MUST be included when Code is 0 or 1 unless this prefix is the same as that used in the New Router's IP Address option in which case it need not be present.

RFC Text:

Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. **This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.**

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited. PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3110
RFC Clause: 6.1.2
Type: Optional
Applies to: Router

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message, the New CoA Option MAY be present when a PrRtAdv is sent unsolicited.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited.
PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3110
RFC Clause: 6.1.2
Type: Optional
Applies to: Mobile_Node

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message, the New CoA Option MAY be present when a PrRtAdv is sent unsolicited.

RFC Text:
Valid Options in the following order:

Source Link-Layer Address
When known, the Link-Layer Address of the sender SHOULD be included using the Link-Layer Address option. See the LLA option format below.

New Access Point Link-Layer Address
The Link-Layer Address or identification of the access point is copied from the RtSolPr message. This option MUST be present.

New Router's Link-Layer Address
The Link-Layer Address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address
The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option.
Specifies the prefix of the Access Router for which the message is proxied and is used for address auto-configuration. This option MUST be included when Code is 0 or 1. However, when this prefix is the same as that used in the New Router's IP Address option (above), the Prefix Information option need not be present.

New CoA Option
MAY be present when a PrRtAdv is sent unsolicited.
PAR MAY compute a new CoA using NAR's prefix information and the MN's L2 address, or by any other means.

Identifier: RQ_001_3111
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the ICMP Proxy Router Advertisement (PrRtAdv) Message, receivers MUST silently ignore any options they do not recognize and continue processing the message.

RFC Text:
Future versions of this protocol may define new option types. **Receivers MUST silently ignore any options they do not recognize and continue processing the message.**

Identifier: RQ_001_3112
RFC Clause: 6.1.2
Type: Recommendation
Applies to: Mobile_Node

Requirement:
When a Mobile Node (MN) receives a Proxy Router Advertisement with Code 2 and the Option-Code field in the New Access Point LLA option is 6, the MN SHOULD attempt to send an FBU as soon as it regains connectivity with the NAR.

RFC Text:
A Proxy Router Advertisement with Code 2 means that no new router information is present. Each New Access Point LLA option contains an Option-Code value (described below) that indicates a specific outcome.

- When the Option-Code field in the New Access Point LLA option is 5, handover to that access point does not require a change of CoA. No other options are REQUIRED in this case.

- **When the Option-Code field in the New Access Point LLA option is 6, the PAR is not aware of the Prefix Information requested. The MN SHOULD attempt to send an FBU as soon as it regains connectivity with the NAR. No other options are REQUIRED in this case.**

- When the Option-Code field in the New Access Point LLA option is 7, it means that the NAR does not support fast handover. The MN MUST stop fast handover protocol operations. No other options are REQUIRED in this case.

Identifier: RQ_001_3113
RFC Clause: 6.1.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
When a Mobile Node (MN) receives a Proxy Router Advertisement with Code 2 and the Option-Code field in the New Access Point LLA option is 7, the MN MUST stop fast handover protocol operations.

RFC Text:
A Proxy Router Advertisement with Code 2 means that no new router information is present. Each New Access Point LLA option contains an Option-Code value (described below) that indicates a specific outcome.

- When the Option-Code field in the New Access Point LLA option is 5, handover to that access point does not require a change of CoA. No other options are REQUIRED in this case.

- When the Option-Code field in the New Access Point LLA option is 6, the PAR is not aware of the Prefix Information requested. The MN SHOULD attempt to send an FBU as soon as it regains connectivity with the NAR. No other options are REQUIRED in this case.

- **When the Option-Code field in the New Access Point LLA option is 7, it means that the NAR does not support fast handover. The MN MUST stop fast handover protocol operations.** No other options are REQUIRED in this case.

Identifier: RQ_001_3114
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Handover Initiate, the Source Address MUST be the IP address of the PAR.

RFC Text:
IP Fields:

Source Address
The IP address of the PAR.

Destination Address
The IP address of the NAR.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
The authentication header MUST be used when this message is sent. See RFC 2402 [5].

Identifier: RQ_001_3115
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Handover Initiate, the Destination Address MUST be the IP address of the NAR.

RFC Text:
IP Fields:

Source Address
The IP address of the PAR.

Destination Address
The IP address of the NAR.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
The authentication header MUST be used when this message is sent. See RFC 2402 [5].

Identifier: RQ_001_3116
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Handover Initiate, the Hop Limit MUST be 255.

RFC Text:
IP Fields:

Source Address
The IP address of the PAR.

Destination Address
The IP address of the NAR.

Hop Limit **255.** See RFC 2461 [6].

Authentication Header
The authentication header MUST be used when this message is sent. See RFC 2402 [5].

Identifier: RQ_001_3117
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Handover Initiate, the authentication header MUST be used when this message is sent.

RFC Text:
IP Fields:

Source Address
The IP address of the PAR.

Destination Address
The IP address of the NAR.

Hop Limit 255. See RFC 2461 [6].

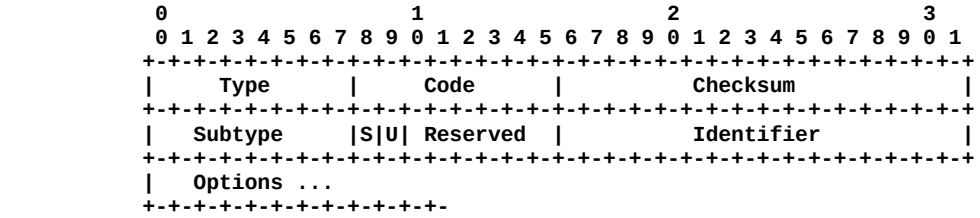
Authentication Header
The authentication header MUST be used when this message is sent. See RFC 2402 [5].

Identifier: RQ_001_3118
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
The ICMP Handover Initiate message shall be structured as follows:

Bits	Field
1-8	Type
9-16	Code
17-32	Checksum
33-40	Subtype
41	S bit
42	U bit
43-48	Reserved
49-64	Identifier
65-end	Options

RFC Text:
The Handover Initiate (HI) is an ICMPv6 message sent by an Access Router (typically PAR) to another Access Router (typically NAR) to initiate the process of a MN's handover.



Identifier: RQ_001_3119
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the Type field shall be the Experimental Mobility Protocol Type which is 150.

RFC Text:
ICMP Fields:

Type	**The Experimental Mobility Protocol Type. See RFC 4065 [4].**
Code	0 or 1. See below
Checksum	The ICMPv6 checksum.
Subtype	4
S flag	Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. MUST be 0 when Code = 1.
U flag	Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3120
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the Code field shall be 0 or 1.

RFC Text:
ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	**0 or 1.** See below
Checksum	The ICMPv6 checksum.
Subtype	4
S flag	Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. MUST be 0 when Code = 1.
U flag	Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3121
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the Checksum field shall contain the ICMPv6 checksum.

RFC Text:
ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0 or 1. See below

Checksum — The ICMPv6 checksum.

Subtype — 4

S flag — Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. MUST be 0 when Code = 1.

U flag — Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3122
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the Subtype field is set to 4.

RFC Text:
ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0 or 1. See below

Checksum — The ICMPv6 checksum.

Subtype — 4

S flag — Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. MUST be 0 when Code = 1.

U flag — Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3123
RFC Clause: 6.2.1
Type: Optional
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the S flag may be set when Code = 0.

RFC Text:
ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0 or 1. See below
Checksum	The ICMPv6 checksum.
Subtype	4
S flag	Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. **May be set when Code = 0.** MUST be 0 when Code = 1.
U flag	Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3124
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the S flag MUST be 0 when Code = 1.

RFC Text:
ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0 or 1. See below
Checksum	The ICMPv6 checksum.
Subtype	4
S flag	Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. **MUST be 0 when Code = 1.**
U flag	Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3125
RFC Clause: 6.2.1
Type: Recommendation
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the U flag SHOULD be set to 0 when Code = 1.

RFC Text:
ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0 or 1. See below
Checksum	The ICMPv6 checksum.
Subtype	4
S flag	Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. MUST be 0 when Code = 1.
U flag	Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, **SHOULD be set to 0 when Code = 1.**
Reserved	MUST be set to zero by the sender and ignored by the receiver.
Identifier	MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3126
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the Reserved Field MUST be set to zero by the sender.

RFC Text:
ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0 or 1. See below
Checksum	The ICMPv6 checksum.
Subtype	4
S flag	Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. MUST be 0 when Code = 1.
U flag	Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.
Reserved	**MUST be set to zero by the sender** and ignored by the receiver.
Identifier	MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3127
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the Reserved Field MUST be ignored by the receiver.

RFC Text:
ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0 or 1. See below
Checksum	The ICMPv6 checksum.
Subtype	4
S flag	Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. MUST be 0 when Code = 1.
U flag	Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.
Reserved	MUST be set to zero by the sender and **ignored by the receiver.**
Identifier	MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3128
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Handover Initiate Message the Identifier Field MUST be set by the sender.

RFC Text:
ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code — 0 or 1. See below

Checksum — The ICMPv6 checksum.

Subtype — 4

S flag — Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. MUST be 0 when Code = 1.

U flag — Buffer flag. When set, the destination SHOULD buffer any packets moving toward the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — MUST be set by the sender so replies can be matched to this message.

Identifier: RQ_001_3129
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Handover Initiate Message the "Link-Layer Address of MN" Options MUST be included so that the destination can recognize the MN.

RFC Text:
Valid Options:

Link-Layer Address of MN
The Link-Layer Address of the MN that is undergoing handover to the destination (i.e., NAR). This option MUST be included so that the destination can recognize the MN.

Previous Care of Address
The IP address used by the MN while attached to the originating router. This option SHOULD be included so that a host route can be established if necessary.

New Care of Address
The IP address the MN wishes to use when connected to the destination. When the `S' bit is set, the NAR MAY assign this address.

Identifier: RQ_001_3130
RFC Clause: 6.2.1
Type: Recommendation
Applies to: Router

Requirement:
In the ICMP Handover Initiate Message the "Previous Care of Address" Options SHOULD be included so that a host route can be established if necessary.

RFC Text:
Valid Options:

Link-Layer Address of MN
The Link-Layer Address of the MN that is undergoing handover to the destination (i.e., NAR). This option MUST be included so that the destination can recognize the MN.

Previous Care of Address
The IP address used by the MN while attached to the originating router. This option SHOULD be included so that a host route can be established if necessary.

New Care of Address
The IP address the MN wishes to use when connected to the destination. When the `S' bit is set, the NAR MAY assign this address.

Identifier: RQ_001_3131
RFC Clause: 6.2.1
Type: Optional
Applies to: Router

Requirement:
In the ICMP Handover Initiate Message the "New Care of Address" Options MAY be When the `S' bit is set.

RFC Text:
Valid Options:

Link-Layer Address of MN
The Link-Layer Address of the MN that is undergoing handover to the destination (i.e., NAR). This option MUST be included so that the destination can recognize the MN.

Previous Care of Address
The IP address used by the MN while attached to the originating router. This option SHOULD be included so that a host route can be established if necessary.

New Care of Address
The IP address the MN wishes to use when connected to the destination. When the `S' bit is set, the NAR MAY assign this address.

Identifier: RQ_001_3132
RFC Clause: 6.2.1
Type: Recommendation
Applies to: Router

Requirement:
If a Handover Acknowledge (HAck) message is not received as a response to the the Handover Initiate in a short time period (no less than twice the typical RTT between source and destination, or 100 milliseconds if RTT is not known), the Handover Initiate SHOULD be resent.

RFC Text:
If a Handover Acknowledge (HAck) message is not received as a response in a short time period (no less than twice the typical RTT between source and destination, or 100 milliseconds if RTT is not known), the Handover Initiate SHOULD be resent. Subsequent retransmissions can be up to HI_RETRIES, but MUST use exponential backoff in which the timeout period (i.e., 2xRTT or 100 milliseconds) is doubled during each instance of retransmission.

Identifier: RQ_001_3133
RFC Clause: 6.2.1
Type: Optional
Applies to: Router

Requirement:
If a Handover Acknowledge (HAck) message is not received as a response to the the Handover Initiate and the Handover Initiate is resent, subsequent retransmissions can be up to HI_RETRIES.

RFC Text:
If a Handover Acknowledge (HAck) message is not received as a response in a short time period (no less than twice the typical RTT between source and destination, or 100 milliseconds if RTT is not known), the Handover Initiate SHOULD be resent. Subsequent retransmissions can be up to HI_RETRIES, but MUST use exponential backoff in which the timeout period (i.e., 2xRTT or 100 milliseconds) is doubled during each instance of retransmission.

Identifier: RQ_001_3134
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
If a Handover Acknowledge (HAck) message is not received as a response to the the Handover Initiate and the Handover Initiate is resent, subsequent retransmissions MUST use exponential backoff in which the timeout period (i.e., 2xRTT or 100 milliseconds) is doubled during each instance of retransmission.

RFC Text:
If a Handover Acknowledge (HAck) message is not received as a response in a short time period (no less than twice the typical RTT between source and destination, or 100 milliseconds if RTT is not known), the Handover Initiate SHOULD be resent. Subsequent retransmissions can be up to HI_RETRIES, but **MUST use exponential backoff in which the timeout period (i.e., 2xRTT or 100 milliseconds) is doubled during each instance of retransmission.**

Identifier: RQ_001_3135
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
The Handover Acknowledgment message is a new ICMPv6 message that MUST be sent as a reply to the Handover Initiate message.

RFC Text:
The Handover Acknowledgment message is a new ICMPv6 message that MUST be sent (typically by NAR to PAR) as a reply to the Handover Initiate message.

Identifier: RQ_001_3136
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Handover Acknowledge, the Source Address MUST be copied from the destination address of the Handover Initiate Message to which this message is a response.

RFC Text:
IP Fields:

Source Address
Copied from the destination address of the Handover Initiate Message to which this message is a response.

Destination Address
Copied from the source address of the Handover Initiate Message to which this message is a response.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
The authentication header MUST be used when this message is sent. See RFC 2402 [5].

Identifier: RQ_001_3137
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Handover Acknowledge, the Destination Address MUST be copied from the source address of the Handover Initiate Message to which this message is a response.

RFC Text:
IP Fields:

Source Address
Copied from the destination address of the Handover Initiate Message to which this message is a response.

Destination Address
Copied from the source address of the Handover Initiate Message to which this message is a response.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
The authentication header MUST be used when this message is sent. See RFC 2402 [5].

Identifier: RQ_001_3138
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Handover Acknowledge, the Hop Limit MUST be set to 255.

RFC Text:
IP Fields:

Source Address
Copied from the destination address of the Handover Initiate Message to which this message is a response.

Destination Address
Copied from the source address of the Handover Initiate Message to which this message is a response.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
The authentication header MUST be used when this message is sent. See RFC 2402 [5].

Identifier: RQ_001_3139
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Handover Acknowledge, the authentication header MUST be used when this message is sent.

RFC Text:
IP Fields:

Source Address
Copied from the destination address of the Handover Initiate Message to which this message is a response.

Destination Address
Copied from the source address of the Handover Initiate Message to which this message is a response.

Hop Limit 255. See RFC 2461 [6].

Authentication Header
The authentication header MUST be used when this message is sent. See RFC 2402 [5].

Identifier: RQ_001_3140
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
The ICMP Handover Acknowledge message shall be structured as follows:

Bits	Field
1-8	Type
9-16	Code
17-32	Checksum
33-40	Subtype
41-48	Reserved
49-64	Identifier
65-end	Options

RFC Text:

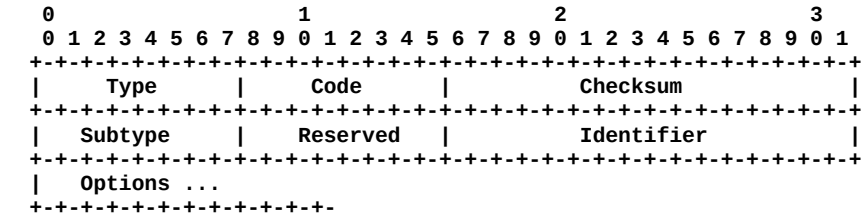


Figure 7: Handover Acknowledge (HAck) Message

Identifier: RQ_001_3141
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
THe ICMP Handover Acknowledge Message the Type field shall be the Experimental Mobility Protocol Type which is 150.

RFC Text:
ICMP Fields:

Type **The Experimental Mobility Protocol Type. See RFC 4065 [4].**

Code

0: Handover Accepted, NCoA valid
1: Handover Accepted, NCoA not valid
2: Handover Accepted, NCoA in use
3: Handover Accepted, NCoA assigned (used in Assigned addressing)
4: Handover Accepted, NCoA not assigned (used in Assigned addressing)
128: Handover Not Accepted, reason unspecified
129: Administratively prohibited
130: Insufficient resources

Checksum The ICMPv6 checksum.

Subtype 5

Reserved MUST be set to zero by the sender and ignored by the receiver.

Identifier Copied from the corresponding field in the Handover Initiate message to which this message is a response.

Identifier: RQ_001_3142
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Handover Acknowledge Message the Code field shall be 0, 1, 2, 3, 4, 128, 129 or 130.

RFC Text:
ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code

0: Handover Accepted, NCoA valid
1: Handover Accepted, NCoA not valid
2: Handover Accepted, NCoA in use
3: Handover Accepted, NCoA assigned (used in Assigned addressing)
4: Handover Accepted, NCoA not assigned (used in Assigned addressing)
128: Handover Not Accepted, reason unspecified
129: Administratively prohibited
130: Insufficient resources

Checksum — The ICMPv6 checksum.

Subtype — 5

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the corresponding field in the Handover Initiate message to which this message is a response.

Identifier: RQ_001_3143
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Handover Acknowledge Message the Checksum field shall contain the ICMPv6 checksum.

RFC Text:
ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code

0: Handover Accepted, NCoA valid
1: Handover Accepted, NCoA not valid
2: Handover Accepted, NCoA in use
3: Handover Accepted, NCoA assigned (used in Assigned addressing)
4: Handover Accepted, NCoA not assigned (used in Assigned addressing)
128: Handover Not Accepted, reason unspecified
129: Administratively prohibited
130: Insufficient resources

Checksum — **The ICMPv6 checksu**m.

Subtype — 5

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the corresponding field in the Handover Initiate message to which this message is a response.

Identifier: RQ_001_3144
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Handover Acknowledge Message the Subtype field is set to 5.

RFC Text:
ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code

0: Handover Accepted, NCoA valid
1: Handover Accepted, NCoA not valid
2: Handover Accepted, NCoA in use
3: Handover Accepted, NCoA assigned (used in Assigned addressing)
4: Handover Accepted, NCoA not assigned (used in Assigned addressing)
128: Handover Not Accepted, reason unspecified
129: Administratively prohibited
130: Insufficient resources

Checksum — The ICMPv6 checksum.

Subtype — **5**

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the corresponding field in the Handover Initiate message to which this message is a response.

Identifier: RQ_001_3145
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Handover Acknowledge Message the Reserved field MUST be set to zero by the sender.

RFC Text:
ICMP Fields:

Type	The Experimental Mobility Protocol Type. See RFC 4065 [4].
Code	0: Handover Accepted, NCoA valid 1: Handover Accepted, NCoA not valid 2: Handover Accepted, NCoA in use 3: Handover Accepted, NCoA assigned (used in Assigned addressing) 4: Handover Accepted, NCoA not assigned (used in Assigned addressing) 128: Handover Not Accepted, reason unspecified 129: Administratively prohibited 130: Insufficient resources
Checksum	The ICMPv6 checksum.
Subtype	5
Reserved	**MUST be set to zero by the sender** and ignored by the receiver.
Identifier	Copied from the corresponding field in the Handover Initiate message to which this message is a response.

Identifier: RQ_001_3146
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Handover Acknowledge Message the Reserved field MUST ignored by the receiver.

RFC Text:
ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code
- 0: Handover Accepted, NCoA valid
- 1: Handover Accepted, NCoA not valid
- 2: Handover Accepted, NCoA in use
- 3: Handover Accepted, NCoA assigned (used in Assigned addressing)
- 4: Handover Accepted, NCoA not assigned (used in Assigned addressing)
- 128: Handover Not Accepted, reason unspecified
- 129: Administratively prohibited
- 130: Insufficient resources

Checksum — The ICMPv6 checksum.

Subtype — 5

Reserved — MUST be set to zero by the sender and **ignored by the receiver.**

Identifier — Copied from the corresponding field in the Handover Initiate message to which this message is a response.

Identifier: RQ_001_3147
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Handover Acknowledge Message the Identifier field MUST be copied from the corresponding field in the Handover Initiate message to which this message is a response.

RFC Text:
ICMP Fields:

Type — The Experimental Mobility Protocol Type. See RFC 4065 [4].

Code
- 0: Handover Accepted, NCoA valid
- 1: Handover Accepted, NCoA not valid
- 2: Handover Accepted, NCoA in use
- 3: Handover Accepted, NCoA assigned (used in Assigned addressing)
- 4: Handover Accepted, NCoA not assigned (used in Assigned addressing)
- 128: Handover Not Accepted, reason unspecified
- 129: Administratively prohibited
- 130: Insufficient resources

Checksum — The ICMPv6 checksum.

Subtype — 5

Reserved — MUST be set to zero by the sender and ignored by the receiver.

Identifier — Copied from the corresponding field in the Handover Initiate message to which this message is a response.

Identifier: RQ_001_3148
RFC Clause: 6.2.2
Type: Mandatory
Applies to: Router

Requirement:
In the ICMP Handover Acknowledge Message the "New Care of Address" Option MUST be included if he S flag in the Handover Initiate message is set.

RFC Text:
Valid Options:

New Care of Address
If the S flag in the Handover Initiate message is set, this option MUST be used to provide NCoA the MN should use when connected to this router. This option MAY be included, even when the `S' bit is not set, e.g., Code 2 above.

Identifier: RQ_001_3149
RFC Clause: 6.2.1
Type: Optional
Applies to: Router

Requirement:
In the ICMP Handover Acknowledge Message the " New Care of Address" Option MAY be included, when the the S flag in the Handover Initiate message is not set.

RFC Text:
Valid Options:

New Care of Address
If the S flag in the Handover Initiate message is set, this option MUST be used to provide NCoA the MN should use when connected to this router. **This option MAY be included, even when the `S' bit is not set, e.g., Code 2 above.**

Identifier: RQ_001_3150
RFC Clause: 6.2.1
Type: Mandatory
Applies to: Router

Requirement:
Upon receiving an HI message, the NAR MUST respond with a Handover Acknowledge message.

RFC Text:
Upon receiving an HI message, the NAR MUST respond with a Handover Acknowledge message. If the `S' flag is set in the HI message, the NAR SHOULD include the New Care of Address option and a Code 3.

Identifier: RQ_001_3151
RFC Clause: 6.2.1
Type: Recommendation
Applies to: Router

Requirement:
Upon receiving an HI message with the `S' flag is set, the NAR the NAR SHOULD include the New Care of Address option and a Code 3 in its respond (Handover Acknowledge message).

RFC Text:
Upon receiving an HI message, the NAR MUST respond with a Handover Acknowledge message. If the `S' flag is set in the HI message, the NAR SHOULD include the New Care of Address option and a Code 3.

Identifier: RQ_001_3152
RFC Clause: 6.2.1
Type: Optional
Applies to: Router

Requirement:
The NAR MAY set up a tunnel to the PAR to forward MN's packets sent with PCoA as a source IP address.

RFC Text:
The NAR MAY provide support for PCoA (instead of accepting or assigning NCoA), establish a host route entry for PCoA, and set up a tunnel to the PAR to forward MN's packets sent with PCoA as a source IP address. This host route entry SHOULD be used to forward packets once the NAR detects that the particular MN is attached to its link.

Identifier: RQ_001_3153
RFC Clause: 6.2.1
Type: Optional
Applies to: Router

Requirement:
The new access router can always refuse handover, in which case it should indicate the reason in one of the available Code values in the Handover Acknowledge message.

RFC Text:
Finally, the new access router can always refuse handover, in which case it should indicate the reason in one of the available Code values.

Identifier: RQ_001_3154
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
The Fast Binding Update message shall be structured as follows:

Bit	Field
1 - 16	Sequence # Field
17	A Bit
18	H Bit
19	L Bit
20	K Bit
21 - 32	Reserved Field
33 - 48	Lifetime Field
49 - end	Mobility Options Field.

RFC Text:
The Fast Binding Update message is identical to the Mobile IPv6 Binding Update (BU) message. However, the processing rules are slightly different.

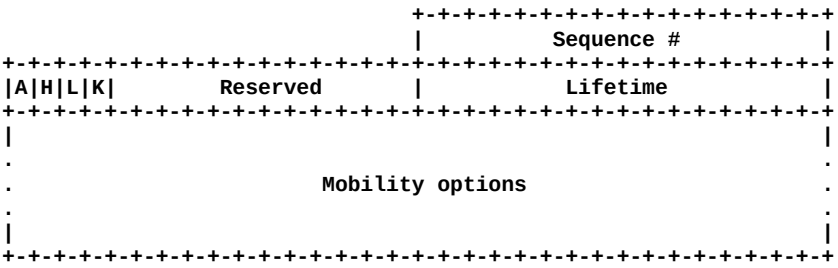


Figure 8: Fast Binding Update (FBU) Message

Identifier: RQ_001_3154
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Fast Binding Update message shall be structured as follows:

Bit	Field
1 - 16	Sequence # Field
17	A Bit
18	H Bit
19	L Bit
20	K Bit
21 - 32	Reserved Field
33 - 48	Lifetime Field
49 - end	Mobility Options Field.

RFC Text:
The Fast Binding Update message is identical to the Mobile IPv6 Binding Update (BU) message. However, the processing rules are slightly different.

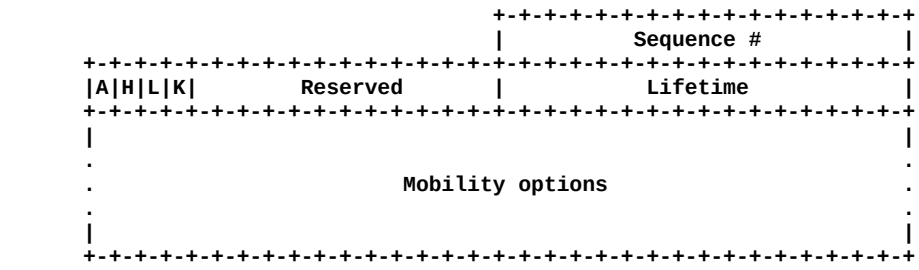


Figure 8: Fast Binding Update (FBU) Message

Identifier: RQ_001_3155
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Binding Update, the Source Address MUST be the PCoA or NCoA.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3155
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Update, the Source Address MUST be the PCoA or NCoA.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3156
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Binding Update, the Destination Address MUST be the IP address of the Previous Access Router

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3156
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Update, the Destination Address MUST be the IP address of the Previous Access Router

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3157
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:

In the Fast Binding Update message, the A flag MUST be set to 1.

RFC Text:

IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag **MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.**

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3157
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the Fast Binding Update message, the A flag MUST be set to 1.

RFC Text:

IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag **MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.**

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3158
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:

In the Fast Binding Update message, the H flag MUST be set to 1.

RFC Text:

IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3158
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the Fast Binding Update message, the H flag MUST be set to 1.

RFC Text:

IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3159
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
In the Fast Binding Update message, the L flag MUST be set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3159
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Fast Binding Update message, the L flag MUST be set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3160
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:

In the Fast Binding Update message, the K flag MUST be ignored.

RFC Text:

IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3161
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
In the Fast Binding Update message, the Reserved field MUST be set zero.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3161
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Fast Binding Update message, the Reserved field MUST be set zero.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3162
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
In the Fast Binding Update message, the Sequence Number field MUST contain a A 16-bit unsigned integer .

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3162
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Fast Binding Update message, the Sequence Number field MUST contain a A 16-bit unsigned integer .

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3163
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
In the Fast Binding Update message, the Lifetime field MUST contain a 16-bit unsigned integer.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3163
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Fast Binding Update message, the Lifetime field MUST contain a 16-bit unsigned integer.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3164
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
In the Fast Binding Update message, the Mobility Options MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3164
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Fast Binding Update message, the Mobility Options MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

RFC Text:
IP fields:

Source Address
The PCoA or NCoA

Destination Address
The IP address of the Previous Access Router

A flag MUST be set to one to request that PAR send a Fast Binding Acknowledgment message.

H flag MUST be set to one. See RFC 3775 [3].

L flag See RFC 3775 [3].

K flag See RFC 3775 [3].

Reserved This field is unused. MUST be set zero.

Sequence Number
See RFC 3775 [3].

Lifetime See RFC 3775 [3].

Mobility Options
MUST contain an alternate CoA option set to the NCoA when an FBU is sent from PAR's link.

Identifier: RQ_001_3165
RFC Clause: 6.3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the MN moves prior to receiving a PrRtAdv message, it SHOULD send an FBU to the PAR after configuring NCoA on the NAR according to Neighbor Discovery and IPv6 Address Configuration protocols.

RFC Text:
The MN sends an FBU message any time after receiving a PrRtAdv message. If the MN moves prior to receiving a PrRtAdv message, it SHOULD send an FBU to the PAR after configuring NCoA on the NAR according to Neighbor Discovery and IPv6 Address Configuration protocols.

Identifier: RQ_001_3166
RFC Clause: 6.3.1
Type: Recommendation
Applies to: Router

Requirement:
When the FBU is sent from NAR's link, it SHOULD be encapsulated within an FNA.

RFC Text:
The source IP address is PCoA when the FBU is sent from PAR's link, and the source IP address is NCoA when sent from NAR's link. **When the FBU is sent from NAR's link, it SHOULD be encapsulated within an FNA.**

Identifier: RQ_001_3167
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
The FBU MUST include the Home Address Option.

RFC Text:
The FBU MUST also include the Home Address Option, and the Home Address is PCoA. An FBU message MUST be protected so that PAR is able to determine that the FBU message is sent by a genuine MN.

Identifier: RQ_001_3167
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The FBU MUST include the Home Address Option.

RFC Text:
The FBU MUST also include the Home Address Option, and the Home Address is PCoA. An FBU message MUST be protected so that PAR is able to determine that the FBU message is sent by a genuine MN.

Identifier: RQ_001_3168
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Router

Requirement:
An FBU message MUST be protected.

RFC Text:
The FBU MUST also include the Home Address Option, and the Home Address is PCoA. **An FBU message MUST be protected** so that PAR is able to determine that the FBU message is sent by a genuine MN.

Identifier: RQ_001_3168
RFC Clause: 6.3.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
An FBU message MUST be protected.

RFC Text:
The FBU MUST also include the Home Address Option, and the Home Address is PCoA. **An FBU message MUST be protected** so that PAR is able to determine that the FBU message is sent by a genuine MN.

Identifier: RQ_001_3169
RFC Clause: 6.3.2
Type: Recommendation
Applies to: Router

Requirement:
The Fast Binding Acknowledgment message SHOULD NOT be sent to the MN before the PAR receives a HAck message from the NAR.

RFC Text:
The Fast Binding Acknowledgment message is sent by the PAR to acknowledge receipt of a Fast Binding Update message in which the 'A' bit is set. **The Fast Binding Acknowledgment message SHOULD NOT be sent to the MN before the PAR receives a HAck message from the NAR**. The Fast Binding Acknowledgment MAY also be sent to the MN on the old link.

Identifier: RQ_001_3170
RFC Clause: 6.3.2
Type: Optional
Applies to: Router

Requirement:
The Fast Binding Acknowledgment MAY also be sent to the MN on the old link.

RFC Text:
The Fast Binding Acknowledgment message is sent by the PAR to acknowledge receipt of a Fast Binding Update message in which the 'A' bit is set. The Fast Binding Acknowledgment message SHOULD NOT be sent to the MN before the PAR receives a HAck message from the NAR. **The Fast Binding Acknowledgment MAY also be sent to the MN on the old link.**

Identifier: RQ_001_3171
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Router

Requirement:
The Fast Binding Acknowledgement message shall be structured as follows:

Bit	Field
1 - 8	Status Field
9	K Bit
10 - 16	Reserved Field
17 - 32	Sequence # Field
33 - 48	Lifetime Field
49 - end	Mobility Options

RFC Text:

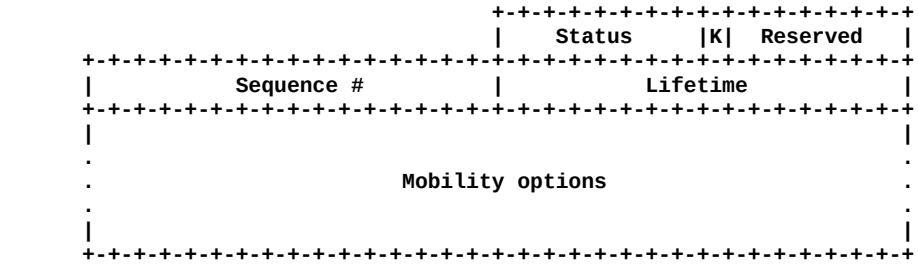


Figure 9: Fast Binding Acknowledgment (FBack) Message

Identifier: RQ_001_3171
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:

The Fast Binding Acknowledgement message shall be structured as follows:

Bit	Field
1 - 8	Status Field
9	K Bit
10 - 16	Reserved Field
17 - 32	Sequence # Field
33 - 48	Lifetime Field
49 - end	Mobility Options

RFC Text:

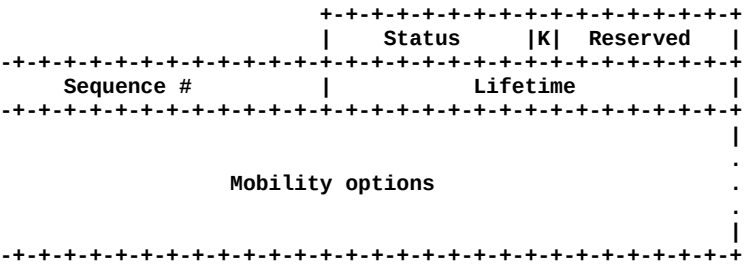


Figure 9: Fast Binding Acknowledgment (FBack) Message

Identifier: RQ_001_3172
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Source Address MUST be the IP address of the Previous Access Router.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
The NCoA

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3172
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Source Address MUST be the IP address of the Previous Access Router.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
The NCoA

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3173
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Destination Address MUST be the NAR's IP Address.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3173
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Destination Address MUST be the NAR's IP Address.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3174
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Status Field MUST be an 8-bit unsigned integer of value 0, 1, 128, 129, 130 or 131.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status **8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:**

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3174
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Status Field MUST be an 8-bit unsigned integer of value 0, 1, 128, 129, 130 or 131.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status **8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:**

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3175
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Router

Requirement:

In the IP Header for the Fast Binding Acknowledgement, the `K' flag MUST be ignored.

RFC Text:

IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag **See RFC 3775 [3].**

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3175
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the `K' flag MUST be ignored.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag **See RFC 3775 [3].**

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3176
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Reserved field MUST be set to zero.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved **An unused field. MUST be set to zero.**

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3176
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Reserved field MUST be set to zero.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved **An unused field. MUST be set to zero.**

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3177
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Sequence Number field MUST be copied from the FBU message.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3177
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Sequence Number field MUST be copied from the FBU message.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3178
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Lifetime field MUST contain the granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime **The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.**

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3178
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Lifetime field MUST contain the granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status 8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag See RFC 3775 [3].

Reserved An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime **The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.**

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3179
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Mobility Options MUST contain an "alternate" CoA if Status is 1.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status
8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag
See RFC 3775 [3].

Reserved
An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime
The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3179
RFC Clause: 6.3.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Binding Acknowledgement, the Mobility Options MUST contain an "alternate" CoA if Status is 1.

RFC Text:
IP fields:

Source Address
The IP address of the Previous Access Router.

Destination Address
NAR's IP Address

Status
8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field that are less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted
1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in "alternate" CoA

Values of the Status field that are greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Incorrect interface identifier length

`K' flag
See RFC 3775 [3].

Reserved
An unused field. MUST be set to zero.

Sequence Number
Copied from the FBU message for use by the MN in matching this acknowledgment with an outstanding FBU.

Lifetime
The granted lifetime in seconds for which the sender of this message will retain a binding for traffic redirection.

Mobility Options
MUST contain an "alternate" CoA if Status is 1.

Identifier: RQ_001_3180
RFC Clause: 6.3.3
Type: Optional
Applies to: Router

Requirement:
When the Mobility Header Type of a Fast Neighbor Advertisement is FNA, the Payload Proto field may be set to IPv6 to assist FBU encapsulation.

RFC Text:
A MN sends a Fast Neighbor Advertisement to announce itself to the NAR. When the Mobility Header Type is FNA, the Payload Proto field may be set to IPv6 to assist FBU encapsulation.

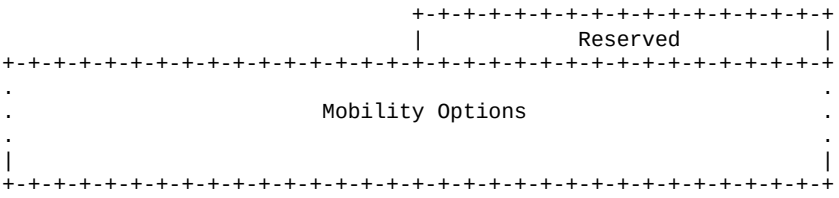


Figure 10: Fast Neighbor Advertisement (FNA) Message

Identifier: RQ_001_3180
RFC Clause: 6.3.3
Type: Optional
Applies to: Mobile_Node

Requirement:
When the Mobility Header Type of a Fast Neighbor Advertisement is FNA, the Payload Proto field may be set to IPv6 to assist FBU encapsulation.

RFC Text:
A MN sends a Fast Neighbor Advertisement to announce itself to the NAR. When the Mobility Header Type is FNA, the Payload Proto field may be set to IPv6 to assist FBU encapsulation.

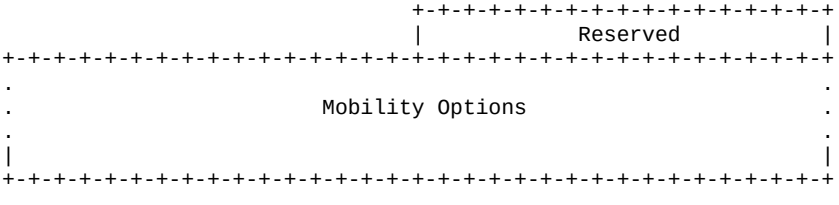


Figure 10: Fast Neighbor Advertisement (FNA) Message

Identifier: RQ_001_3181
RFC Clause: 6.3.3
Type: Mandatory
Applies to: Router

Requirement:
The Fast Neighbor Advertisement message shall be structured as follows:

Bit	Field
1-16	Reserved
17-end	Mobility Options

RFC Text:
A MN sends a Fast Neighbor Advertisement to announce itself to the NAR. When the Mobility Header Type is FNA, the Payload Proto field may be set to IPv6 to assist FBU encapsulation.

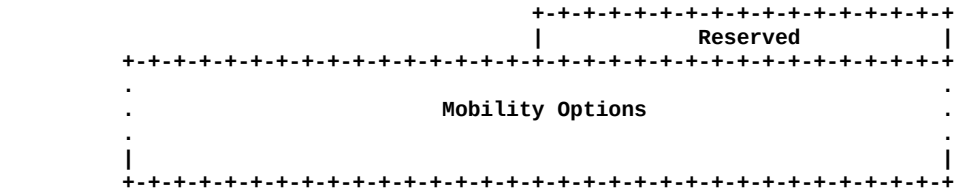


Figure 10: Fast Neighbor Advertisement (FNA) Message

Identifier: RQ_001_3181
RFC Clause: 6.3.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Fast Neighbor Advertisement message shall be structured as follows:

Bit	Field
1-16	Reserved
17-end	Mobility Options

RFC Text:
A MN sends a Fast Neighbor Advertisement to announce itself to the NAR. When the Mobility Header Type is FNA, the Payload Proto field may be set to IPv6 to assist FBU encapsulation.

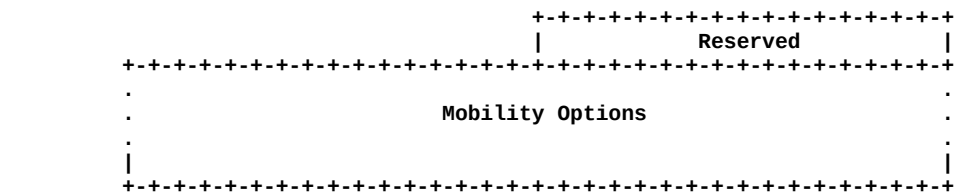


Figure 10: Fast Neighbor Advertisement (FNA) Message

Identifier: RQ_001_3182
RFC Clause: 6.3.3
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Neighbor Advertisement, the Source Address MUST be the NCoA.

RFC Text:
IP fields:

Source Address
NCoA

Destination Address
NAR's IP Address

Mobility Options
MUST contain the Mobility Header Link-Layer Address of the MN in the MH-LLA option format. See Section 6.4.4.

Identifier: RQ_001_3182
RFC Clause: 6.3.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Neighbor Advertisement, the Source Address MUST be the NCoA.

RFC Text:
IP fields:

Source Address
NCoA

Destination Address
NAR's IP Address

Mobility Options
MUST contain the Mobility Header Link-Layer Address of the MN in the MH-LLA option format. See Section 6.4.4.

Identifier: RQ_001_3183
RFC Clause: 6.3.3
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Neighbor Advertisement, the Destination Address MUST be the NAR's IP Address.

RFC Text:
IP fields:

Source Address
NCoA

Destination Address
NAR's IP Address

Mobility Options
MUST contain the Mobility Header Link-Layer Address of the MN in the MH-LLA option format. See Section 6.4.4.

Identifier: RQ_001_3183
RFC Clause: 6.3.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Neighbor Advertisement, the Destination Address MUST be the NAR's IP Address.

RFC Text:
IP fields:

Source Address
NCoA

Destination Address
NAR's IP Address

Mobility Options
MUST contain the Mobility Header Link-Layer Address of the MN in the MH-LLA option format. See Section 6.4.4.

Identifier: RQ_001_3184
RFC Clause: 6.3.3
Type: Mandatory
Applies to: Router

Requirement:
In the IP Header for the Fast Neighbor Advertisement, the Mobility Options MUST contain the Mobility Header Link-Layer Address of the MN in the MH-LLA option format.

RFC Text:
IP fields:

Source Address
NCoA

Destination Address
NAR's IP Address

Mobility Options
MUST contain the Mobility Header Link-Layer Address of the MN in the MH-LLA option format. See Section 6.4.4.

Identifier: RQ_001_3184
RFC Clause: 6.3.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Header for the Fast Neighbor Advertisement, the Mobility Options MUST contain the Mobility Header Link-Layer Address of the MN in the MH-LLA option format.

RFC Text:
IP fields:

Source Address
NCoA

Destination Address
NAR's IP Address

Mobility Options
MUST contain the Mobility Header Link-Layer Address of the MN in the MH-LLA option format. See Section 6.4.4.

Identifier: RQ_001_3185
RFC Clause: 6.3.3
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The combination of NCoA (present in source IP address) and the Link-Layer Address SHOULD be used to distinguish the MN from other nodes.

RFC Text:
The combination of NCoA (present in source IP address) and the Link-Layer Address (present as a Mobility Option) SHOULD be used to distinguish the MN from other nodes.

Identifier: RQ_001_3186
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Router

Requirement:

The IP Address Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-32	Prefix Length
33-64	Reserved
65-192	IPv6 Address

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

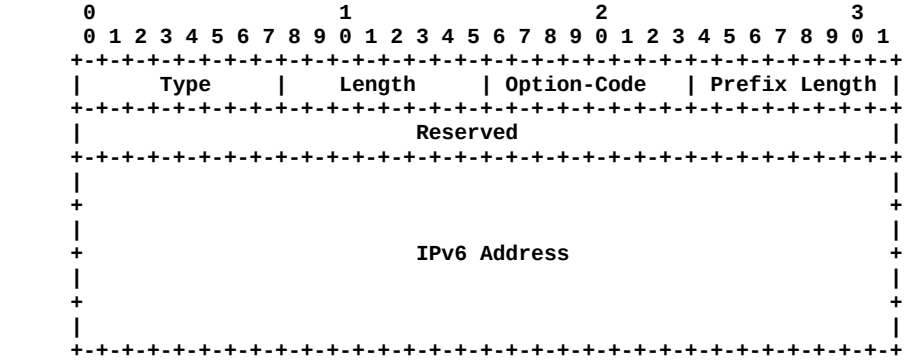


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3186
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:

The IP Address Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-32	Prefix Length
33-64	Reserved
65-192	IPv6 Address

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

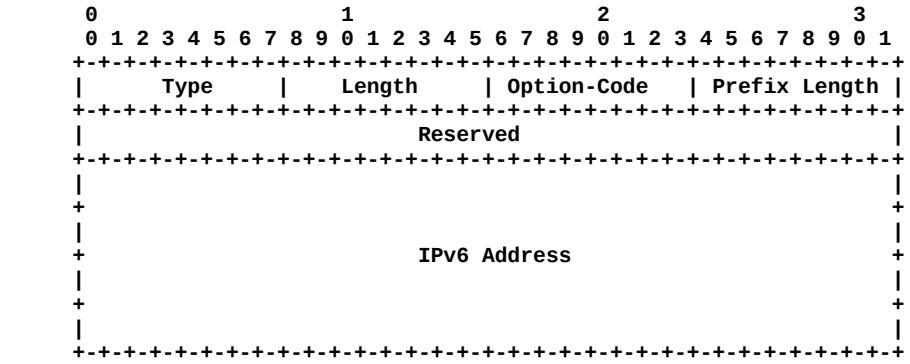


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3187
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Address Option, the Type Fied shall be set to 17.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

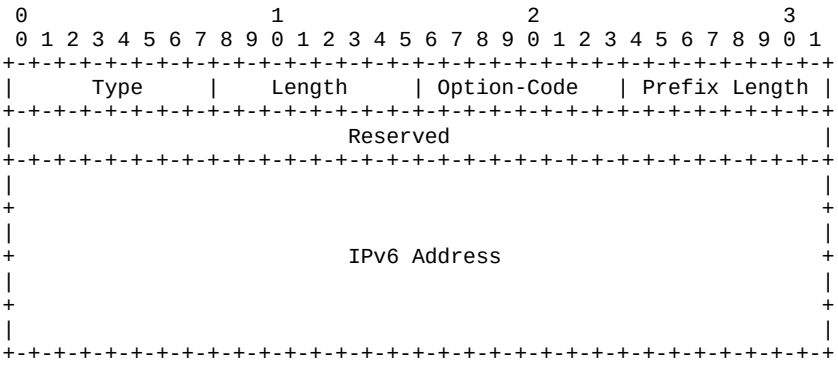


Figure 12: IPv6 Address Option

Type **17**

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3187
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Address Option, the Type Fied shall be set to 17.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

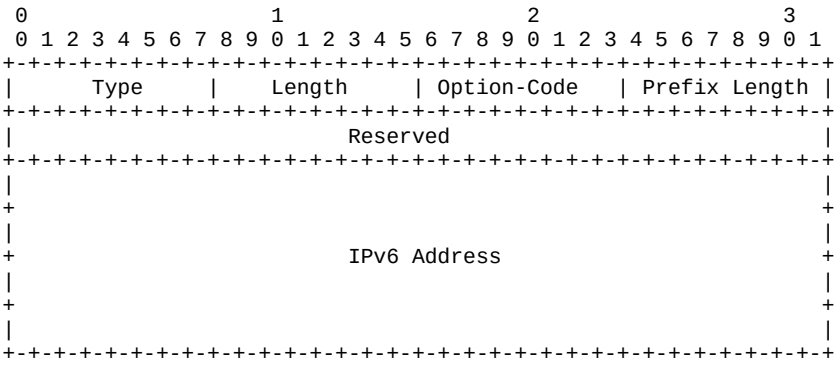


Figure 12: IPv6 Address Option

Type **17**

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3188
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Address Option, the Length Fied shall be set to the size of this option in 8 octets including the Type, Option-Code, and Length fields.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

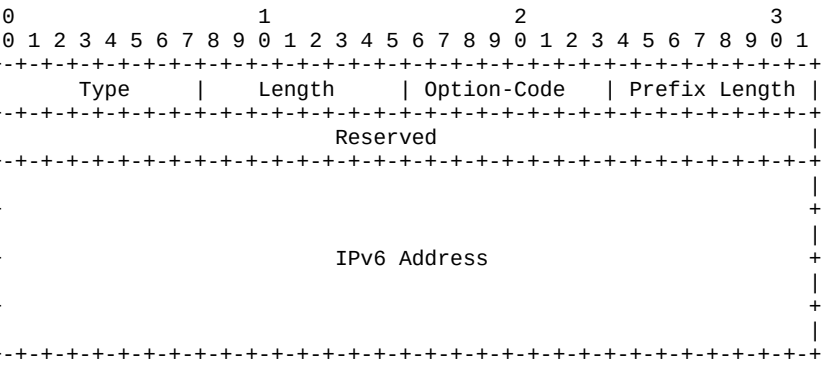


Figure 12: IPv6 Address Option

Type 17

Length **The size of this option in 8 octets including the Type, Option-Code, and Length fields**.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3188
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Address Option, the Length Fied shall be set to the size of this option in 8 octets including the Type, Option-Code, and Length fields.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

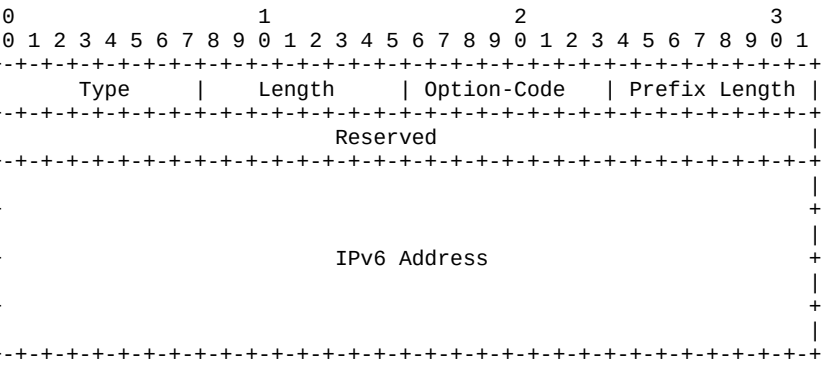


Figure 12: IPv6 Address Option

Type 17

Length **The size of this option in 8 octets including the Type, Option-Code, and Length fields**.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3189
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Address Option, the Option-Code, Field shall be set to 1, 2 or 3.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

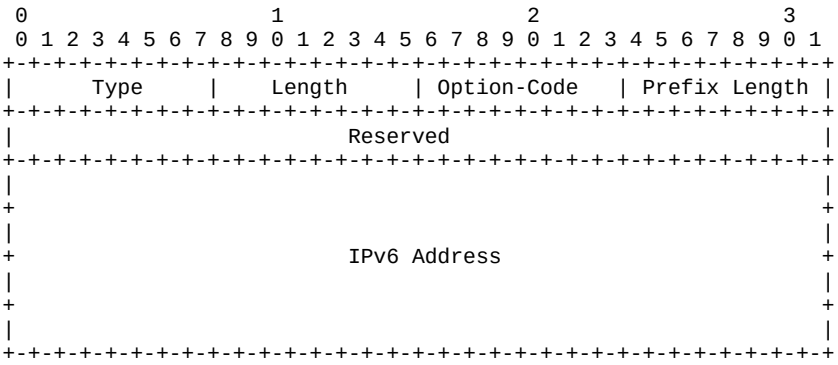


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3189
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Address Option, the Option-Code, Field shall be set to 1, 2 or 3.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

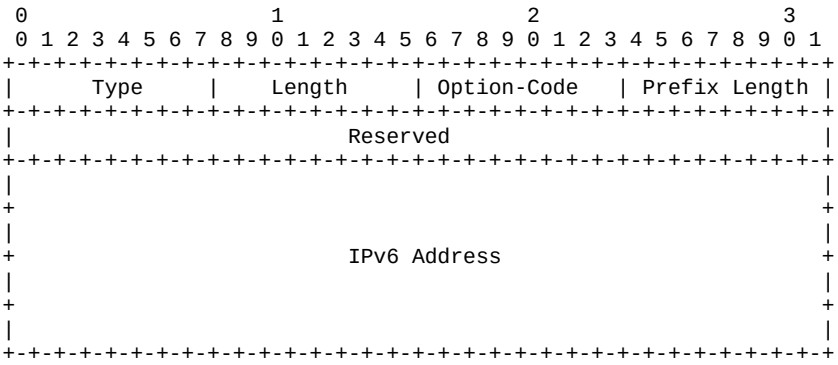


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3190
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Router

Requirement:

In the IP Address Option, the Prefix Length Field shall be set to the Length of the IPv6 Address Prefix.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

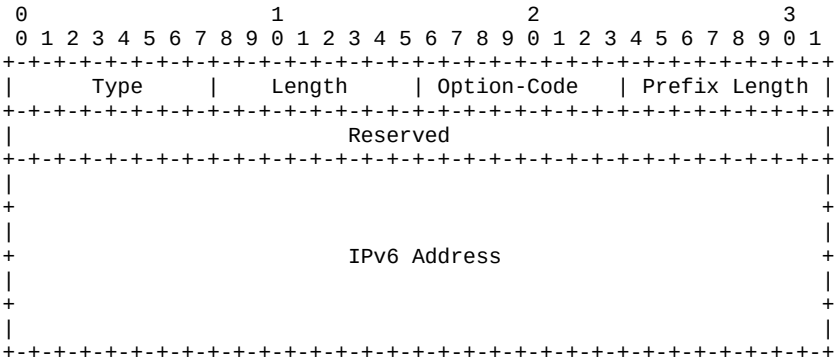


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3190
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the IP Address Option, the Prefix Length Field shall be set to the Length of the IPv6 Address Prefix.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

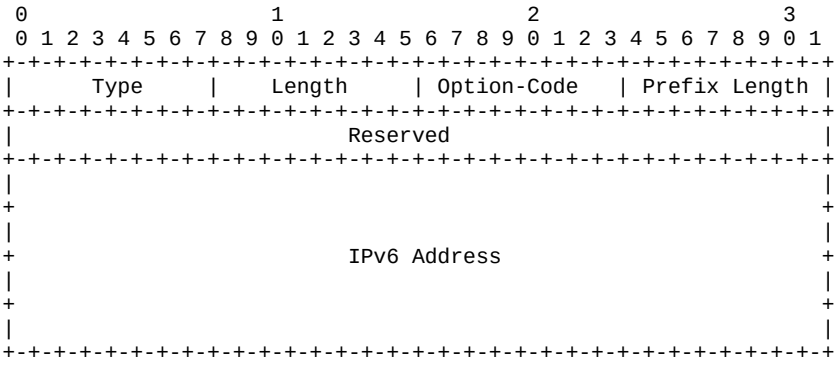


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3191
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Address Option, the Reserved Field MUST be set to zero by the sender.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

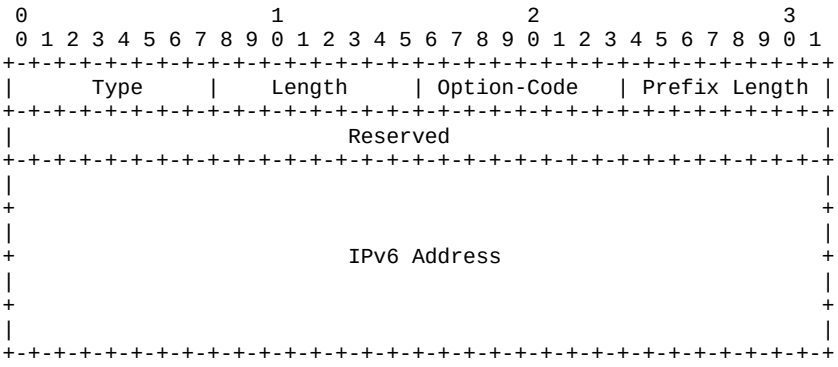


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved **MUST be set to zero by the sender** and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3192
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Address Option, the Reserved Field MUST be ignored by the receiver.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

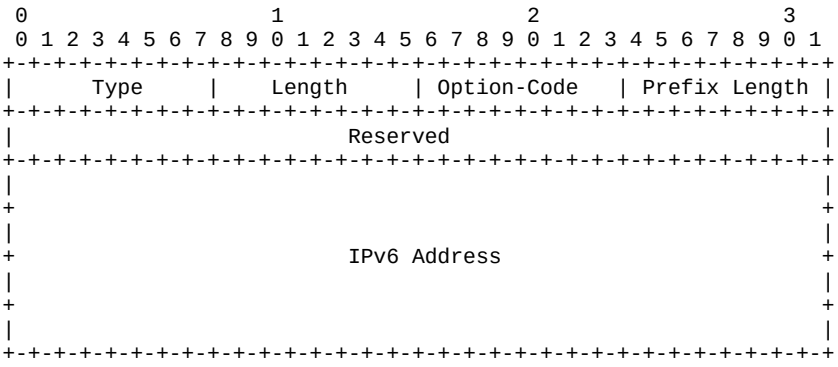


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and **MUST be ignored by the receiver.**

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3193
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Router

Requirement:
In the IP Address Option, the IPv6 Address Field MUST contain the IP address for the unit defined by the Type field.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

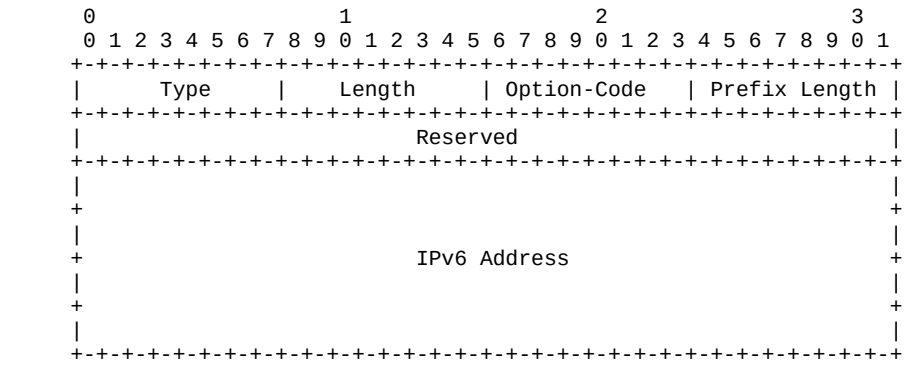


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3193
RFC Clause: 6.4.1
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the IP Address Option, the IPv6 Address Field MUST contain the IP address for the unit defined by the Type field.

RFC Text:

This option is sent in the Proxy Router Advertisement, the Handover Initiate, and Handover Acknowledge messages.

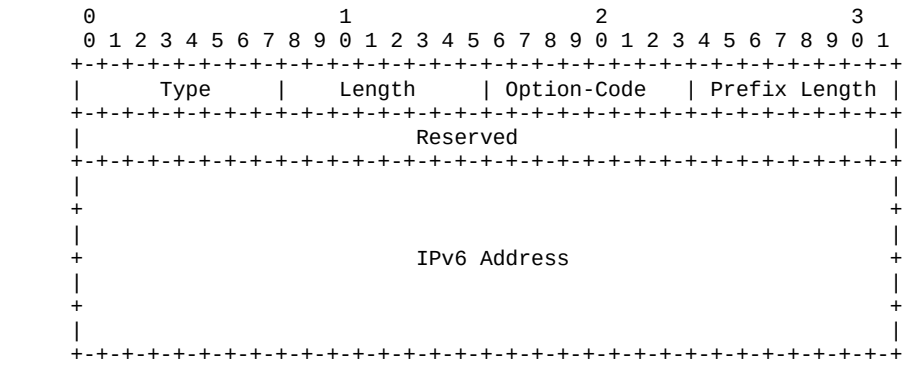


Figure 12: IPv6 Address Option

Type 17

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
1 Old Care-of Address
2 New Care-of Address
3 NAR's IP address

Prefix Length
The Length of the IPv6 Address Prefix.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

IPv6 Address The IP address for the unit defined by the Type field.

Identifier: RQ_001_3194
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Router

Requirement:
The New Router Prefix Information Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-32	Prefix Length
33-64	Reserved
65-192	IPv6 Address

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

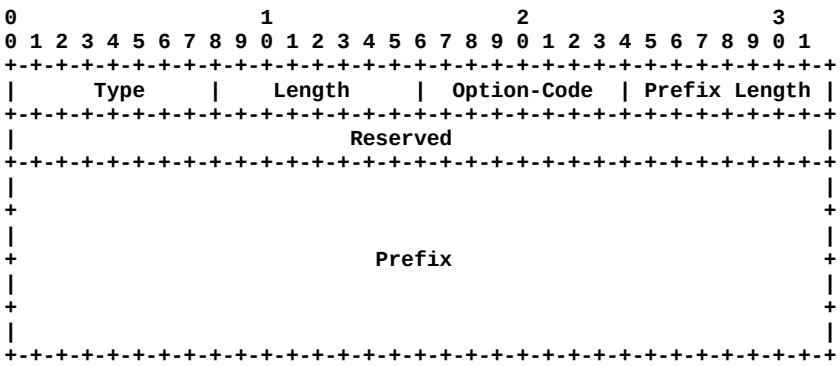


Figure 13: New Router Prefix Information Option

Type — 18

Length — The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code — 0

Prefix Length — 8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved — MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix — An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3194
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The New Router Prefix Information Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-32	Prefix Length
33-64	Reserved
65-192	IPv6 Address

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

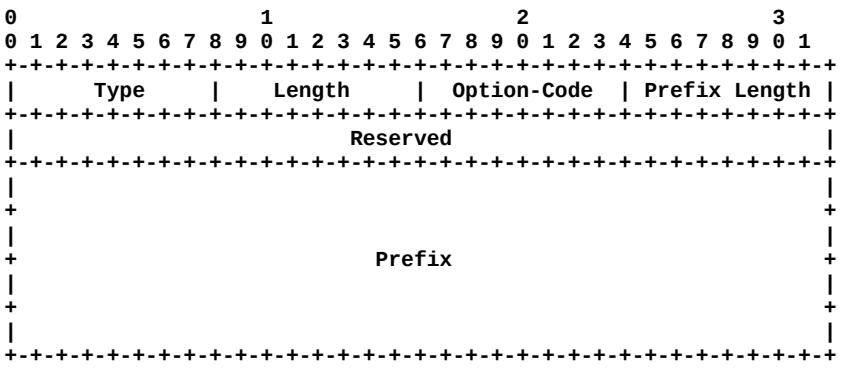


Figure 13: New Router Prefix Information Option

Type — 18

Length — The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code — 0

Prefix Length — 8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved — MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix — An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3195
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Router

Requirement:
In the New Router Prefix Information Option, the Type Field shall be set to 18.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

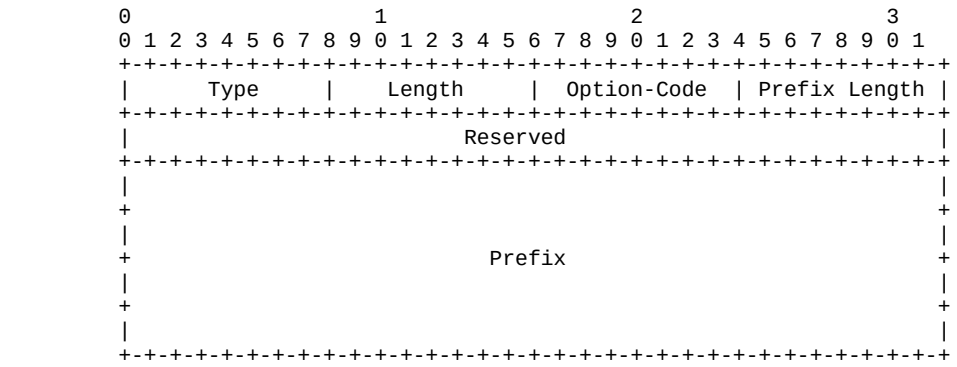


Figure 13: New Router Prefix Information Option

Type **18**

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3195
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the New Router Prefix Information Option, the Type Field shall be set to 18.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

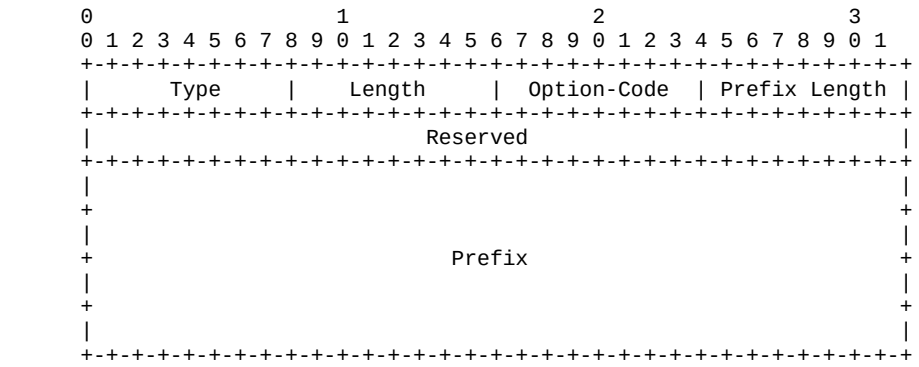


Figure 13: New Router Prefix Information Option

Type **18**

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3196
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Router

Requirement:
In the New Router Prefix Information Option, the Length Fied shall be set to the size of this option in 8 octets including the Type, Option-Code, and Length fields.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

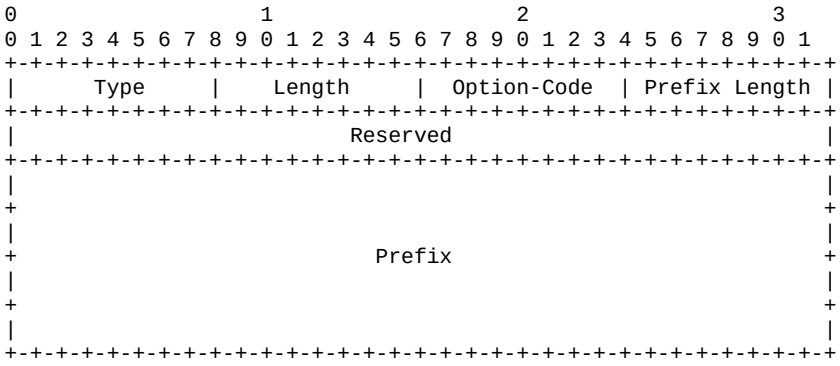


Figure 13: New Router Prefix Information Option

Type 18

Length **The size of this option in 8 octets including the Type, Option-Code, and Length fields**.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3196
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the New Router Prefix Information Option, the Length Fied shall be set to the size of this option in 8 octets including the Type, Option-Code, and Length fields.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

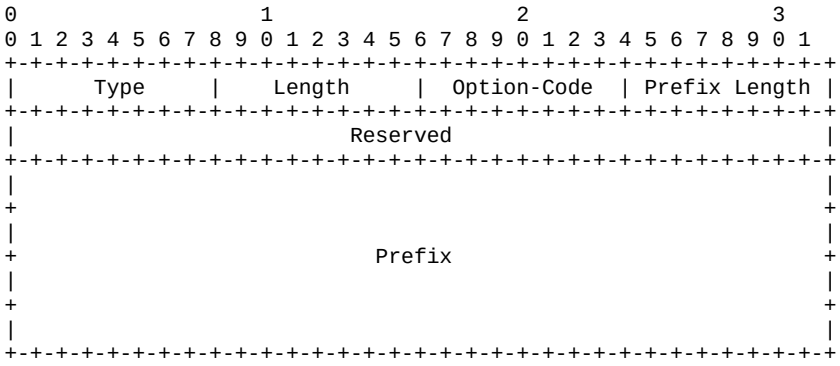


Figure 13: New Router Prefix Information Option

Type 18

Length **The size of this option in 8 octets including the Type, Option-Code, and Length fields**.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3197
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Router

Requirement:
In the New Router Prefix Information Option, the Option-Code Fied shall be set to 0.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

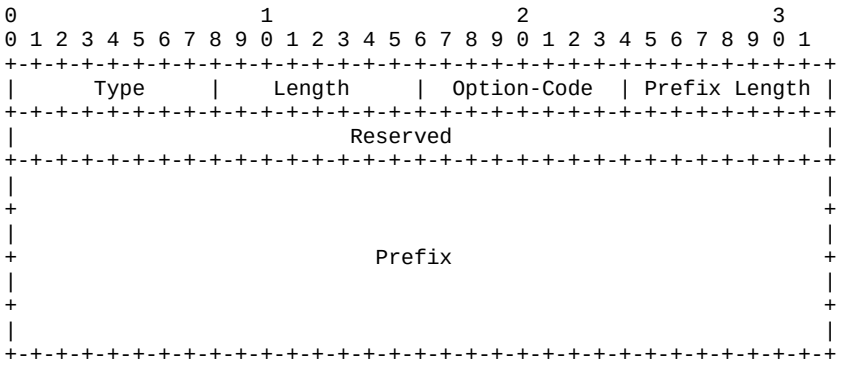


Figure 13: New Router Prefix Information Option

Type 18

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3197
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the New Router Prefix Information Option, the Option-Code Fied shall be set to 0.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

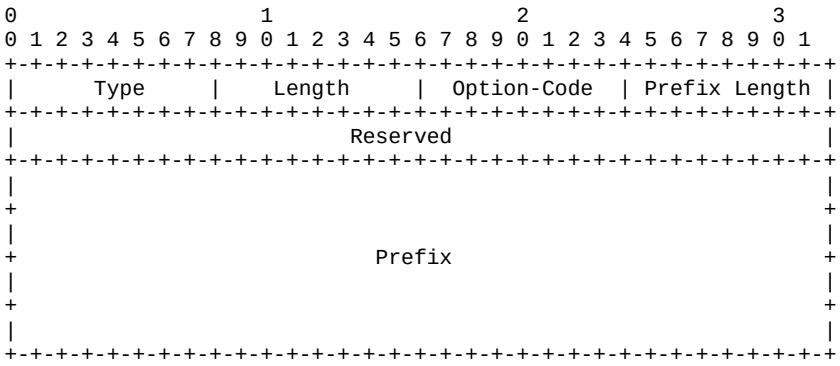


Figure 13: New Router Prefix Information Option

Type 18

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3198
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Router

Requirement:
In the New Router Prefix Information Option, the Prefix LengthField is an 8-bit unsigned integer. The value ranges from 0 to 128.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

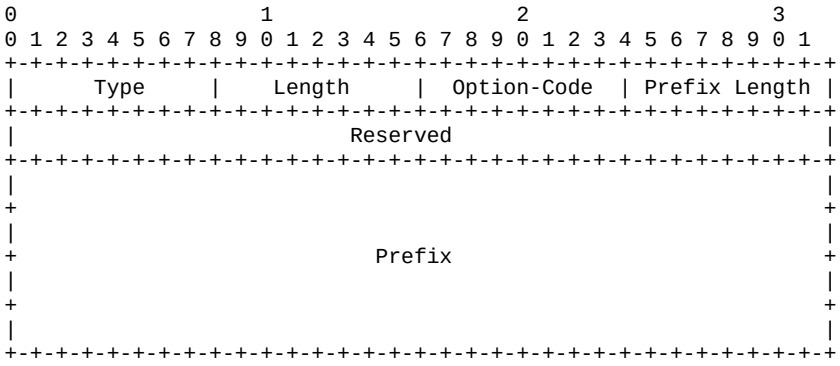


Figure 13: New Router Prefix Information Option

Type 18

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3198
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the New Router Prefix Information Option, the Prefix LengthField is an 8-bit unsigned integer. The value ranges from 0 to 128.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

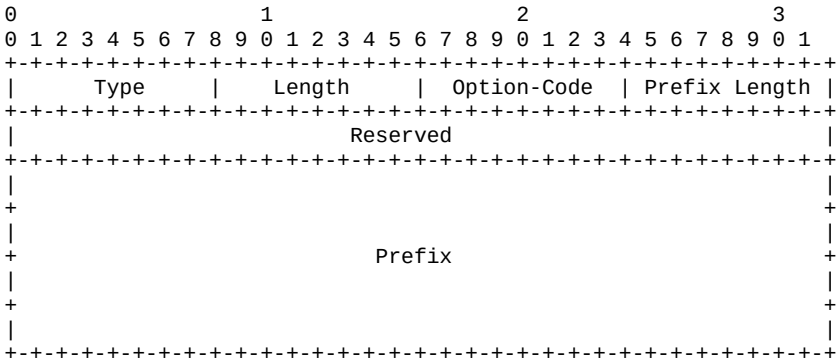


Figure 13: New Router Prefix Information Option

Type 18

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3199
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the New Router Prefix Information Option, the Reserved Field MUST be set to zero by the sender

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

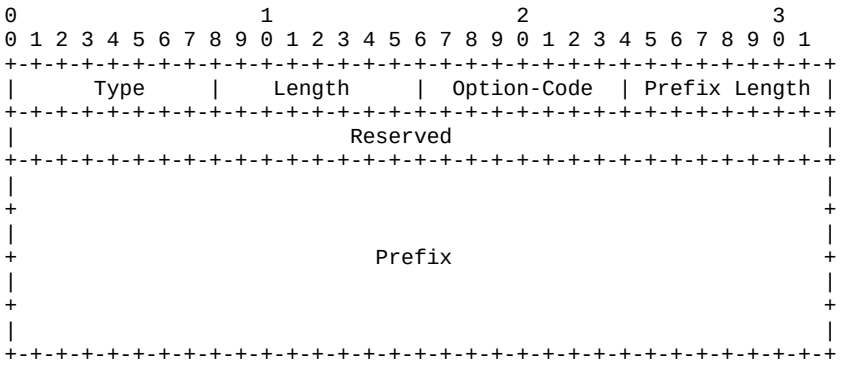


Figure 13: New Router Prefix Information Option

Type 18

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved **MUST be set to zero by the sender** and MUST be ignored by the receiver.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3200
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Router

Requirement:
In the New Router Prefix Information Option, the Reserved Field and MUST be ignored by the receiver.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

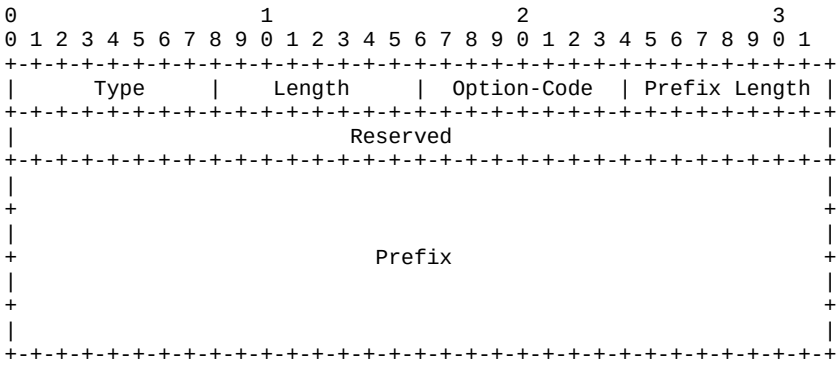


Figure 13: New Router Prefix Information Option

Type 18

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and **MUST be ignored by the receiver.**

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3201
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Router

Requirement:
In the New Router Prefix Information Option, the Prefix Field contains an IP address or a prefix of an IP address.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

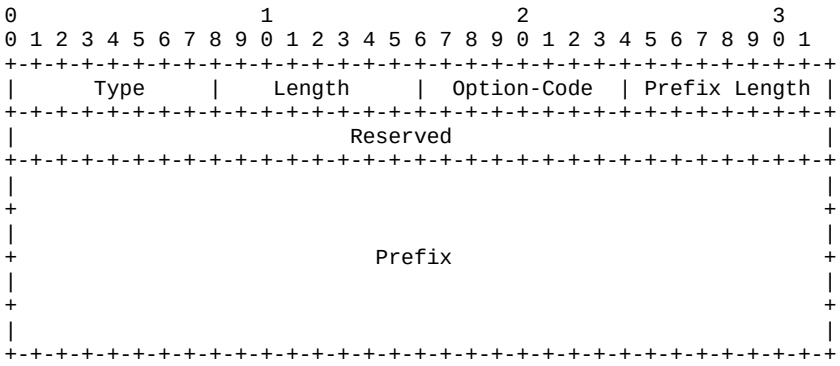


Figure 13: New Router Prefix Information Option

Type 18

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix **An IP address or a prefix of an IP address.** The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3201
RFC Clause: 6.4.2
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the New Router Prefix Information Option, the Prefix Field contains an IP address or a prefix of an IP address.

RFC Text:
This option is sent in the PrRtAdv message to provide the prefix information valid on the NAR.

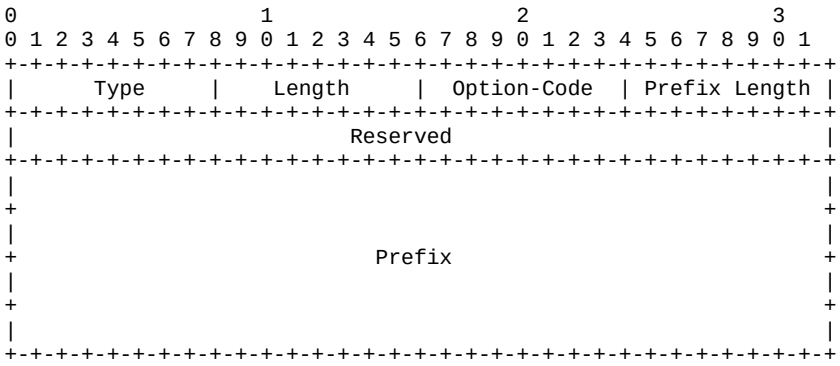


Figure 13: New Router Prefix Information Option

Type 18

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code 0

Prefix Length
8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Prefix **An IP address or a prefix of an IP address.** The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

Identifier: RQ_001_3202
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Router

Requirement:

The Link Layer Address Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-end	LLA

RFC Text:

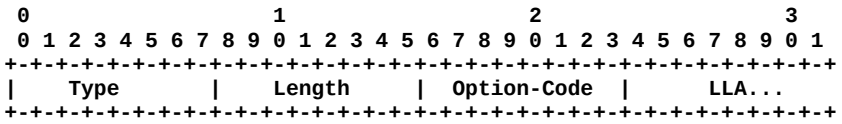


Figure 14: Link-Layer Address Option

Type 19

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code

0 wildcard requesting resolution for all nearby access points
1 Link-Layer Address of the New Access Point
2 Link-Layer Address of the MN
3 Link-Layer Address of the NAR (i.e., Proxied Originator)
4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
5 The access point identified by the LLA belongs to the current interface of the router
6 No prefix information available for the access point identified by the LLA
7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3202
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:

The Link Layer Address Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-end	LLA

RFC Text:

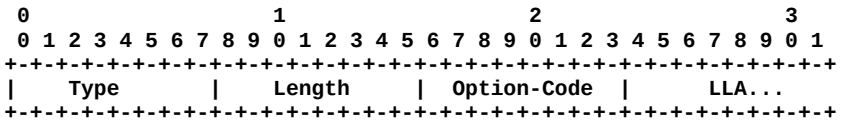


Figure 14: Link-Layer Address Option

Type 19

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
- 0 wildcard requesting resolution for all nearby access points
- 1 Link-Layer Address of the New Access Point
- 2 Link-Layer Address of the MN
- 3 Link-Layer Address of the NAR (i.e., Proxied Originator)
- 4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
- 5 The access point identified by the LLA belongs to the current interface of the router
- 6 No prefix information available for the access point identified by the LLA
- 7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3203
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Router

Requirement:
In the Link Layer Address Option, the Type Field shall be set to 19.

RFC Text:

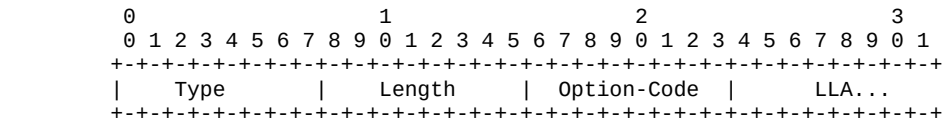


Figure 14: Link-Layer Address Option

Type **19**

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code

0 wildcard requesting resolution for all nearby access points
1 Link-Layer Address of the New Access Point
2 Link-Layer Address of the MN
3 Link-Layer Address of the NAR (i.e., Proxied Originator)
4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
5 The access point identified by the LLA belongs to the current interface of the router
6 No prefix information available for the access point identified by the LLA
7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3203
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Link Layer Address Option, the Type Field shall be set to 19.

RFC Text:

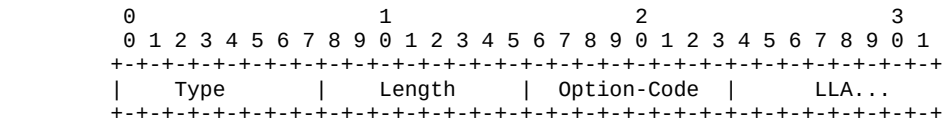


Figure 14: Link-Layer Address Option

Type **19**

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
- 0 wildcard requesting resolution for all nearby access points
- 1 Link-Layer Address of the New Access Point
- 2 Link-Layer Address of the MN
- 3 Link-Layer Address of the NAR (i.e., Proxied Originator)
- 4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
- 5 The access point identified by the LLA belongs to the current interface of the router
- 6 No prefix information available for the access point identified by the LLA
- 7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3204
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Router

Requirement:
In the Link Layer Address Option, the Length Field shall shall contain the size of this option in 8 octets including the Type, Option-Code, and Length fields.

RFC Text:

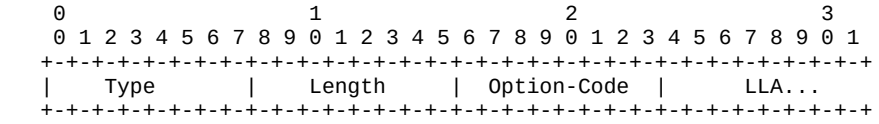


Figure 14: Link-Layer Address Option

Type 19

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
0 wildcard requesting resolution for all nearby access points
1 Link-Layer Address of the New Access Point
2 Link-Layer Address of the MN
3 Link-Layer Address of the NAR (i.e., Proxied Originator)
4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
5 The access point identified by the LLA belongs to the current interface of the router
6 No prefix information available for the access point identified by the LLA
7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3204
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Link Layer Address Option, the Length Field shall shall contain the size of this option in 8 octets including the Type, Option-Code, and Length fields.

RFC Text:

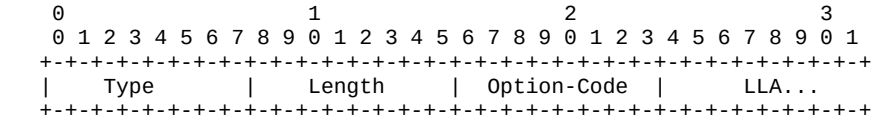


Figure 14: Link-Layer Address Option

Type 19

Length **The size of this option in 8 octets including the Type, Option-Code, and Length fields.**

Option-Code
0 wildcard requesting resolution for all nearby access points
1 Link-Layer Address of the New Access Point
2 Link-Layer Address of the MN
3 Link-Layer Address of the NAR (i.e., Proxied Originator)
4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
5 The access point identified by the LLA belongs to the current interface of the router
6 No prefix information available for the access point identified by the LLA
7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3205
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Router

Requirement:
In the Link Layer Address Option, the Option-Code Field shall contain the value 1, 2, 3, 4, 5, 6 or 7

RFC Text:

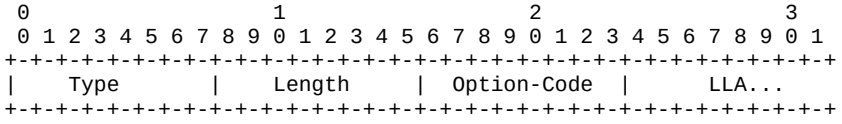


Figure 14: Link-Layer Address Option

Type 19

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code

0 wildcard requesting resolution for all nearby access points
1 Link-Layer Address of the New Access Point
2 Link-Layer Address of the MN
3 Link-Layer Address of the NAR (i.e., Proxied Originator)
4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
5 The access point identified by the LLA belongs to the current interface of the router
6 No prefix information available for the access point identified by the LLA
7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3205
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:

In the Link Layer Address Option, the Option-Code Field shall contain the value 1, 2, 3, 4, 5, 6 or 7

RFC Text:

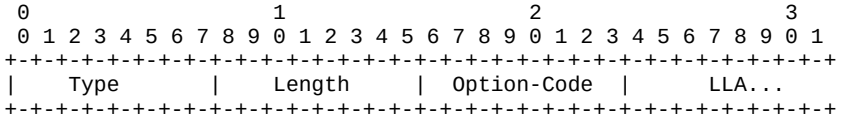


Figure 14: Link-Layer Address Option

Type 19

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code

0 wildcard requesting resolution for all nearby access points
1 Link-Layer Address of the New Access Point
2 Link-Layer Address of the MN
3 Link-Layer Address of the NAR (i.e., Proxied Originator)
4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
5 The access point identified by the LLA belongs to the current interface of the router
6 No prefix information available for the access point identified by the LLA
7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3206
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Router

Requirement:
In the Link Layer Address Option, the LLA Field shall contain the variable length Link-Layer Address.

RFC Text:

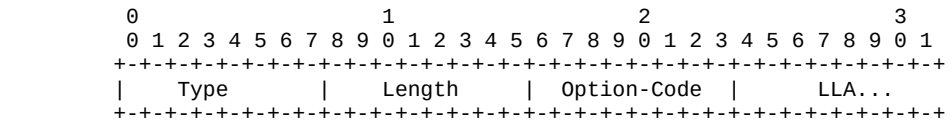


Figure 14: Link-Layer Address Option

Type 19

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
0 wildcard requesting resolution for all nearby access points
1 Link-Layer Address of the New Access Point
2 Link-Layer Address of the MN
3 Link-Layer Address of the NAR (i.e., Proxied Originator)
4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
5 The access point identified by the LLA belongs to the current interface of the router
6 No prefix information available for the access point identified by the LLA
7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3206
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
In the Link Layer Address Option, the LLA Field shall contain the variable length Link-Layer Address.

RFC Text:

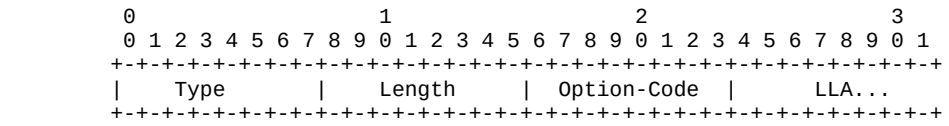


Figure 14: Link-Layer Address Option

Type 19

Length The size of this option in 8 octets including the Type, Option-Code, and Length fields.

Option-Code
0 wildcard requesting resolution for all nearby access points
1 Link-Layer Address of the New Access Point
2 Link-Layer Address of the MN
3 Link-Layer Address of the NAR (i.e., Proxied Originator)
4 Link-Layer Address of the source of the RtSolPr or PrRtAdv message
5 The access point identified by the LLA belongs to the current interface of the router
6 No prefix information available for the access point identified by the LLA
7 No fast handovers support available for the access point identified by the LLA

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3207
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Router

Requirement:
Depending on the size of the individual LLA option, appropriate padding MUST be used to ensure that the entire option size is a multiple of 8 octets.

RFC Text:
Depending on the size of the individual LLA option, appropriate padding MUST be used to ensure that the entire option size is a multiple of 8 octets.

Identifier: RQ_001_3207
RFC Clause: 6.4.3
Type: Mandatory
Applies to: Mobile_Node

Requirement:
Depending on the size of the individual LLA option, appropriate padding MUST be used to ensure that the entire option size is a multiple of 8 octets.

RFC Text:
Depending on the size of the individual LLA option, appropriate padding MUST be used to ensure that the entire option size is a multiple of 8 octets.

Identifier: RQ_001_3208
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Router

Requirement:
The Mobility Header Link Layer Address Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-(8*N)	Pad
(8*N)+1-end	LLA

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].

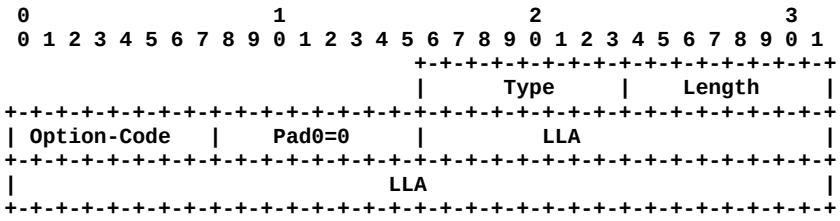


Figure 15: Mobility Header Link-Layer Address Option

Type 7

Length The size of this option in octets not including the Type, Length, and Option-Code fields.

Option-Code 2 Link-Layer Address of the MN

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3208
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Mobility Header Link Layer Address Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-(8*N)	Pad
(8*N)+1-end	LLA

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].

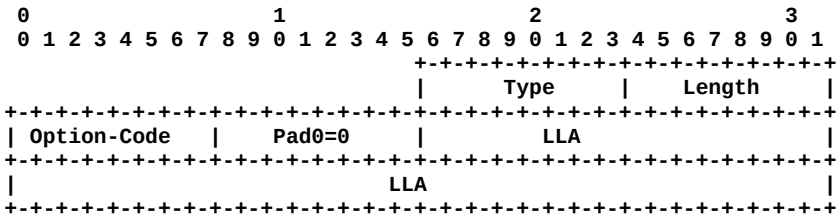


Figure 15: Mobility Header Link-Layer Address Option

Type 7

Length The size of this option in octets not including the Type, Length, and Option-Code fields.

Option-Code 2 Link-Layer Address of the MN

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3209
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Router

Requirement:
IN the Mobility Header Link Layer Address Option, the Type Field shall be set to 7.

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].

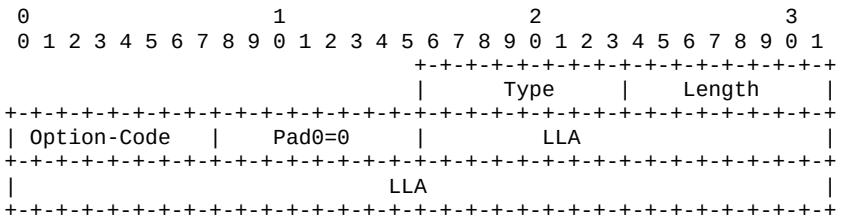


Figure 15: Mobility Header Link-Layer Address Option

Type **7**

Length The size of this option in octets not including the Type, Length, and Option-Code fields.

Option-Code 2 Link-Layer Address of the MN

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3209
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Mobility Header Link Layer Address Option, the Type Field shall be set to 7.

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].

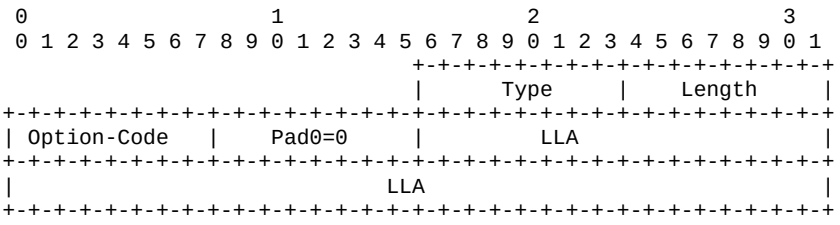


Figure 15: Mobility Header Link-Layer Address Option

Type **7**

Length The size of this option in octets not including the Type, Length, and Option-Code fields.

Option-Code 2 Link-Layer Address of the MN

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3210
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Router

Requirement:
IN the Mobility Header Link Layer Address Option, the Length Field shall be the size of this option in octets not including the Type, Length, and Option-Code fields.

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].

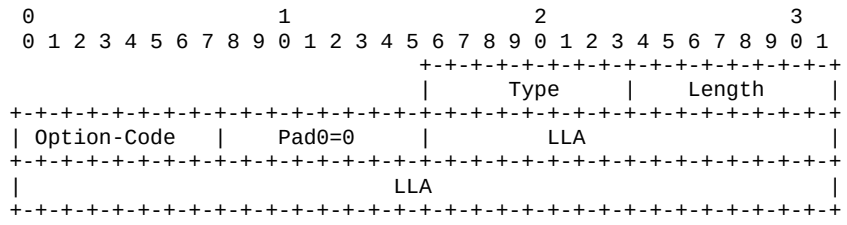


Figure 15: Mobility Header Link-Layer Address Option

Type 7

Length **The size of this option in octets not including the Type, Length, and Option-Code fields**.

Option-Code 2 Link-Layer Address of the MN

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3210
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Mobility Header Link Layer Address Option, the Length Field shall be the size of this option in octets not including the Type, Length, and Option-Code fields.

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].

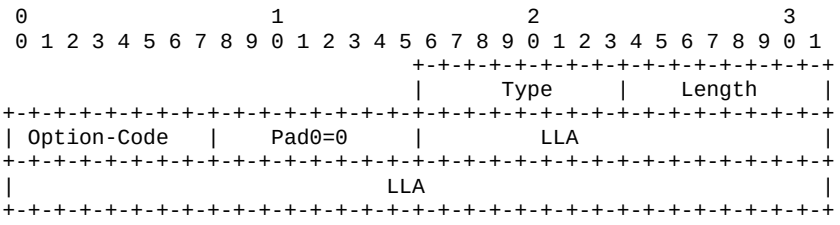


Figure 15: Mobility Header Link-Layer Address Option

Type 7

Length **The size of this option in octets not including the Type, Length, and Option-Code fields**.

Option-Code 2 Link-Layer Address of the MN

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3211
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Router

Requirement:
IN the Mobility Header Link Layer Address Option, the Option-Code Field shall be set to 2.

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].

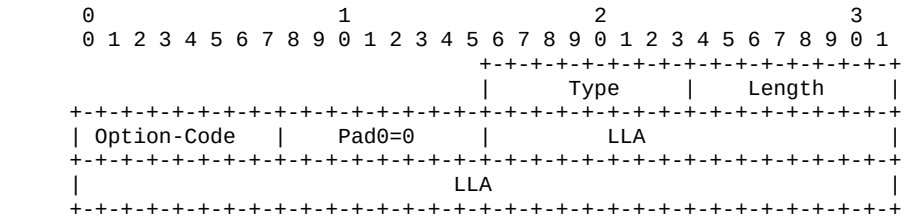


Figure 15: Mobility Header Link-Layer Address Option

Type 7

Length The size of this option in octets not including the Type, Length, and Option-Code fields.

Option-Code 2 Link-Layer Address of the MN

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3211
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Mobility Header Link Layer Address Option, the Option-Code Field shall be set to 2.

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].

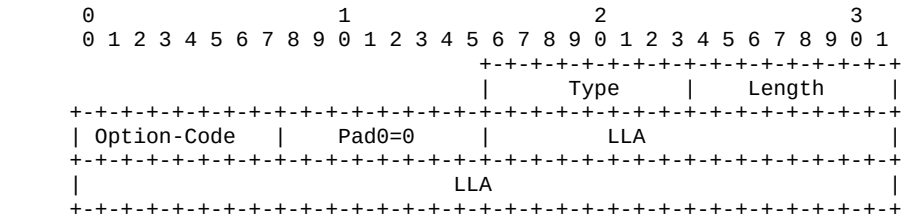


Figure 15: Mobility Header Link-Layer Address Option

Type 7

Length The size of this option in octets not including the Type, Length, and Option-Code fields.

Option-Code 2 Link-Layer Address of the MN

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3212
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Mobility Header Link Layer Address Option, the Pad Field shall contain a suitable Pad to aligned the option appropriately.

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. **The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].**

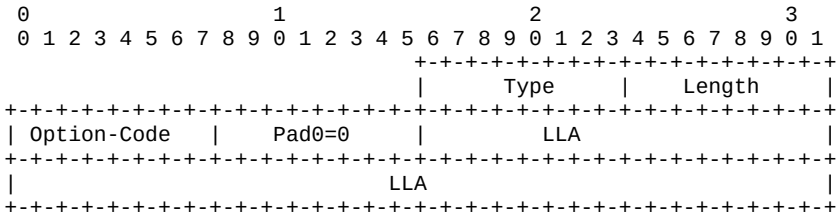


Figure 15: Mobility Header Link-Layer Address Option

Type	7
Length	The size of this option in octets not including the Type, Length, and Option-Code fields.
Option-Code	2 Link-Layer Address of the MN
LLA	The variable length Link-Layer Address.

Identifier: RQ_001_3213
RFC Clause: 6.4.4
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Mobility Header Link Layer Address Option, the LLA Field shall contain the variable length Link-Layer Address.

RFC Text:
This option is identical to the LLA option, but is carried in the Mobility Header messages (i.e., FNA). In the future, other Mobility Header messages may also make use of this option. For instance, including this option in FBU allows PAR to obtain the MN's LLA readily. The format of the option when the LLA is 6 bytes is shown in Figure 15. When the LLA size is different, the option MUST be aligned appropriately. See Section 6.2 in [3].

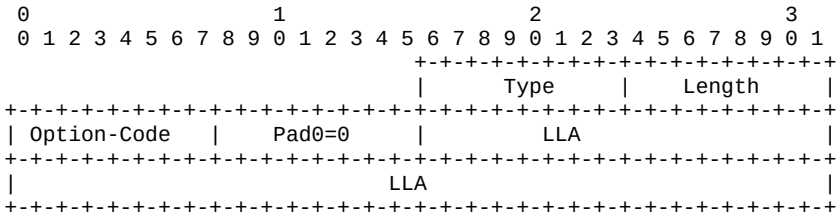


Figure 15: Mobility Header Link-Layer Address Option

Type 7

Length The size of this option in octets not including the Type, Length, and Option-Code fields.

Option-Code 2 Link-Layer Address of the MN

LLA The variable length Link-Layer Address.

Identifier: RQ_001_3214
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Router

Requirement:
The Neighbor Advertisement Acknowledgement Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-32	Status
33-64	Reserved

RFC Text:

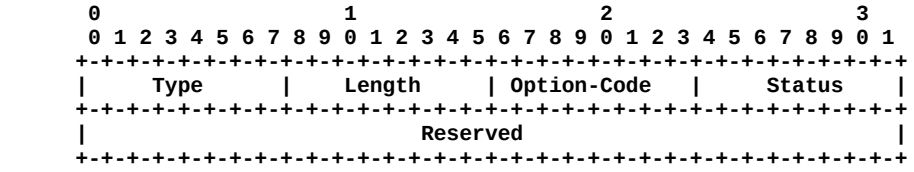


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3214
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
The Neighbor Advertisement Acknowledgement Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Length
17-24	Option-Code
25-32	Status
33-64	Reserved

RFC Text:

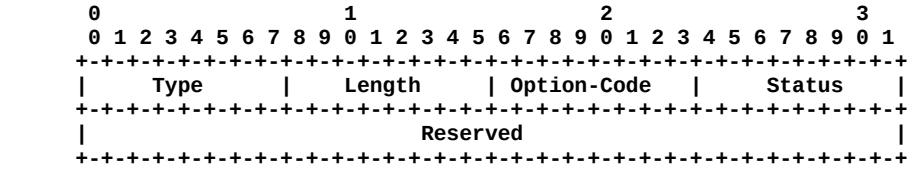


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3215
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Router

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Type Field shall be set to 20.

RFC Text:

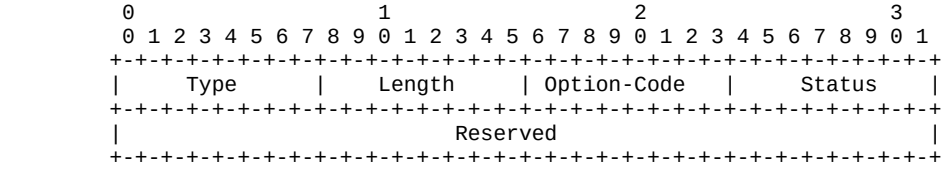


Figure 16: Neighbor Advertisement Acknowledgment Option

Type **20**

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3215
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Type Field shall be set to 20.

RFC Text:

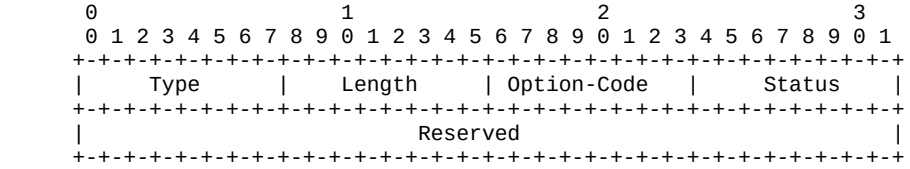


Figure 16: Neighbor Advertisement Acknowledgment Option

Type **20**

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3216
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Router

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Length Field shall be an 8-bit unsigned integer. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied.

RFC Text:

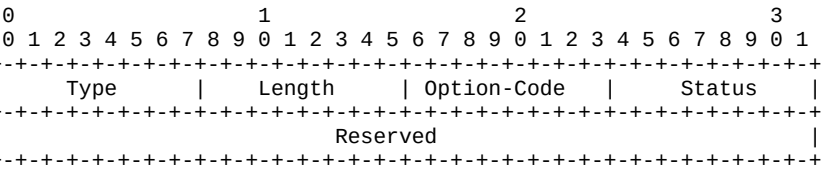


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length **8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).**

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3216
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Length Field shall be an 8-bit unsigned integer. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied.

RFC Text:

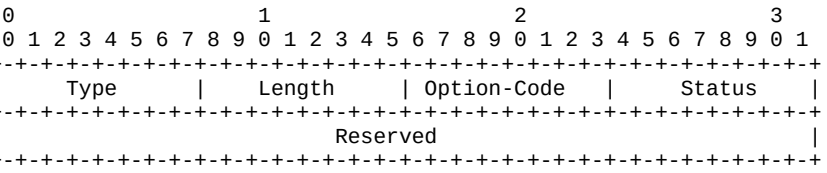


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length **8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).**

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3217
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Router

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Option-Code shall be set to 0.

RFC Text:

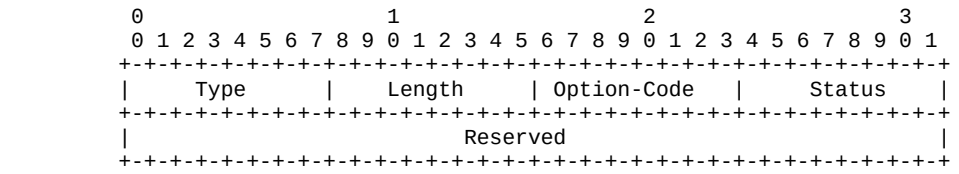


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3217
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Option-Code shall be set to 0.

RFC Text:

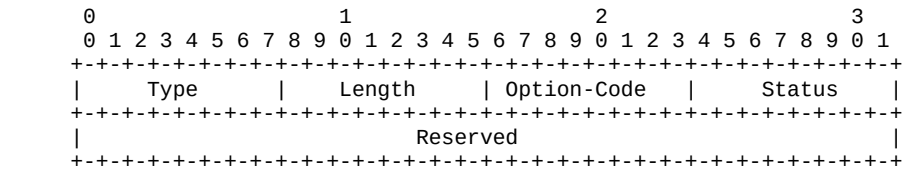


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3218
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Router

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Status Field shall contain an 8-bit unsigned integer of value 1, 2 or 128.

RFC Text:

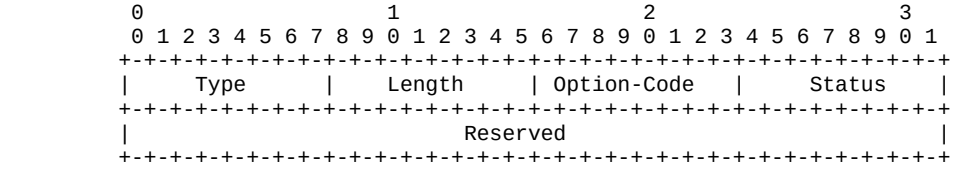


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3218
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Status Field shall contain an 8-bit unsigned integer of value 1, 2 or 128.

RFC Text:

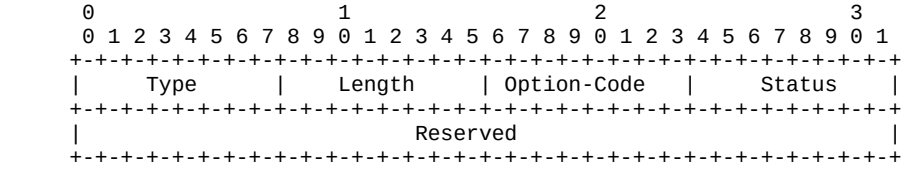


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and MUST be ignored by the receiver.

Identifier: RQ_001_3219
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Reserved Field MUST be set to zero by the sender.

RFC Text:

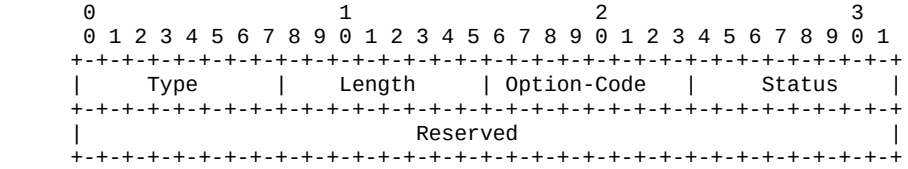


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved **MUST be set to zero by the sender** and MUST be ignored by the receiver.

Identifier: RQ_001_3220
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Router

Requirement:
IN the Neighbor Advertisement Acknowledgement Option, the Reserved Field MUST be ignored by the receiver.

RFC Text:

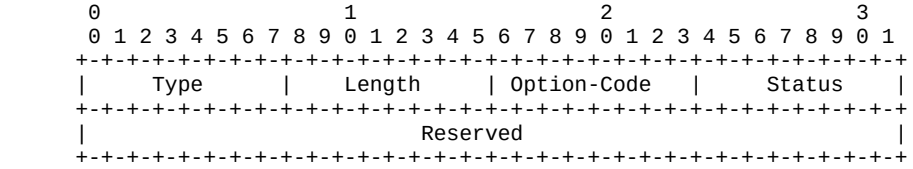


Figure 16: Neighbor Advertisement Acknowledgment Option

Type 20

Length 8-bit unsigned integer. Length of the option, in 8 octets. The length is 1 when NCoA is not supplied. The length is 3 when NCoA is supplied (immediately following the Reserved field).

Option-Code 0

Status 8-bit unsigned integer indicating the disposition of the Fast Neighbor Advertisement message. The following Status values are currently defined:

1 The New CoA is invalid.
2 The New CoA is invalid; use the supplied CoA. The New CoA MUST be present following the Reserved field.
128 Link Layer Address unrecognized.

Reserved MUST be set to zero by the sender and **MUST be ignored by the receiver.**

Identifier: RQ_001_3221
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Router

Requirement:
If the NCoA is invalid, the Router Advertisement MUST use the NCoA as the destination address but use the L2 address present in the FNA.

RFC Text:
The NAR responds to the FNA with the NAACK option to notify the MN to use a different NCoA if there is address collision. **If the NCoA is invalid, the Router Advertisement MUST use the NCoA as the destination address but use the L2 address present in the FNA. The MN SHOULD use the NCoA if it is supplied with the NAACK option.** If the NAACK indicates that the Link-Layer Address is unrecognized, the MN MUST NOT use the NCoA or PCoA and SHOULD start the process of acquiring an NCoA at the NAR immediately.

Identifier: RQ_001_3222
RFC Clause: 6.4.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
The MN SHOULD use the NCoA if it is supplied with the NAACK option.

RFC Text:
The NAR responds to the FNA with the NAACK option to notify the MN to use a different NCoA if there is address collision. If the NCoA is invalid, the Router Advertisement MUST use the NCoA as the destination address but use the L2 address present in the FNA. **The MN SHOULD use the NCoA if it is supplied with the NAACK option.** If the NAACK indicates that the Link-Layer Address is unrecognized, the MN MUST NOT use the NCoA or PCoA and SHOULD start the process of acquiring an NCoA at the NAR immediately.

Identifier: RQ_001_3223
RFC Clause: 6.4.5
Type: Mandatory
Applies to: Mobile_Node

Requirement:
If the NAACK indicates that the Link-Layer Address is unrecognized, the MN MUST NOT use the NCoA or PCoA.

RFC Text:
The NAR responds to the FNA with the NAACK option to notify the MN to use a different NCoA if there is address collision. If the NCoA is invalid, the Router Advertisement MUST use the NCoA as the destination address but use the L2 address present in the FNA. The MN SHOULD use the NCoA if it is supplied with the NAACK option. **If the NAACK indicates that the Link-Layer Address is unrecognized, the MN MUST NOT use the NCoA or PCoA** and SHOULD start the process of acquiring an NCoA at the NAR immediately.

Identifier: RQ_001_3224
RFC Clause: 6.4.5
Type: Recommendation
Applies to: Mobile_Node

Requirement:
If the NAACK indicates that the Link-Layer Address is unrecognized, the MN SHOULD start the process of acquiring an NCoA at the NAR immediately.

RFC Text:
The NAR responds to the FNA with the NAACK option to notify the MN to use a different NCoA if there is address collision. If the NCoA is invalid, the Router Advertisement MUST use the NCoA as the destination address but use the L2 address present in the FNA. The MN SHOULD use the NCoA if it is supplied with the NAACK option. If the NAACK indicates that the Link-Layer Address is unrecognized, **the MN** MUST NOT use the NCoA or PCoA and **SHOULD start the process of acquiring an NCoA at the NAR immediately.**

Identifier: RQ_001_3225
RFC Clause: 8
Type: Mandatory
Applies to: Router

Requirement:
The PAR MUST verify that the NCoA to which PCoA is being bound actually belongs to NAR's prefix.

RFC Text:
However, the target of malicious traffic redirection is limited to an interface on an access router with which the PAR has a security association. **The PAR MUST verify that the NCoA to which PCoA is being bound actually belongs to NAR's prefix.** To do this, HI and HAck message exchanges are to be used. When NAR accepts NCoA in HI (with Code = 0), it proxies NCoA so that any arriving packets are not sent on the link until the MN attaches and announces itself through FNA. Therefore, any inadvertent or malicious redirection to a host is avoided. It is still possible to jam NAR's buffer with redirected traffic. However, since NAR's handover state corresponding to NCoA has a finite (and short) lifetime corresponding to a small multiple of anticipated handover latency, the extent of this vulnerability is arguably small.

Identifier: RQ_001_3226
RFC Clause: 4
Type: Mandatory
Applies to: Router

Requirement:
As a response to the Router Solicitation for Proxy Advertisement (RtSolPr), if the new access point is known and the PAR has information about it, but it does not support fast handover, the PAR MUST indicate this with Code 3.

RFC Text:
As a response to RtSolPr, PAR sends a PrRtAdv message that indicates one of the following possible conditions.

1. If the PAR does not have an entry corresponding to the new access point, it MUST respond indicating that the new access point is unknown. The MN MUST stop fast handover protocol operations on the current link. The MN MAY send an FBU from its new link.

2. If the new access point is connected to the PAR's current interface (to which MN is attached), the PAR MUST respond with a Code value indicating that the new access point is connected to the current interface, but not send any prefix information. This scenario could arise, for example, when several wireless access points are bridged into a wired network. No further protocol action is necessary.

3. **If the new access point is known and the PAR has information about it**, then PAR MUST respond indicating that the new access point is known and supply the [AP-ID, AR-Info] tuple. **If the new access point is known, but does not support fast handover, the PAR MUST indicate this with Code 3 (See Section 6.1.2).**

4. If a wildcard is supplied as an identifier for the new access point, the PAR SHOULD supply neighborhood [AP-ID, AR-Info] tuples that are subject to path MTU restrictions (i.e., provide any `n' tuples without exceeding the link MTU).

Identifier: RQ_001_3227
RFC Clause: 5.2
Type: Optional
Applies to: Router

Requirement:
When the New Access Router (NAR) responds to HI using a HAck, it may include another NCoA to use.

RFC Text:
Typically, the MN formulates its prospective NCoA using the information provided in a PrRtAdv message and sends the FBU. The PAR MUST use the NCoA present in the FBU in its HI message. The NAR MUST verify if the NCoA present in HI is already in use. **In any case, NAR MUST respond to HI using a HAck, in which it may include another NCoA to use,** especially when assigned address configuration is used. If there is a CoA present in HAck, the PAR MUST include it in the FBack message.

4.4 Requirements extracted from RFC2473

Identifier: RQ_001_4001
RFC Clause: 3.1
Type: Mandatory
Applies to: Node

Requirement:
To prepare a packet for IPv6 tunnelling, the Tunnel Entry-Point Node shall encapsulate the packet by prepending to the original packet an IPv6 header plus zero or more IPv6 extension headers, which are collectively called tunnel IPv6 headers.

RFC Text:
IPv6 encapsulation consists of prepending to the original packet an IPv6 header and, optionally, a set of IPv6 extension headers (see Fig.3), which are collectively called tunnel IPv6 headers. The encapsulation takes place in an IPv6 tunnel entry-point node, as the result of an original packet being forwarded onto the virtual link represented by the tunnel. The original packet is processed during forwarding according to the forwarding rules of the protocol of that packet. For instance if the original packet is an:

(a) IPv6 packet, the IPv6 original header hop limit is decremented by one.

(b) IPv4 packet, the IPv4 original header time to live field (TTL) is decremented by one.

Identifier: RQ_001_4002
RFC Clause: 3.1
Type: Recommendation
Applies to: Mobile_Node

Requirement:
Tunnel extension headers should appear in the order recommended by the specifications that define the extension headers.

RFC Text:
Tunnel extension headers should appear in the order recommended by the specifications that define the extension headers, such as [IPv6-Spec].

Identifier: RQ_001_4003
RFC Clause: 3.2
Type: Mandatory
Applies to: Router

Requirement:
The intermediate nodes in the tunnel SHALL process the IPv6 tunnel packets according to the IPv6 protocol.

RFC Text:
The intermediate nodes in the tunnel process the IPv6 tunnel packets according to the IPv6 protocol. For example, a tunnel Hop by Hop Options extension header is processed by each receiving node in the tunnel; a tunnel Routing extension header identifies the intermediate processing nodes, and controls at a finer granularity the forwarding path of the tunnel packet through the tunnel; a tunnel Destination Options extension header is processed at the tunnel exit-point node.

Identifier: RQ_001_4004
RFC Clause: 3.3
Type: Mandatory
Applies to: Node

Requirement:
Upon receiving an IPv6 packet destined to an IPv6 address of a tunnel exit-point node, its IPv6 protocol layer processes the tunnel headers. The strict left-to-right processing rules for extension headers is applied.

RFC Text:
Upon receiving an IPv6 packet destined to an IPv6 address of a tunnel exit-point node, its IPv6 protocol layer processes the tunnel headers. The strict left-to-right processing rules for extension headers is applied. When processing is complete, control is handed to the next protocol engine, which is identified by the Next Header field value in the last header processed. If this is set to a tunnel protocol value, the tunnel protocol engine discards the tunnel headers and passes the resulting original packet to the Internet or lower layer protocol identified by that value for further processing.

Identifier: RQ_001_4005
RFC Clause: 3.1
Type: Mandatory
Applies to: Node

Requirement:
At encapsulation, the source field of the tunnel IPv6 header is filled with an IPv6 address of the tunnel entry-point node, and the destination field with an IPv6 address of the tunnel exit-point.

RFC Text:
At encapsulation, the source field of the tunnel IPv6 header is filled with an IPv6 address of the tunnel entry-point node, and the destination field with an IPv6 address of the tunnel exit-point. Subsequently, the tunnel packet resulting from encapsulation is sent towards the tunnel exit-point node.

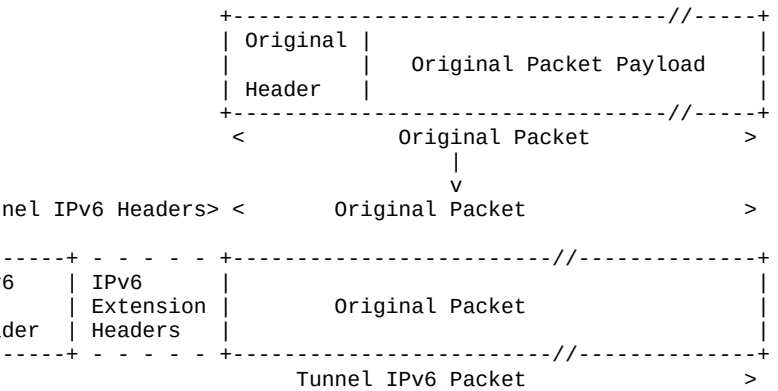


Fig.3 Encapsulating a Packet

Identifier: RQ_001_4006
RFC Clause: 3.3
Type: Mandatory
Applies to: Node

Requirement:
When processing is complete at the tunnel exit-point node, control is handed to the next protocol engine, which is identified by the Next Header field value in the last header processed.

RFC Text:
Upon receiving an IPv6 packet destined to an IPv6 address of a tunnel exit-point node, its IPv6 protocol layer processes the tunnel headers. The strict left-to-right processing rules for extension headers is applied. **When processing is complete, control is handed to the next protocol engine, which is identified by the Next Header field value in the last header processed.** If this is set to a tunnel protocol value, the tunnel protocol engine discards the tunnel headers and passes the resulting original packet to the Internet or lower layer protocol identified by that value for further processing.

Identifier: RQ_001_4007
RFC Clause: 3.3
Type: Mandatory
Applies to: Node

Requirement:
If the Next Header field value in the last header processed is set to a tunnel protocol value, the tunnel protocol engine discards the tunnel headers and passes the resulting original packet to the Internet or lower layer protocol identified by that value for further processing.

RFC Text:
Upon receiving an IPv6 packet destined to an IPv6 address of a tunnel exit-point node, its IPv6 protocol layer processes the tunnel headers. The strict left-to-right processing rules for extension headers is applied. When processing is complete, control is handed to the next protocol engine, which is identified by the Next Header field value in the last header processed. **If this is set to a tunnel protocol value, the tunnel protocol engine discards the tunnel headers and passes the resulting original packet to the Internet or lower layer protocol identified by that value for further processing.**

Identifier: RQ_001_4008
RFC Clause: 4
Type: Optional
Applies to: Node

Requirement:
A tunneled packet may be encapsulated and nested in one or more tunnels

RFC Text:
Nested IPv6 encapsulation is the encapsulation of a tunnel packet. It takes place when a hop of an IPv6 tunnel is a tunnel. The tunnel containing a tunnel is called an outer tunnel. The tunnel contained in the outer tunnel is called an inner tunnel - see Fig.6. Inner tunnels and their outer tunnels are nested tunnels.

Identifier: RQ_001_4009
RFC Clause: 4.1
Type: Recommendation
Applies to: Node

Requirement:
Limiting nested encapsulation is recommended.

RFC Text:
The increase in the size of a tunnel IPv6 packet due to nested encapsulations may require fragmentation [IPv6-Spec] at a tunnel entry point - see section 7. Furthermore, each fragmentation, due to nested encapsulation, of an already fragmented tunnel packet results in a doubling of the number of fragments. Moreover, it is probable that once this fragmentation begins, each new nested encapsulation results in yet additional fragmentation. **Therefore limiting nested encapsulation is recommended.**

The proposed mechanism for limiting excessive nested encapsulation is a "Tunnel Encapsulation Limit" option, which is carried in an IPv6 Destination Options extension header accompanying an encapsulating IPv6 header.

Identifier: RQ_001_4010
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:
The Tunnel Encapsulation Limit Option shall be structured as follows:

Bit	Field
1-8	Type
9-16	Opt Data Len value
17-24	Opt Data Value

RFC Text:
The Tunnel Encapsulation Limit option has the following format:

```
      Option Type     Opt Data Len   Opt Data Len
    0 1 2 3 4 5 6 7
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |0 0 0 0 0 1 0 0|       1       | Tun Encap Lim |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option Type decimal value 4

- the highest-order two bits - set to 00 - indicate "skip over this option if the option is not recognized".

- the third-highest-order bit - set to 0 - indicates that the option data in this option does not change en route to the packet's destination [IPv6-Spec].

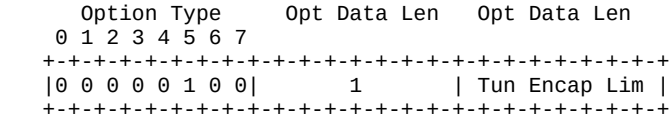
Opt Data Len value 1 - the data portion of the Option is one octet long.

Opt Data Value the Tunnel Encapsulation Limit value - 8-bit unsigned integer specifying how many further levels of encapsulation are permitted for the

Identifier: RQ_001_4011
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:
In the Tunnel Encapsulation Limit Option, the Type Field SHALL be set with the decimal value 4 (0000100).

RFC Text:
The Tunnel Encapsulation Limit option has the following format:



Option Type decimal value 4

- the highest-order two bits - set to 00 - indicate "skip over this option if the option is not recognized".

- the third-highest-order bit - set to 0 - indicates that the option data in this option does not change en route to the packet's destination [IPv6-Spec].

Opt Data Len value 1 - the data portion of the Option is one octet long.

Opt Data Value the Tunnel Encapsulation Limit value - 8-bit unsigned integer specifying how many further levels of encapsulation are permitted for the

Identifier: RQ_001_4012
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:
In the Tunnel Encapsulation Limit Option, the Opt Data Len Field SHALL be set to 1.

RFC Text:
The Tunnel Encapsulation Limit option has the following format:

```
   Option Type     Opt Data Len   Opt Data Len
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0 0 0 1 0 0|       1       | Tun Encap Lim |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option Type decimal value 4

- the highest-order two bits - set to 00 - indicate "skip over this option if the option is not recognized".

- the third-highest-order bit - set to 0 - indicates that the option data in this option does not change en route to the packet's destination [IPv6-Spec].

Opt Data Len value 1 - the data portion of the Option is one octet long.

Opt Data Value the Tunnel Encapsulation Limit value - 8-bit unsigned integer specifying how many further levels of encapsulation are permitted for the

Identifier: RQ_001_4013
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:
In the Tunnel Encapsulation Limit Option, the Opt Data Value Field SHALL be an 8-bit unsigned integer set to the Tunnel Encapsulation Limit value.

RFC Text:
The Tunnel Encapsulation Limit option has the following format:

```
      Option Type     Opt Data Len   Opt Data Len
    0 1 2 3 4 5 6 7
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |0 0 0 0 0 1 0 0|       1       | Tun Encap Lim |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option Type decimal value 4

- the highest-order two bits - set to 00 - indicate "skip over this option if the option is not recognized".

- the third-highest-order bit - set to 0 - indicates that the option data in this option does not change en route to the packet's destination [IPv6-Spec].

Opt Data Len value 1 - the data portion of the Option is one octet long.

Opt Data Value the Tunnel Encapsulation Limit value - 8-bit unsigned integer specifying how many further levels of encapsulation are permitted for the

Identifier: RQ_001_4014
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:
For every packet entering a tunnel at that node, the tunnel entry-point node SHALL examine the packet to see if a Tunnel Encapsulation Limit option is present following its IPv6 header.

RFC Text:
Tunnel Encapsulation Limit options are of interest only to tunnel entry points. A tunnel entry-point node is required to execute the following procedure for every packet entering a tunnel at that node:

(a) **Examine the packet to see if a Tunnel Encapsulation Limit option is present following its IPv6 header.** The headers following the IPv6 header must be examined in strict "left-to-right" order, with the examination stopping as soon as any one of the following headers is encountered: (i) a Destination Options extension header containing a Tunnel Encapsulation Limit, (ii) another IPv6 header, (iii) a non-extension header, such as TCP, UDP, or ICMP, or (iv) a header that cannot be parsed because it is encrypted or its type is unknown. (Note that this requirment is an exception to the general IPv6 rule that a Destination Options extension header need only be examined by a packet's destination node. An alternative and "cleaner" approach would have been to use a Hop-by-Hop extension header for this purpose, but that would have imposed an undesirable extra processing burden, and possible consequent extra delay, at every IPv6 node along the path of a tunnel.)

(b) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is zero, the packet is discarded and an ICMP Parameter Problem message [ICMP-Spec] is sent to the source of the packet, which is the previous tunnel entry-point node. The Code field of the Parameter Problem message is set to zero ("erroneous header field encountered") and the Pointer field is set to point to the third octet of the Tunnel Encapsulation Limit option (i.e., the octet containing the limit value of zero).

(c) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is non-zero, an additional Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the encapsulating option is set to one less than the limit value found in the packet being encapsulated.

(d) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if an encapsulation limit has been configured for this tunnel, a Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the option is set to the configured limit.

(e) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if no encapsulation limit has been configured for this tunnel, then no Tunnel Encapsulation Limit option is included as part of the encapsulating headers being added at this entry point.

Identifier: RQ_001_4015
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:
For every packet entering a tunnel at that node, the tunnel entry-point node SHALL examine the headers following the IPv6 header in strict "left-to-right" order.

RFC Text:
Tunnel Encapsulation Limit options are of interest only to tunnel entry points. A tunnel entry-point node is required to execute the following procedure for every packet entering a tunnel at that node:

(a) Examine the packet to see if a Tunnel Encapsulation Limit option is present following its IPv6 header. **The headers following the IPv6 header must be examined in strict "left-to-right" order**, with the examination stopping as soon as any one of the following headers is encountered: (i) a Destination Options extension header containing a Tunnel Encapsulation Limit, (ii) another IPv6 header, (iii) a non-extension header, such as TCP, UDP, or ICMP, or (iv) a header that cannot be parsed because it is encrypted or its type is unknown. (Note that this requirment is an exception to the general IPv6 rule that a Destination Options extension header need only be examined by a packet's destination node. An alternative and "cleaner" approach would have been to use a Hop-by-Hop extension header for this purpose, but that would have imposed an undesirable extra processing burden, and possible consequent extra delay, at every IPv6 node along the path of a tunnel.)

(b) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is zero, the packet is discarded and an ICMP Parameter Problem message [ICMP-Spec] is sent to the source of the packet, which is the previous tunnel entry-point node. The Code field of the Parameter Problem message is set to zero ("erroneous header field encountered") and the Pointer field is set to point to the third octet of the Tunnel Encapsulation Limit option (i.e., the octet containing the limit value of zero).

(c) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is non-zero, an additional Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the encapsulating option is set to one less than the limit value found in the packet being encapsulated.

(d) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if an encapsulation limit has been configured for this tunnel, a Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the option is set to the configured limit.

(e) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if no encapsulation limit has been configured for this tunnel, then no Tunnel Encapsulation Limit option is included as part of the encapsulating headers being added at this entry point.

Identifier: RQ_001_4016
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:

For every packet entering a tunnel at that node, the tunnel entry-point node SHALL stop examinitation of the headers following the IPv6 header as soon as any one of the following headers is encountered:

(i) a Destination Options extension header containing a Tunnel Encapsulation Limit,
(ii) another IPv6 header,
(iii) a non-extension header, such as TCP, UDP, or ICMP, or
(iv) a header that cannot be parsed because it is encrypted or its type is unknown.

RFC Text:

Tunnel Encapsulation Limit options are of interest only to tunnel entry points. A tunnel entry-point node is required to execute the following procedure for every packet entering a tunnel at that node:

(a) **Examine the packet to see if a Tunnel Encapsulation Limit option is present following its IPv6 header. The headers following the IPv6 header must be examined in strict "left-to-right" order, with the examination stopping as soon as any one of the following headers is encountered: (i) a Destination Options extension header containing a Tunnel Encapsulation Limit, (ii) another IPv6 header, (iii) a non-extension header, such as TCP, UDP, or ICMP, or (iv) a header that cannot be parsed because it is encrypted or its type is unknown.** (Note that this requirment is an exception to the general IPv6 rule that a Destination Options extension header need only be examined by a packet's destination node. An alternative and "cleaner" approach would have been to use a Hop-by-Hop extension header for this purpose, but that would have imposed an undesirable extra processing burden, and possible consequent extra delay, at every IPv6 node along the path of a tunnel.)

(b) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is zero, the packet is discarded and an ICMP Parameter Problem message [ICMP-Spec] is sent to the source of the packet, which is the previous tunnel entry-point node. The Code field of the Parameter Problem message is set to zero ("erroneous header field encountered") and the Pointer field is set to point to the third octet of the Tunnel Encapsulation Limit option (i.e., the octet containing the limit value of zero).

(c) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is non-zero, an additional Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the encapsulating option is set to one less than the limit value found in the packet being encapsulated.

(d) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if an encapsulation limit has been configured for this tunnel, a Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the option is set to the configured limit.

(e) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if no encapsulation limit has been configured for this tunnel, then no Tunnel Encapsulation Limit option is included as part of the encapsulating headers being added at this entry point.

Identifier: RQ_001_4017
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:

When the tunnel entry point finds a Tunnel Encapsulation Limit option in the packet entering the tunnel and its limit value is zero, the packet is discarded and an ICMP Parameter Problem message [ICMP-Spec] is sent to the source of the packet, with the Code field of the Parameter Problem message set to zero and the Pointer field is set to point to the third octet of the Tunnel Encapsulation Limit option

RFC Text:

Tunnel Encapsulation Limit options are of interest only to tunnel entry points. A tunnel entry-point node is required to execute the following procedure for every packet entering a tunnel at that node:

(a) Examine the packet to see if a Tunnel Encapsulation Limit option is present following its IPv6 header. The headers following the IPv6 header must be examined in strict "left-to-right" order, with the examination stopping as soon as any one of the following headers is encountered: (i) a Destination Options extension header containing a Tunnel Encapsulation Limit, (ii) another IPv6 header, (iii) a non-extension header, such as TCP, UDP, or ICMP, or (iv) a header that cannot be parsed because it is encrypted or its type is unknown. (Note that this requirment is an exception to the general IPv6 rule that a Destination Options extension header need only be examined by a packet's destination node. An alternative and "cleaner" approach would have been to use a Hop-by-Hop extension header for this purpose, but that would have imposed an undesirable extra processing burden, and possible consequent extra delay, at every IPv6 node along the path of a tunnel.)

(b**) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is zero, the packet is discarded and an ICMP Parameter Problem message [ICMP-Spec] is sent to the source of the packet, which is the previous tunnel entry-point node. The Code field of the Parameter Problem message is set to zero ("erroneous header field encountered") and the Pointer field is set to point to the third octet of the Tunnel Encapsulation Limit option (i.e., the octet containing the limit value of zero)**.

(c) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is non-zero, an additional Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the encapsulating option is set to one less than the limit value found in the packet being encapsulated.

(d) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if an encapsulation limit has been configured for this tunnel, a Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the option is set to the configured limit.

(e) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if no encapsulation limit has been configured for this tunnel, then no Tunnel Encapsulation Limit option is included as part of the encapsulating headers being added at this entry point.

Identifier: RQ_001_4018
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:
When the tunnel entry point finds a Tunnel Encapsulation Limit option in the packet entering the tunnel and its limit value is non-zero, an additional Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point, with the limit value in the encapsulating option set to one less than the limit value found in the packet being encapsulated.

RFC Text:
Tunnel Encapsulation Limit options are of interest only to tunnel entry points. A tunnel entry-point node is required to execute the following procedure for every packet entering a tunnel at that node:

(a) Examine the packet to see if a Tunnel Encapsulation Limit option is present following its IPv6 header. The headers following the IPv6 header must be examined in strict "left-to-right" order, with the examination stopping as soon as any one of the following headers is encountered: (i) a Destination Options extension header containing a Tunnel Encapsulation Limit, (ii) another IPv6 header, (iii) a non-extension header, such as TCP, UDP, or ICMP, or (iv) a header that cannot be parsed because it is encrypted or its type is unknown. (Note that this requirment is an exception to the general IPv6 rule that a Destination Options extension header need only be examined by a packet's destination node. An alternative and "cleaner" approach would have been to use a Hop-by-Hop extension header for this purpose, but that would have imposed an undesirable extra processing burden, and possible consequent extra delay, at every IPv6 node along the path of a tunnel.)

(b) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is zero, the packet is discarded and an ICMP Parameter Problem message [ICMP-Spec] is sent to the source of the packet, which is the previous tunnel entry-point node. The Code field of the Parameter Problem message is set to zero ("erroneous header field encountered") and the Pointer field is set to point to the third octet of the Tunnel Encapsulation Limit option (i.e., the octet containing the limit value of zero).

(c) **If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is non-zero, an additional Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the encapsulating option is set to one less than the limit value found in the packet being encapsulated.**

(d) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if an encapsulation limit has been configured for this tunnel, a Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the option is set to the configured limit.

(e) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if no encapsulation limit has been configured for this tunnel, then no Tunnel Encapsulation Limit option is included as part of the encapsulating headers being added at this entry point.

Identifier: RQ_001_4019
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:
If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if no encapsulation limit has been configured for this tunnel, then no Tunnel Encapsulation Limit option is included as part of the encapsulating headers being added at this entry point and the limit value in the option is set to the configured limit.

RFC Text:
Tunnel Encapsulation Limit options are of interest only to tunnel entry points. A tunnel entry-point node is required to execute the following procedure for every packet entering a tunnel at that node:

(a) Examine the packet to see if a Tunnel Encapsulation Limit option is present following its IPv6 header. The headers following the IPv6 header must be examined in strict "left-to-right" order, with the examination stopping as soon as any one of the following headers is encountered: (i) a Destination Options extension header containing a Tunnel Encapsulation Limit, (ii) another IPv6 header, (iii) a non-extension header, such as TCP, UDP, or ICMP, or (iv) a header that cannot be parsed because it is encrypted or its type is unknown. (Note that this requirment is an exception to the general IPv6 rule that a Destination Options extension header need only be examined by a packet's destination node. An alternative and "cleaner" approach would have been to use a Hop-by-Hop extension header for this purpose, but that would have imposed an undesirable extra processing burden, and possible consequent extra delay, at every IPv6 node along the path of a tunnel.)

(b) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is zero, the packet is discarded and an ICMP Parameter Problem message [ICMP-Spec] is sent to the source of the packet, which is the previous tunnel entry-point node. The Code field of the Parameter Problem message is set to zero ("erroneous header field encountered") and the Pointer field is set to point to the third octet of the Tunnel Encapsulation Limit option (i.e., the octet containing the limit value of zero).

(c) If a Tunnel Encapsulation Limit option is found in the packet entering the tunnel and its limit value is non-zero, an additional Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the encapsulating option is set to one less than the limit value found in the packet being encapsulated.

(d) If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if an encapsulation limit has been configured for this tunnel, a Tunnel Encapsulation Limit option must be included as part of the encapsulating headers being added at this entry point. The limit value in the option is set to the configured limit.

(e) **If a Tunnel Encapsulation Limit option is not found in the packet entering the tunnel and if no encapsulation limit has been configured for this tunnel, then no Tunnel Encapsulation Limit option is included as part of the encapsulating headers being added at this entry point.**

Identifier: RQ_001_4020
RFC Clause: 4.1.1
Type: Mandatory
Applies to: Node

Requirement:
A Tunnel Encapsulation Limit option added at a tunnel entry-point node is removed as part of the decapsulation process at that tunnel's exit-point node.

RFC Text:
A Tunnel Encapsulation Limit option added at a tunnel entry-point node is removed as part of the decapsulation process at that tunnel's exit-point node.

Identifier: RQ_001_4021
RFC Clause: 4.1.3
Type: Recommendation
Applies to: Node

Requirement:
When the path of a packet from source to final destination includes tunnels, the maximum number of hops that the packet can traverse should be controlled by two mechanisms used together to avoid the negative effects of recursive encapsulation in routing loops:

(a) the original packet hop limit.
(b) the tunnel IPv6 packet encapsulation limit.

RFC Text:
In the case of a forwarding path with multiple-level nested tunnels, a routing-loop from an inner tunnel to an outer tunnel is particularly dangerous when packets from the inner tunnels reenter an outer tunnel from which they have not yet exited. In such a case, the nested encapsulation becomes a recursive encapsulation with the negative effects described in 4.1. Because each nested encapsulation adds a tunnel header with a new hop limit value, the IPv6 hop limit mechanism cannot control the number of times the packet reaches the outer tunnel entry-point node, and thus cannot control the number of recursive encapsulations.

When the path of a packet from source to final destination includes tunnels, the maximum number of hops that the packet can traverse should be controlled by two mechanisms used together to avoid the negative effects of recursive encapsulation in routing loops:

(a) the original packet hop limit.

It is decremented at each forwarding operation performed on an original packet. This includes each encapsulation of the original packet. It does not include nested encapsulations of the original packet

(b) the tunnel IPv6 packet encapsulation limit.

It is decremented at each nested encapsulation of the packet.

Identifier: RQ_001_4022
RFC Clause: 5
Type: Mandatory
Applies to: Node

Requirement:
In the Main Header for the tunnel IPv6 packet, the the tunnel entry-point node shall insert value 6 in the Version Field.

RFC Text:
The tunnel entry-point node fills out a tunnel IPv6 main header [IPv6-Spec] as follows:

Version:

value 6

Traffic Class:

Depending on the entry-point node tunnel configuration, the traffic class can be set to that of either the original packet or a pre-configured value - see section 6.4.

Flow Label:

Depending on the entry-point node tunnel configuration, the flow label can be set to a pre-configured value. The typical value is zero - see section 6.5.

Payload Length:

The original packet length, plus the length of the encapsulating (prepended) IPv6 extension headers, if any.

Next Header:

The next header value according to [IPv6-Spec] from the Assigned Numbers RFC [RFC-1700 or its successors].

For example, if the original packet is an IPv6 packet, this is set to:

- decimal value 41 (Assigned Next Header number for IPv6) - if there are no tunnel extension headers.

- value 0 (Assigned Next Header number for IPv6 Hop by Hop Options extension header) - if a hop by hop options extension header immediately follows the tunnel IPv6 header.

- decimal value 60 (Assigned Next Header number for IPv6 Destination Options extension header) - if a destination options extension header immediately follows the tunnel IPv6 header.

Hop Limit:

The tunnel IPv6 header hop limit is set to a pre-configured value - see section 6.3.

The default value for hosts is the Neighbor Discovery advertised hop limit [ND-Spec]. The default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).

Source Address:

An IPv6 address of the outgoing interface of the tunnel entry-point node. This address is configured as the tunnel entry-point node address - see section 6.1.

Destination Address:

An IPv6 address of the tunnel exit-point node. This address is configured as the tunnel exit-point node address - see section 6.2.

Identifier: RQ_001_4023
RFC Clause: 5
Type: Mandatory
Applies to: Node

Requirement:
In the Main Header for the tunnel IPv6 packet, the the tunnel entry-point node fills in the Traffic Class field as either the original packet or a pre-configured value.

RFC Text:
The tunnel entry-point node fills out a tunnel IPv6 main header [IPv6-Spec] as follows:

```
      Version:

        value 6

      Traffic Class:

        Depending on the entry-point node tunnel configuration, the
        traffic class can be set to that of either the original
        packet or a pre-configured value - see section 6.4.

      Flow Label:

        Depending on the entry-point node tunnel configuration, the
        flow label can be set to a pre-configured value. The typical
        value is zero - see section 6.5.

      Payload Length:

        The original packet length, plus the length of the
        encapsulating (prepended) IPv6 extension headers, if any.

      Next Header:

        The next header value according to [IPv6-Spec] from the
        Assigned Numbers RFC [RFC-1700 or its successors].

        For example, if the original packet is an IPv6 packet, this
        is set to:

             - decimal value 41 (Assigned Next Header number for
             IPv6) - if there are no tunnel extension headers.

             - value 0 (Assigned Next Header number for IPv6 Hop by
             Hop Options extension header) - if a hop by hop options
             extension header immediately follows the tunnel IPv6
             header.

             - decimal value 60 (Assigned Next Header number for
             IPv6 Destination Options extension header) - if a
             destination options extension header immediately
             follows the tunnel IPv6 header.

      Hop Limit:

        The tunnel IPv6 header hop limit is set to a pre-configured
        value - see section 6.3.

        The default value for hosts is the Neighbor Discovery
        advertised hop limit [ND-Spec].  The default value for
        routers is the default IPv6 Hop Limit value from the
        Assigned Numbers RFC (64 at the time of writing this
        document).

      Source Address:

        An IPv6 address of the outgoing interface of the tunnel
        entry-point node.  This address is configured as the tunnel
        entry-point node address - see section 6.1.

      Destination Address:

        An IPv6 address of the tunnel exit-point node. This address
        is configured as the tunnel exit-point node address - see
        section 6.2.
```

Identifier: RQ_001_4024
RFC Clause: 5
Type: Mandatory
Applies to: Node

Requirement:
In the Main Header for the tunnel IPv6 packet, the the tunnel entry-point node fills in the Flow Label field to a pre-configured value.

RFC Text:
The tunnel entry-point node fills out a tunnel IPv6 main header [IPv6-Spec] as follows:

Version:

value 6

Traffic Class:

Depending on the entry-point node tunnel configuration, the traffic class can be set to that of either the original packet or a pre-configured value - see section 6.4.

Flow Label:

Depending on the entry-point node tunnel configuration, the flow label can be set to a pre-configured value. The typical value is zero - see section 6.5.

Payload Length:

The original packet length, plus the length of the encapsulating (prepended) IPv6 extension headers, if any.

Next Header:

The next header value according to [IPv6-Spec] from the Assigned Numbers RFC [RFC-1700 or its successors].

For example, if the original packet is an IPv6 packet, this is set to:

- decimal value 41 (Assigned Next Header number for IPv6) - if there are no tunnel extension headers.

- value 0 (Assigned Next Header number for IPv6 Hop by Hop Options extension header) - if a hop by hop options extension header immediately follows the tunnel IPv6 header.

- decimal value 60 (Assigned Next Header number for IPv6 Destination Options extension header) - if a destination options extension header immediately follows the tunnel IPv6 header.

Hop Limit:

The tunnel IPv6 header hop limit is set to a pre-configured value - see section 6.3.

The default value for hosts is the Neighbor Discovery advertised hop limit [ND-Spec]. The default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).

Source Address:

An IPv6 address of the outgoing interface of the tunnel entry-point node. This address is configured as the tunnel entry-point node address - see section 6.1.

Destination Address:

An IPv6 address of the tunnel exit-point node. This address is configured as the tunnel exit-point node address - see section 6.2.

Identifier: RQ_001_4025
RFC Clause: 5
Type: Mandatory
Applies to: Node

Requirement:
In the Main Header for the tunnel IPv6 packet, the the tunnel entry-point node fills in the Payload Length field to the original packet length, plus the length of the encapsulating (prepended) IPv6 extension headers, if any.

RFC Text:
The tunnel entry-point node fills out a tunnel IPv6 main header [IPv6-Spec] as follows:

Version:

value 6

Traffic Class:

Depending on the entry-point node tunnel configuration, the traffic class can be set to that of either the original packet or a pre-configured value - see section 6.4.

Flow Label:

Depending on the entry-point node tunnel configuration, the flow label can be set to a pre-configured value. The typical value is zero - see section 6.5.

Payload Length:

The original packet length, plus the length of the encapsulating (prepended) IPv6 extension headers, if any.

Next Header:

The next header value according to [IPv6-Spec] from the Assigned Numbers RFC [RFC-1700 or its successors].

For example, if the original packet is an IPv6 packet, this is set to:

- decimal value 41 (Assigned Next Header number for IPv6) - if there are no tunnel extension headers.

- value 0 (Assigned Next Header number for IPv6 Hop by Hop Options extension header) - if a hop by hop options extension header immediately follows the tunnel IPv6 header.

- decimal value 60 (Assigned Next Header number for IPv6 Destination Options extension header) - if a destination options extension header immediately follows the tunnel IPv6 header.

Hop Limit:

The tunnel IPv6 header hop limit is set to a pre-configured value - see section 6.3.

The default value for hosts is the Neighbor Discovery advertised hop limit [ND-Spec]. The default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).

Source Address:

An IPv6 address of the outgoing interface of the tunnel entry-point node. This address is configured as the tunnel entry-point node address - see section 6.1.

Destination Address:

An IPv6 address of the tunnel exit-point node. This address is configured as the tunnel exit-point node address - see section 6.2.

Identifier: RQ_001_4026
RFC Clause: 5
Type:
Applies to: Node

Requirement:
In the Main Header for the tunnel IPv6 packet, the the tunnel entry-point node fills in the Next Header field to the next header value according to [RFC 2460] from the Assigned Numbers RFC [RFC-1700 or its successors].

RFC Text:
The tunnel entry-point node fills out a tunnel IPv6 main header [IPv6-Spec] as follows:

Version:

value 6

Traffic Class:

Depending on the entry-point node tunnel configuration, the traffic class can be set to that of either the original packet or a pre-configured value - see section 6.4.

Flow Label:

Depending on the entry-point node tunnel configuration, the flow label can be set to a pre-configured value. The typical value is zero - see section 6.5.

Payload Length:

The original packet length, plus the length of the encapsulating (prepended) IPv6 extension headers, if any.

Next Header:

The next header value according to [IPv6-Spec] from the Assigned Numbers RFC [RFC-1700 or its successors].

For example, if the original packet is an IPv6 packet, this is set to:

- decimal value 41 (Assigned Next Header number for IPv6) - if there are no tunnel extension headers.

- value 0 (Assigned Next Header number for IPv6 Hop by Hop Options extension header) - if a hop by hop options extension header immediately follows the tunnel IPv6 header.

- decimal value 60 (Assigned Next Header number for IPv6 Destination Options extension header) - if a destination options extension header immediately follows the tunnel IPv6 header.

Hop Limit:

The tunnel IPv6 header hop limit is set to a pre-configured value - see section 6.3.

The default value for hosts is the Neighbor Discovery advertised hop limit [ND-Spec]. The default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).

Source Address:

An IPv6 address of the outgoing interface of the tunnel entry-point node. This address is configured as the tunnel entry-point node address - see section 6.1.

Destination Address:

An IPv6 address of the tunnel exit-point node. This address is configured as the tunnel exit-point node address - see section 6.2.

Identifier: RQ_001_4027
RFC Clause: 5
Type: Mandatory
Applies to: Node

Requirement:
In the Main Header for the tunnel IPv6 packet, the the tunnel entry-point node fills in the Hop Limit field to a pre-configured value.

RFC Text:
The tunnel entry-point node fills out a tunnel IPv6 main header [IPv6-Spec] as follows:

Version:

value 6

Traffic Class:

Depending on the entry-point node tunnel configuration, the traffic class can be set to that of either the original packet or a pre-configured value - see section 6.4.

Flow Label:

Depending on the entry-point node tunnel configuration, the flow label can be set to a pre-configured value. The typical value is zero - see section 6.5.

Payload Length:

The original packet length, plus the length of the encapsulating (prepended) IPv6 extension headers, if any.

Next Header:

The next header value according to [IPv6-Spec] from the Assigned Numbers RFC [RFC-1700 or its successors].

For example, if the original packet is an IPv6 packet, this is set to:

- decimal value 41 (Assigned Next Header number for IPv6) - if there are no tunnel extension headers.

- value 0 (Assigned Next Header number for IPv6 Hop by Hop Options extension header) - if a hop by hop options extension header immediately follows the tunnel IPv6 header.

- decimal value 60 (Assigned Next Header number for IPv6 Destination Options extension header) - if a destination options extension header immediately follows the tunnel IPv6 header.

Hop Limit:

The tunnel IPv6 header hop limit is set to a pre-configured value - see section 6.3.

The default value for hosts is the Neighbor Discovery advertised hop limit [ND-Spec]. The default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).

Source Address:

An IPv6 address of the outgoing interface of the tunnel entry-point node. This address is configured as the tunnel entry-point node address - see section 6.1.

Destination Address:

An IPv6 address of the tunnel exit-point node. This address is configured as the tunnel exit-point node address - see section 6.2.

Identifier: RQ_001_4028
RFC Clause: 5
Type: Mandatory
Applies to: Node

Requirement:
In the Main Header for the tunnel IPv6 packet, the the tunnel entry-point node fills in the Source Address field to the tunnel entry-point node address.

RFC Text:
The tunnel entry-point node fills out a tunnel IPv6 main header [IPv6-Spec] as follows:

Version:

value 6

Traffic Class:

Depending on the entry-point node tunnel configuration, the traffic class can be set to that of either the original packet or a pre-configured value - see section 6.4.

Flow Label:

Depending on the entry-point node tunnel configuration, the flow label can be set to a pre-configured value. The typical value is zero - see section 6.5.

Payload Length:

The original packet length, plus the length of the encapsulating (prepended) IPv6 extension headers, if any.

Next Header:

The next header value according to [IPv6-Spec] from the Assigned Numbers RFC [RFC-1700 or its successors].

For example, if the original packet is an IPv6 packet, this is set to:

- decimal value 41 (Assigned Next Header number for IPv6) - if there are no tunnel extension headers.

- value 0 (Assigned Next Header number for IPv6 Hop by Hop Options extension header) - if a hop by hop options extension header immediately follows the tunnel IPv6 header.

- decimal value 60 (Assigned Next Header number for IPv6 Destination Options extension header) - if a destination options extension header immediately follows the tunnel IPv6 header.

Hop Limit:

The tunnel IPv6 header hop limit is set to a pre-configured value - see section 6.3.

The default value for hosts is the Neighbor Discovery advertised hop limit [ND-Spec]. The default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).

Source Address:

An IPv6 address of the outgoing interface of the tunnel entry-point node. This address is configured as the tunnel entry-point node address - see section 6.1.

Destination Address:

An IPv6 address of the tunnel exit-point node. This address is configured as the tunnel exit-point node address - see section 6.2.

Identifier: RQ_001_4029
RFC Clause: 5
Type: Mandatory
Applies to: Node

Requirement:
In the Main Header for the tunnel IPv6 packet, the the tunnel entry-point node fills in the Destination Address field to the tunnel exit-point node address.

RFC Text:
The tunnel entry-point node fills out a tunnel IPv6 main header [IPv6-Spec] as follows:

Version:

value 6

Traffic Class:

Depending on the entry-point node tunnel configuration, the traffic class can be set to that of either the original packet or a pre-configured value - see section 6.4.

Flow Label:

Depending on the entry-point node tunnel configuration, the flow label can be set to a pre-configured value. The typical value is zero - see section 6.5.

Payload Length:

The original packet length, plus the length of the encapsulating (prepended) IPv6 extension headers, if any.

Next Header:

The next header value according to [IPv6-Spec] from the Assigned Numbers RFC [RFC-1700 or its successors].

For example, if the original packet is an IPv6 packet, this is set to:

- decimal value 41 (Assigned Next Header number for IPv6) - if there are no tunnel extension headers.

- value 0 (Assigned Next Header number for IPv6 Hop by Hop Options extension header) - if a hop by hop options extension header immediately follows the tunnel IPv6 header.

- decimal value 60 (Assigned Next Header number for IPv6 Destination Options extension header) - if a destination options extension header immediately follows the tunnel IPv6 header.

Hop Limit:

The tunnel IPv6 header hop limit is set to a pre-configured value - see section 6.3.

The default value for hosts is the Neighbor Discovery advertised hop limit [ND-Spec]. The default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).

Source Address:

An IPv6 address of the outgoing interface of the tunnel entry-point node. This address is configured as the tunnel entry-point node address - see section 6.1.

Destination Address:

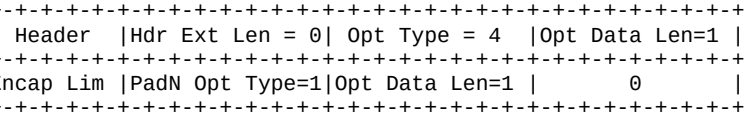
An IPv6 address of the tunnel exit-point node. This address is configured as the tunnel exit-point node address - see section 6.2.

Identifier: RQ_001_4030
RFC Clause: 5.1
Type: Optional
Applies to: Node

Requirement:
To limit the number of nested encapsulations of a packet, if it was configured to do so, a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option.

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |Hdr Ext Len = 0| Opt Type = 4  |Opt Data Len=1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Tun Encap Lim |PadN Opt Type=1|Opt Data Len=1 |       0       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

value 0 - one zero-valued octet.

Identifier: RQ_001_4031
RFC Clause: 5.1
Type: Mandatory
Applies to: Node

Requirement:

If the Tunnel Encapsulation Limit option is the only option present in the Destination Options extension header, the header has the following format:

Bits	Field
1-8	Next Header
9-16	Hdr Ext Len
17-24	Opt Type
25-32	Opt Data Len
33-40	Tun Encap Lim
41-48	PadN Opt Type
49-56	Opt Data Len
57-64	Option Data

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |Hdr Ext Len = 0| Opt Type = 4  |Opt Data Len=1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Tun Encap Lim |PadN Opt Type=1|Opt Data Len=1 |       0       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

value 0 - one zero-valued octet.

Identifier: RQ_001_4032
RFC Clause: 5.1
Type: Mandatory
Applies to: Node

Requirement:
If the Tunnel Encapsulation Limit option is the only option present in the Destination Options extension header, the next header field identifies the type of the original packet header

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |Hdr Ext Len = 0| Opt Type = 4  |Opt Data Len=1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Tun Encap Lim |PadN Opt Type=1|Opt Data Len=1 |       0       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

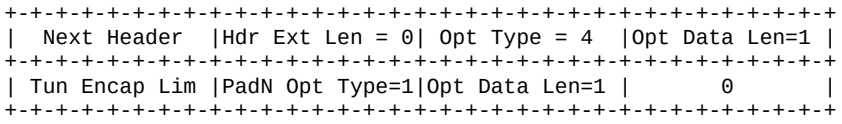
value 0 - one zero-valued octet.

Identifier: RQ_001_4033
RFC Clause: 5.1
Type: Mandatory
Applies to: Node

Requirement:
If the Tunnel Encapsulation Limit option is the only option present in the Destination Options extension header, the header extension length field is set to 0.

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:



Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

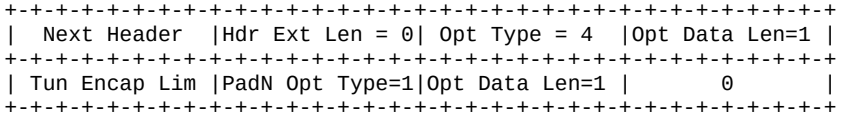
value 0 - one zero-valued octet.

Identifier: RQ_001_4034
RFC Clause: 5.1
Type: Mandatory
Applies to: Node

Requirement:
If the Tunnel Encapsulation Limit option is the only option present in the Destination Options extension header, the Option Type field is set to 4.

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |Hdr Ext Len = 0| Opt Type = 4  |Opt Data Len=1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Tun Encap Lim |PadN Opt Type=1|Opt Data Len=1 |       0       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

value 0 - one zero-valued octet.

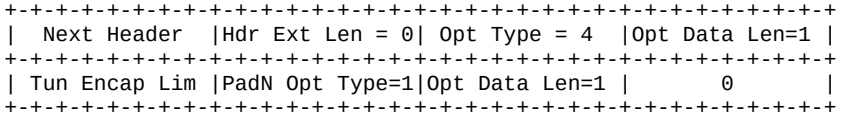
Identifier: RQ_001_4035
RFC Clause: 5.1
Type: Mandatory
Applies to: Node

Requirement:

If the Tunnel Encapsulation Limit option is the only option present in the Destination Options extension header, the Option Data Length field is set to 1.

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |Hdr Ext Len = 0| Opt Type = 4  |Opt Data Len=1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Tun Encap Lim |PadN Opt Type=1|Opt Data Len=1 |       0       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

value 0 - one zero-valued octet.

Identifier: RQ_001_4036
RFC Clause: 5.1
Type: Mandatory
Applies to: Node

Requirement:
If the Tunnel Encapsulation Limit option is the only option present in the Destination Options extension header, the Tunnel Encapsulation Limit field shall conatain an 8 bit unsigned integer.

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |Hdr Ext Len = 0| Opt Type = 4  |Opt Data Len=1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Tun Encap Lim |PadN Opt Type=1|Opt Data Len=1 |       0       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

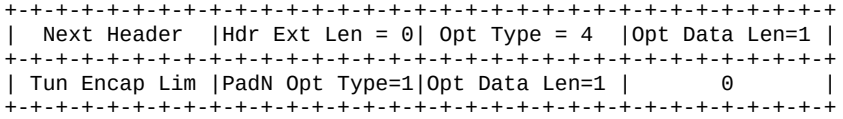
value 0 - one zero-valued octet.

Identifier: RQ_001_4037
RFC Clause: 5.1
Type: Mandatory
Applies to: Node

Requirement:
If the Tunnel Encapsulation Limit option is the only option present in the Destination Options extension header, the PadN Option type field shall be set to 1.

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:



Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

value 0 - one zero-valued octet.

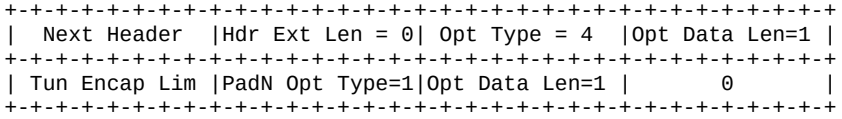
Identifier: RQ_001_4038
RFC Clause: 5.1
Type: Mandatory
Applies to: Node

Requirement:

If the Tunnel Encapsulation Limit option is the only option present in the Destination Options extension header, the Option Data Length field shall be set to 1.

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:



Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

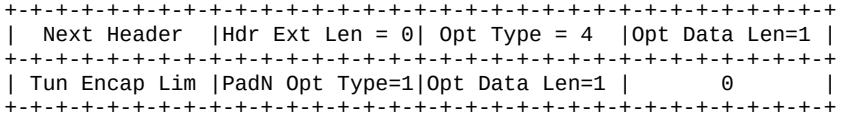
value 0 - one zero-valued octet.

Identifier: RQ_001_4039
RFC Clause: 5.1
Type: Mandatory
Applies to: Node

Requirement:
If the Tunnel Encapsulation Limit option is the only option present in the Destination Options extension header, the Option Data field shall be set to 0.

RFC Text:

To limit the number of nested encapsulations of a packet, if it was configured to do so - see section 6.6 - a tunnel entry-point includes a Destination Options extension header containing a Tunnel Encapsulation Limit option. If that option is the only option present in the Destination Options header, the header has the following format:



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |Hdr Ext Len = 0| Opt Type = 4  |Opt Data Len=1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Tun Encap Lim |PadN Opt Type=1|Opt Data Len=1 |       0       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Next Header:

Identifies the type of the original packet header. For example, if the original packet is an IPv6 packet, the next header protocol value is set to decimal value 41 (Assigned payload type number for IPv6).

Hdr Ext Len:

Length of the Destination Options extension header in 8-octet units, not including the first 8 octets. Set to value 0, if no other options are present in this destination options header.

Option Type:

value 4 - see section 4.1.1.

Opt Data Len:

value 1 - see section 4.1.1.

Tun Encap Lim:

8 bit unsigned integer - see section 4.1.1.

Option Type:

value 1 - PadN option, to align the header following this header.

Opt Data Len:

value 1 - one octet of option data.

Option Data:

value 0 - one zero-valued octet.

Identifier: RQ_001_4040
RFC Clause: 6.1
Type: Recommendation
Applies to: Node

Requirement:
The validation of the IPv6 tunnel entry point node address at tunnel configuration time is recommended.

RFC Text:
The tunnel entry-point node address is one of the valid IPv6 unicast addresses of the entry-point node - the validation of the address at tunnel configuration time is recommended.

Identifier: RQ_001_4041
RFC Clause: 6.3
Type: Recommendation
Applies to: Node

Requirement:
The "single-hop" mechanism should be implemented by having the tunnel entry point node set a tunnel IPv6 header hop limit independently of the hop limit of the original header.

RFC Text:
The "single-hop" mechanism should be implemented by having the tunnel entry point node set a tunnel IPv6 header hop limit independently of the hop limit of the original header.

Identifier: RQ_001_4042
RFC Clause: 6.3
Type: Recommendation
Applies to: Node

Requirement:
It is recommended that the tunnel hop limit be configured with a value that ensures:

(a) that tunnel IPv6 packets can reach the tunnel exit-point node

(b) a quick expiration of the tunnel packet if a routing loop occurs within the IPv6 tunnel.

RFC Text:
It is recommended that the tunnel hop limit be configured with a value that ensures:

(a) that tunnel IPv6 packets can reach the tunnel exit-point node

(b) a quick expiration of the tunnel packet if a routing loop occurs within the IPv6 tunnel.

Identifier: RQ_001_4043
RFC Clause: 6.3
Type: Mandatory
Applies to: Host

Requirement:
The tunnel hop limit default value for hosts is the IPv6 Neighbor Discovery advertised hop limit [RFC 2461].

RFC Text:
The tunnel hop limit default value for hosts is the IPv6 Neighbor Discovery advertised hop limit [ND-Spec]. The tunnel hop limit default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).

Identifier: RQ_001_4044
RFC Clause: 6.3
Type: Mandatory
Applies to: Router

Requirement:
The tunnel hop limit default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).

RFC Text:
The tunnel hop limit default value for hosts is the IPv6 Neighbor Discovery advertised hop limit [ND-Spec]. **The tunnel hop limit default value for routers is the default IPv6 Hop Limit value from the Assigned Numbers RFC (64 at the time of writing this document).**

Identifier: RQ_001_4045
RFC Clause: 6.3
Type: Mandatory
Applies to: Node

Requirement:
The tunnel hop limit is copied into the hop limit field of the tunnel IPv6 header of each packet encapsulated by the tunnel entry-point node.

RFC Text:
The tunnel hop limit is copied into the hop limit field of the tunnel IPv6 header of each packet encapsulated by the tunnel entry-point node.

Identifier: RQ_001_4046
RFC Clause: 6.4
Type: Mandatory
Applies to: Node

Requirement:
The default value of the IPv6 Tunnel Packet Traffic Class field of a tunnel header is zero.

RFC Text:
The IPv6 Tunnel Packet Traffic Class indicates the value that a tunnel entry-point node sets in the Traffic Class field of a tunnel header. The default value is zero. The configured Packet Traffic Class can also indicate whether the value of the Traffic Class field in the tunnel header is copied from the original header, or it is set to the pre-configured value.

Identifier: RQ_001_4047
RFC Clause: 6.4
Type: Mandatory
Applies to: Node

Requirement:
The configured value of the IPv6 Tunnel Packet Traffic Class field of a tunnel header is either:
- copied from the original header, or
- is set to the pre-configured value.

RFC Text:
The IPv6 Tunnel Packet Traffic Class indicates the value that a tunnel entry-point node sets in the Traffic Class field of a tunnel header. The default value is zero. **The configured Packet Traffic Class can also indicate whether the value of the Traffic Class field in the tunnel header is copied from the original header, or it is set to the pre-configured value.**

Identifier: RQ_001_4048
RFC Clause: 6.5
Type: Mandatory
Applies to: Node

Requirement:
The default value of the IPv6 Tunnel Flow Label is zero.

RFC Text:
The IPv6 Tunnel Flow Label indicates the value that a tunnel entry-point node sets in the flow label of a tunnel header. The default value is zero.

Identifier: RQ_001_4049
RFC Clause: 6.6
Type: Recommendation
Applies to: Node

Requirement:
The recommended default value of the IPv6 Tunnel Encapsulation Limit is 4.

RFC Text:
The Tunnel Encapsulation Limit value can indicate whether the entry-point node is configured to limit the number of encapsulations of tunnel packets originating on that node. The IPv6 Tunnel Encapsulation Limit is the maximum number of additional encapsulations permitted for packets undergoing encapsulation at that entry-point node. **Recommended default value is 4.** An entry-point node configured to limit the number of nested encapsulations prepends a Destination Options extension header containing a Tunnel Encapsulation Limit option to an original packet undergoing encapsulation - see sections 4.1 and 4.1.1.

Identifier: RQ_001_4050
RFC Clause: 6.7
Type: Mandatory
Applies to: Node

Requirement:
The tunnel MTU is set to the Path MTU between the tunnel entry-point and the tunnel exit-point nodes, minus the size of the tunnel headers.

RFC Text:
The tunnel MTU is set dynamically to the Path MTU between the tunnel entry-point and the tunnel exit-point nodes, minus the size of the tunnel headers: the maximum size of a tunnel packet payload that can be sent through the tunnel without fragmentation [IPv6-Spec]. The tunnel entry-point node performs Path MTU discovery on the path between the tunnel entry-point and exit-point nodes [PMTU-Spec], [ICMP-Spec]. The tunnel MTU of a nested tunnel is the tunnel MTU of the outer tunnel minus the size of the nested tunnel headers.

Identifier: RQ_001_4051
RFC Clause: 7
Type: Mandatory
Applies to: Node

Requirement:
A tunnel entry-point node must support fragmentation of tunnel IPv6 packets.

RFC Text:

A tunnel IPv6 packet resulting from the encapsulation of an original packet is considered an IPv6 packet originating from the tunnel entry-point node. **Therefore, like any source of an IPv6 packet, a tunnel entry-point node must support fragmentation of tunnel IPv6 packets.**

Identifier: RQ_001_4052
RFC Clause: 7
Type: Mandatory
Applies to: Node

Requirement:
A tunnel intermediate node that forwards a tunnel packet to another node in the tunnel follows the general IPv6 rule that it must not fragment a packet undergoing forwarding.

RFC Text:
A tunnel intermediate node that forwards a tunnel packet to another node in the tunnel follows the general IPv6 rule that it must not fragment a packet undergoing forwarding.

Identifier: RQ_001_4053
RFC Clause: 7
Type: Mandatory
Applies to: Node

Requirement:
A tunnel exit-point node receiving tunnel packets at the end of the tunnel for decapsulation applies the strict left-to-right processing rules for extension headers.

RFC Text:
A tunnel exit-point node receiving tunnel packets at the end of the tunnel for decapsulation applies the strict left-to-right processing rules for extension headers. In the case of a fragmented tunnel packet, the fragments are reassembled into a complete tunnel packet before determining that an embedded packet is present.

Identifier: RQ_001_4054
RFC Clause: 7.1
Type: Mandatory
Applies to: Node

Requirement:
When an IPv6 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU and if the original IPv6 packet size is larger than the IPv6 minimum link MTU [RFC 2460], the entry-point node discards the packet.

RFC Text:
When an IPv6 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU (i.e., the Path MTU between the tunnel entry-point and the tunnel exit-point, minus the size of the tunnel header(s)), it is handled as follows:

(a) if the original IPv6 packet size is larger than the IPv6 minimum link MTU [IPv6-Spec], the entry-point node discards the packet and sends an ICMPv6 "Packet Too Big" message to the source address of the original packet with the recommended MTU size field set to the tunnel MTU or the IPv6 minimum link MTU, whichever is larger, i.e. max (tunnel MTU, IPv6 minimum link MTU). Also see sections 6.7 and 8.2.

(b) if the original IPv6 packet is equal or smaller than the IPv6 minimum link MTU, the tunnel entry-point node encapsulates the original packet, and subsequently fragments the resulting IPv6 tunnel packet into IPv6 fragments that do not exceed the Path MTU to the tunnel exit-point.

Identifier: RQ_001_4055
RFC Clause: 7.1
Type: Mandatory
Applies to: Node

Requirement:
When an IPv6 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU and if the original IPv6 packet size is larger than the IPv6 minimum link MTU [RFC 2460], the entry-point node sends an ICMPv6 "Packet Too Big" message to the source address of the original packet with the recommended MTU size field set to the tunnel MTU or the IPv6 minimum link MTU, whichever is larger, i.e. max(tunnel MTU, IPv6 minimum link MTU).

RFC Text:
When an IPv6 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU (i.e., the Path MTU between the tunnel entry-point and the tunnel exit-point, minus the size of the tunnel header(s)), it is handled as follows:

(a) if the original IPv6 packet size is larger than the IPv6 minimum link MTU [IPv6-Spec], the entry-point node discards the packet and **sends an ICMPv6 "Packet Too Big" message to the source address of the original packet with the recommended MTU size field set to the tunnel MTU or the IPv6 minimum link MTU, whichever is larger, i.e. max (tunnel MTU, IPv6 minimum link MTU). Also see sections 6.7 and 8.2.**

(b) if the original IPv6 packet is equal or smaller than the IPv6 minimum link MTU, the tunnel entry-point node encapsulates the original packet, and subsequently fragments the resulting IPv6 tunnel packet into IPv6 fragments that do not exceed the Path MTU to the tunnel exit-point.

Identifier: RQ_001_4056
RFC Clause: 7.1
Type: Mandatory
Applies to: Node

Requirement:
When an IPv6 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU and if the original IPv6 packet is equal or smaller than the IPv6 minimum link MTU, the tunnel entry-point node encapsulates the original packet, and sequently fragments the resulting IPv6 tunnel packet into IPv6 fragments that do not exceed the Path MTU to the tunnel exit-point.

RFC Text:
When an IPv6 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU (i.e., the Path MTU between the tunnel entry-point and the tunnel exit-point, minus the size of the tunnel header(s)), it is handled as follows:

(a) if the original IPv6 packet size is larger than the IPv6 minimum link MTU [IPv6-Spec], the entry-point node discards the packet and sends an ICMPv6 "Packet Too Big" message to the source address of the original packet with the recommended MTU size field set to the tunnel MTU or the IPv6 minimum link MTU, whichever is larger, i.e. max (tunnel MTU, IPv6 minimum link MTU). Also see sections 6.7 and 8.2.

(b) **if the original IPv6 packet is equal or smaller than the IPv6 minimum link MTU, the tunnel entry-point node encapsulates the original packet, and subsequently fragments the resulting IPv6 tunnel packet into IPv6 fragments that do not exceed the Path MTU to the tunnel exit-point.**

Identifier: RQ_001_4057
RFC Clause: 7.2
Type: Mandatory
Applies to: Node

Requirement:
When an IPv4 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU and if in the original IPv4 packet header the Don't Fragment - DF - bit flag is SET, the entry-point node discards the packet.

RFC Text:
When an IPv4 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU (i.e., the Path MTU between the tunnel entry-point and the tunnel exit-point, minus the size of the tunnel header(s)), it is handled as follows:

(a) if in the original IPv4 packet header the Don't Fragment - DF - bit flag is SET, the entry-point node discards the packet and returns an ICMP message. The ICMP message has the type = "unreachable", the code = "packet too big", and the recommended MTU size field set to the size of the tunnel MTU - see sections 6.7 and 8.3.

(b) if in the original packet header the Don't Fragment - DF - bit flag is CLEAR, the tunnel entry-point node encapsulates the original packet, and subsequently fragments the resulting IPv6 tunnel packet into IPv6 fragments that do not exceed the Path MTU to the tunnel exit-point.

Identifier: RQ_001_4058
RFC Clause: 7.2
Type: Mandatory
Applies to: Node

Requirement:
When an IPv4 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU and if in the original IPv4 packet header the Don't Fragment - DF - bit flag is SET, the entry-point node returns an ICMP message with the type = "unreachable", the code = "packet too big", and the recommended MTU size field set to the size of the tunnel MTU.

RFC Text:
When an IPv4 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU (i.e., the Path MTU between the tunnel entry-point and the tunnel exit-point, minus the size of the tunnel header(s)), it is handled as follows:

(a) if in the original IPv4 packet header the Don't Fragment - DF - bit flag is SET, the entry-point node discards the packet and **returns an ICMP message. The ICMP message has the type = "unreachable", the code = "packet too big", and the recommended MTU size field set to the size of the tunnel MTU** - see sections 6.7 and 8.3.

(b) if in the original packet header the Don't Fragment - DF - bit flag is CLEAR, the tunnel entry-point node encapsulates the original packet, and subsequently fragments the resulting IPv6 tunnel packet into IPv6 fragments that do not exceed the Path MTU to the tunnel exit-point.

Identifier: RQ_001_4059
RFC Clause: 7.2
Type: Mandatory
Applies to: Node

Requirement:
When an IPv4 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU and if in the original packet header the Don't Fragment - DF - bit flag is CLEAR, the tunnel entry-point node encapsulates the original packet, and subsequently fragments the resulting IPv6 tunnel packet into IPv6 fragments that do not exceed the Path MTU to the tunnel exit-point.

RFC Text:
When an IPv4 original packet enters a tunnel, if the original packet size exceeds the tunnel MTU (i.e., the Path MTU between the tunnel entry-point and the tunnel exit-point, minus the size of the tunnel header(s)), it is handled as follows:

(a) if in the original IPv4 packet header the Don't Fragment - DF - bit flag is SET, the entry-point node discards the packet and returns an ICMP message. The ICMP message has the type = "unreachable", the code = "packet too big", and the recommended MTU size field set to the size of the tunnel MTU - see sections 6.7 and 8.3.

(b) **if in the original packet header the Don't Fragment - DF - bit flag is CLEAR, the tunnel entry-point node encapsulates the original packet, and subsequently fragments the resulting IPv6 tunnel packet into IPv6 fragments that do not exceed the Path MTU to the tunnel exit-point.**

Identifier: RQ_001_4060
RFC Clause: 8
Type: Mandatory
Applies to: Node

Requirement:
An error detected by a node inside a tunnel SHALL result in a ICMP message, containing the original packet as its payload, being sent to the tunnel entry-point node.

RFC Text:
An error detected by a node inside a tunnel is reported to the source of the tunnel packet, that is, the tunnel entry-point node. The ICMP message sent to the tunnel entry-point node has as ICMP payload the tunnel IPv6 packet that has the original packet as its payload.

Identifier: RQ_001_4061
RFC Clause: 8
Type: Mandatory
Applies to: Node

Requirement:
In order to report a problem with the original packet to the source of an original packet, the tunnel entry point node MUST relay the ICMP message received from inside the tunnel to the source of that original IPv6 packet.

RFC Text:
To report a problem detected inside the tunnel to the source of an original packet, the tunnel entry point node must relay the ICMP message received from inside the tunnel to the source of that original IPv6 packet.

Identifier: RQ_001_4062
RFC Clause: 8.1
Type: Mandatory
Applies to: Node

Requirement:
The tunnel ICMP messages that are reported to the source of the original packet by the tunnel entry point are, "hop limit exceeded", "unreachable node", "parameter problem" and "packet too big".

RFC Text:

The tunnel ICMP messages that are reported to the source of the original packet are:

hop limit exceeded

The tunnel has a misconfigured hop limit, or contains a routing loop, and packets do not reach the tunnel exit-point node. This problem is reported to the tunnel entry-point node, where the tunnel hop limit can be reconfigured to a higher value. The problem is further reported to the source of the original packet as described in section 8.2, or 8.3.

unreachable node

One of the nodes in the tunnel is not or is no longer reachable. This problem is reported to the tunnel entry-point node, which should be reconfigured with a valid and active path between the entry and exit-point of the tunnel.

The problem is further reported to the source of the original packet as described in section 8.2, or 8.3.

parameter problem

A Parameter Problem ICMP message pointing to a valid Tunnel Encapsulation Limit Destination header with a Tun Encap Lim field value set to one is an indication that the tunnel

packet exceeded the maximum number of encapsulations allowed. The problem is further reported to the source of the original packet as described in section 8.2, or 8.3.

The above three problems detected inside the tunnel, which are a tunnel configuration and a tunnel topology problem, are reported to the source of the original IPv6 packet, as a tunnel generic "unreachable" problem caused by a "link problem" - see section 8.2 and 8.3.

packet too big

The tunnel packet exceeds the tunnel Path MTU.

The information carried by this type of ICMP message is used as follows:

- by a receiving tunnel entry-point node to set or adjust the tunnel MTU

- by a sending tunnel entry-point node to indicate to the source of an original packet the MTU size that should be used in sending IPv6 packets towards the tunnel entry-point node.

Identifier: RQ_001_4063
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:

In the IPv6 header of the ICMP message sent by the tunnel entry-point node to the source of the original IPv6 packet, the Source Address SHALL be a valid unicast IPv6 address of the outgoing interface.

RFC Text:

The tunnel entry-point node builds the ICMP and IPv6 headers of the ICMP message that is sent to the source of the original packet as follows:

IPv6 Fields:
Source Address
A valid unicast IPv6 address of the outgoing interface.

Destination Address
Copied from the Source Address field of the Original IPv6 header.

ICMP Fields:
For any of the following tunnel ICMP error messages:
"hop limit exceeded"
"unreachable node"
"parameter problem" - pointing to a valid Tunnel Encapsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 1 - unreachable node

Code 3 - address unreachable

For tunnel ICMP error message "packet too big":

Type 2 - packet too big

Code 0

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in 7.1, an ICMP "packet too big" message is sent to the source of the original packet only if the original packet size is larger than the minimum link MTU size required for IPv6 [IPv6-Spec].

Identifier: RQ_001_4064
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:

In the IPv6 header of the ICMP message sent by the tunnel entry-point node to the source of the original IPv6 packet, the Destination Address SHALL be copied from the Source Address field of the Original IPv6 header.

RFC Text:

The tunnel entry-point node builds the ICMP and IPv6 headers of the ICMP message that is sent to the source of the original packet as follows:

```
   IPv6 Fields:
   Source Address
                A valid unicast IPv6 address of the outgoing
                interface.

   Destination Address
                Copied from the Source Address field of the Original
                IPv6 header.

   ICMP Fields:
   For any of the following tunnel ICMP error messages:
     "hop limit exceeded"
     "unreachable node"
     "parameter problem" - pointing to a valid Tunnel Encapsulation
     Limit destination header with the Tun Encap Lim field set to a
     value zero:

     Type           1 - unreachable node

     Code           3 - address unreachable

   For tunnel ICMP error message "packet too big":

     Type           2 - packet too big

     Code           0

     MTU            The MTU field from the tunnel ICMP message minus
                    the length of the tunnel headers.

   According to the general rules described in 7.1, an ICMP "packet too
   big" message is sent to the source of the original packet only if the
   original packet size is larger than the minimum link MTU size
   required for IPv6 [IPv6-Spec].
```

Identifier: RQ_001_4065
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:

In the ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv6 packet, for "hop limit exceeded", "unreachable node" and "parameter problem" error messages, the Type shall be 1 - unreachable node.

RFC Text:

The tunnel entry-point node builds the ICMP and IPv6 headers of the ICMP message that is sent to the source of the original packet as follows:

```
   IPv6 Fields:
   Source Address
                 A valid unicast IPv6 address of the outgoing
                 interface.

   Destination Address
                 Copied from the Source Address field of the Original
                 IPv6 header.

   ICMP Fields:
   For any of the following tunnel ICMP error messages:
     "hop limit exceeded"
     "unreachable node"
     "parameter problem" - pointing to a valid Tunnel Encapsulation
     Limit destination header with the Tun Encap Lim field set to a
     value zero:

     Type           1 - unreachable node

     Code           3 - address unreachable

   For tunnel ICMP error message "packet too big":

     Type           2 - packet too big

     Code           0

     MTU            The MTU field from the tunnel ICMP message minus
                    the length of the tunnel headers.

   According to the general rules described in 7.1, an ICMP "packet too
   big" message is sent to the source of the original packet only if the
   original packet size is larger than the minimum link MTU size
   required for IPv6 [IPv6-Spec].
```

Identifier: RQ_001_4066
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:

In the ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv6 packet, for "hop limit exceeded", "unreachable node" and "parameter problem" error messages, the Code shall be 3 - address unreachable

RFC Text:

The tunnel entry-point node builds the ICMP and IPv6 headers of the ICMP message that is sent to the source of the original packet as follows:

IPv6 Fields:
Source Address
A valid unicast IPv6 address of the outgoing interface.

Destination Address
Copied from the Source Address field of the Original IPv6 header.

ICMP Fields:
For any of the following tunnel ICMP error messages:
"hop limit exceeded"
"unreachable node"
"parameter problem" - pointing to a valid Tunnel Encapsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 1 - unreachable node

Code 3 - address unreachable

For tunnel ICMP error message "packet too big":

Type 2 - packet too big

Code 0

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in 7.1, an ICMP "packet too big" message is sent to the source of the original packet only if the original packet size is larger than the minimum link MTU size required for IPv6 [IPv6-Spec].

Identifier: RQ_001_4067
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:
In the ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv6 packet, for "parameter problem" error messages, SHALL point to a valid Tunnel Encapsulation Limit destination header with the Tun Encap Lim field set to a value zero.

RFC Text:
The tunnel entry-point node builds the ICMP and IPv6 headers of the ICMP message that is sent to the source of the original packet as follows:

IPv6 Fields:
Source Address
A valid unicast IPv6 address of the outgoing interface.

Destination Address
Copied from the Source Address field of the Original IPv6 header.

ICMP Fields:
For any of the following tunnel ICMP error messages:
"hop limit exceeded"
"unreachable node"
"parameter problem" - pointing to a valid Tunnel Encapsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 1 - unreachable node

Code 3 - address unreachable

For tunnel ICMP error message "packet too big":

Type 2 - packet too big

Code 0

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in 7.1, an ICMP "packet too big" message is sent to the source of the original packet only if the original packet size is larger than the minimum link MTU size required for IPv6 [IPv6-Spec].

Identifier: RQ_001_4068
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:

In the ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv6 packet, for "packet too big": error messages, the Type Field SHALL be set to Type 2 - packet too big.

RFC Text:

The tunnel entry-point node builds the ICMP and IPv6 headers of the ICMP message that is sent to the source of the original packet as follows:

```
IPv6 Fields:
Source Address
              A valid unicast IPv6 address of the outgoing
              interface.

Destination Address
              Copied from the Source Address field of the Original
              IPv6 header.

ICMP Fields:
For any of the following tunnel ICMP error messages:
  "hop limit exceeded"
  "unreachable node"
  "parameter problem" - pointing to a valid Tunnel Encapsulation
  Limit destination header with the Tun Encap Lim field set to a
  value zero:


  Type          1 - unreachable node

  Code          3 - address unreachable
```

For tunnel ICMP error message "packet too big":

```
  Type          2 - packet too big

  Code          0

  MTU           The MTU field from the tunnel ICMP message minus
                the length of the tunnel headers.

According to the general rules described in 7.1, an ICMP "packet too
big" message is sent to the source of the original packet only if the
original packet size is larger than the minimum link MTU size
required for IPv6 [IPv6-Spec].
```

Identifier: RQ_001_4069
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:
In the ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv6 packet, for "packet too big": error messages, the Code Field SHALL be set to 0.

RFC Text:
The tunnel entry-point node builds the ICMP and IPv6 headers of the ICMP message that is sent to the source of the original packet as follows:

IPv6 Fields:
Source Address
A valid unicast IPv6 address of the outgoing interface.

Destination Address
Copied from the Source Address field of the Original IPv6 header.

ICMP Fields:
For any of the following tunnel ICMP error messages:
"hop limit exceeded"
"unreachable node"
"parameter problem" - pointing to a valid Tunnel Encapsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 1 - unreachable node

Code 3 - address unreachable

For tunnel ICMP error message "packet too big":

Type 2 - packet too big

Code 0

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in 7.1, an ICMP "packet too big" message is sent to the source of the original packet only if the original packet size is larger than the minimum link MTU size required for IPv6 [IPv6-Spec].

Identifier: RQ_001_4070
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:
In the ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv6 packet, for "packet too big": error messages, the MTU SHALL be set to the MTU field from the tunnel ICMP message minus the length of the tunnel headers.

RFC Text:
The tunnel entry-point node builds the ICMP and IPv6 headers of the ICMP message that is sent to the source of the original packet as follows:

IPv6 Fields:
Source Address
A valid unicast IPv6 address of the outgoing interface.

Destination Address
Copied from the Source Address field of the Original IPv6 header.

ICMP Fields:
For any of the following tunnel ICMP error messages:
"hop limit exceeded"
"unreachable node"
"parameter problem" - pointing to a valid Tunnel Encapsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 1 - unreachable node

Code 3 - address unreachable

For tunnel ICMP error message "packet too big":

Type 2 - packet too big

Code 0

MTU **The MTU field from the tunnel ICMP message minus the length of the tunnel headers**.

According to the general rules described in 7.1, an ICMP "packet too big" message is sent to the source of the original packet only if the original packet size is larger than the minimum link MTU size required for IPv6 [IPv6-Spec].

Identifier: RQ_001_4071
RFC Clause: 8.3
Type: Mandatory
Applies to: Node

Requirement:

In the IPv4 header of the ICMP message sent by the tunnel entry-point node to the source of the original IPv4 packet, the Source Address SHALL be a valid unicast IPv4 address of the outgoing interface.

RFC Text:

The tunnel entry-point node builds the ICMP and IPv4 header of the ICMP message that is sent to the source of the original packet as follows:

IPv4 Fields:
Source Address
A valid unicast IPv4 address of the outgoing interface.

Destination Address
Copied from the Source Address field of the Original IPv4 header.

ICMP Fields:

For any of the following tunnel ICMP error messages:

"hop limit exceeded"
"unreachable node"
"parameter problem" - pointing to a valid Tunnel Enacpsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 3 - destination unreachable

Code 1 - host unreachable

For a tunnel ICMP error message "packet too big":

Type 3 - destination unreachable

Code 4 - packet too big

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in section 7.2, an ICMP "packet too big" message is sent to the original IPv4 packet source node if the the original IPv4 header has the DF - don't fragment - bit flag SET.

Identifier: RQ_001_4072
RFC Clause: 8.3
Type: Mandatory
Applies to: Node

Requirement:
In the IPv4 header of the ICMP message sent by the tunnel entry-point node to the source of the original IPv4 packet, the Source Address SHALL be Copied from the Source Address field of the Original IPv4 header.

RFC Text:
The tunnel entry-point node builds the ICMP and IPv4 header of the ICMP message that is sent to the source of the original packet as follows:

IPv4 Fields:

Source Address

A valid unicast IPv4 address of the outgoing interface.

Destination Address

Copied from the Source Address field of the Original IPv4 header.

ICMP Fields:

For any of the following tunnel ICMP error messages:

"hop limit exceeded"

"unreachable node"

"parameter problem" - pointing to a valid Tunnel Enacpsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 3 - destination unreachable

Code 1 - host unreachable

For a tunnel ICMP error message "packet too big":

Type 3 - destination unreachable

Code 4 - packet too big

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in section 7.2, an ICMP "packet too big" message is sent to the original IPv4 packet source node if the the original IPv4 header has the DF - don't fragment - bit flag SET.

Identifier: RQ_001_4073
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:
The ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv4 packet, for "parameter problem" error messages, SHALL point to a valid Tunnel Encapsulation Limit destination header with the Tun Encap Lim field set to a value zero.

RFC Text:
The tunnel entry-point node builds the ICMP and IPv4 header of the ICMP message that is sent to the source of the original packet as follows:

IPv4 Fields:

Source Address

A valid unicast IPv4 address of the outgoing interface.

Destination Address

Copied from the Source Address field of the Original IPv4 header.

ICMP Fields:

For any of the following tunnel ICMP error messages:

"hop limit exceeded"

"unreachable node"

"parameter problem" - pointing to a valid Tunnel Enacpsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 3 - destination unreachable

Code 1 - host unreachable

For a tunnel ICMP error message "packet too big":

Type 3 - destination unreachable

Code 4 - packet too big

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in section 7.2, an ICMP "packet too big" message is sent to the original IPv4 packet source node if the the original IPv4 header has the DF - don't fragment - bit flag SET.

Identifier: RQ_001_4074
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:

The ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv4 packet, for "hop limit exceeded", "unreachable node" and "parameter problem" error messages, the Type shall be 3 - destination unreachable.

RFC Text:

The tunnel entry-point node builds the ICMP and IPv4 header of the ICMP message that is sent to the source of the original packet as follows:

IPv4 Fields:

Source Address

A valid unicast IPv4 address of the outgoing interface.

Destination Address

Copied from the Source Address field of the Original IPv4 header.

ICMP Fields:

For any of the following tunnel ICMP error messages:

"hop limit exceeded"

"unreachable node"

"parameter problem" - pointing to a valid Tunnel Enacpsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type **3 - destination unreachable**

Code 1 - host unreachable

For a tunnel ICMP error message "packet too big":

Type 3 - destination unreachable

Code 4 - packet too big

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in section 7.2, an ICMP "packet too big" message is sent to the original IPv4 packet source node if the the original IPv4 header has the DF - don't fragment - bit flag SET.

Identifier: RQ_001_4075
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:

The ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv4 packet, for "hop limit exceeded", "unreachable node" and "parameter problem" error messages, the Code shall be 1 - host unreachable.

RFC Text:

The tunnel entry-point node builds the ICMP and IPv4 header of the ICMP message that is sent to the source of the original packet as follows:

IPv4 Fields:

Source Address

A valid unicast IPv4 address of the outgoing interface.

Destination Address

Copied from the Source Address field of the Original IPv4 header.

ICMP Fields:

For any of the following tunnel ICMP error messages:

"hop limit exceeded"

"unreachable node"

"parameter problem" - pointing to a valid Tunnel Enacpsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 3 - destination unreachable

Code 1 - host unreachable

For a tunnel ICMP error message "packet too big":

Type 3 - destination unreachable

Code 4 - packet too big

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in section 7.2, an ICMP "packet too big" message is sent to the original IPv4 packet source node if the the original IPv4 header has the DF - don't fragment - bit flag SET.

Identifier: RQ_001_4076
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:
The ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv4 packet, for "packet too big": error messages, the Type Field SHALL be set to 3 - destination unreachable.

RFC Text:
The tunnel entry-point node builds the ICMP and IPv4 header of the ICMP message that is sent to the source of the original packet as follows:

IPv4 Fields:

Source Address

A valid unicast IPv4 address of the outgoing interface.

Destination Address

Copied from the Source Address field of the Original IPv4 header.

ICMP Fields:

For any of the following tunnel ICMP error messages:

"hop limit exceeded"

"unreachable node"

"parameter problem" - pointing to a valid Tunnel Enacpsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 3 - destination unreachable

Code 1 - host unreachable

For a tunnel ICMP error message "packet too big":

Type 3 - destination unreachable

Code 4 - packet too big

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in section 7.2, an ICMP "packet too big" message is sent to the original IPv4 packet source node if the the original IPv4 header has the DF - don't fragment - bit flag SET.

Identifier: RQ_001_4077
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:
The ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv4 packet, for "packet too big": error messages, the Code Field SHALL be set to 4 - packet too big.

RFC Text:
The tunnel entry-point node builds the ICMP and IPv4 header of the ICMP message that is sent to the source of the original packet as follows:

IPv4 Fields:

Source Address

A valid unicast IPv4 address of the outgoing interface.

Destination Address

Copied from the Source Address field of the Original IPv4 header.

ICMP Fields:

For any of the following tunnel ICMP error messages:

"hop limit exceeded"

"unreachable node"

"parameter problem" - pointing to a valid Tunnel Enacpsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 3 - destination unreachable

Code 1 - host unreachable

For a tunnel ICMP error message "packet too big":

Type 3 - destination unreachable

Code 4 - packet too big

MTU The MTU field from the tunnel ICMP message minus the length of the tunnel headers.

According to the general rules described in section 7.2, an ICMP "packet too big" message is sent to the original IPv4 packet source node if the the original IPv4 header has the DF - don't fragment - bit flag SET.

Identifier: RQ_001_4078
RFC Clause: 8.2
Type: Mandatory
Applies to: Node

Requirement:
The ICMP Fields of the ICMP message sent by the tunnel entry-point node to the source of the original IPv4 packet, for "packet too big": error messages, the MTU SHALL be set to the MTU field from the tunnel ICMP message minus the length of the tunnel headers.

RFC Text:
The tunnel entry-point node builds the ICMP and IPv4 header of the ICMP message that is sent to the source of the original packet as follows:

IPv4 Fields:

Source Address

A valid unicast IPv4 address of the outgoing interface.

Destination Address

Copied from the Source Address field of the Original IPv4 header.

ICMP Fields:

For any of the following tunnel ICMP error messages:

"hop limit exceeded"

"unreachable node"

"parameter problem" - pointing to a valid Tunnel Enacpsulation Limit destination header with the Tun Encap Lim field set to a value zero:

Type 3 - destination unreachable

Code 1 - host unreachable

For a tunnel ICMP error message "packet too big":

Type 3 - destination unreachable

Code 4 - packet too big

MTU **The MTU field from the tunnel ICMP message minus the length of the tunnel headers.**

According to the general rules described in section 7.2, an ICMP "packet too big" message is sent to the original IPv4 packet source node if the the original IPv4 header has the DF - don't fragment - bit flag SET.

Annex A (informative): Bibliography

IETF RFC2373: "IP Version 6 Addressing Architecture".

IETF RFC2401: "Security Architecture for the Internet Protocol".

IETF RFC2402: "IP Authentication Header".

IETF RFC2406: "IP Encapsulating Security Payload (ESP)".

IETF RFC2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

IETF RFC2460: "Internet Protocol, Version 6 (IPv6) Specification".

IETF RFC2461: "Neighbor Discovery for IP Version 6 (IPv6)".

IETF RFC2462: "IPv6 Stateless Address Autoconfiguration".

IETF RFC2463: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification".

IETF RFC3041: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

History

Document history		
V1.1.1	December 2006	Publication