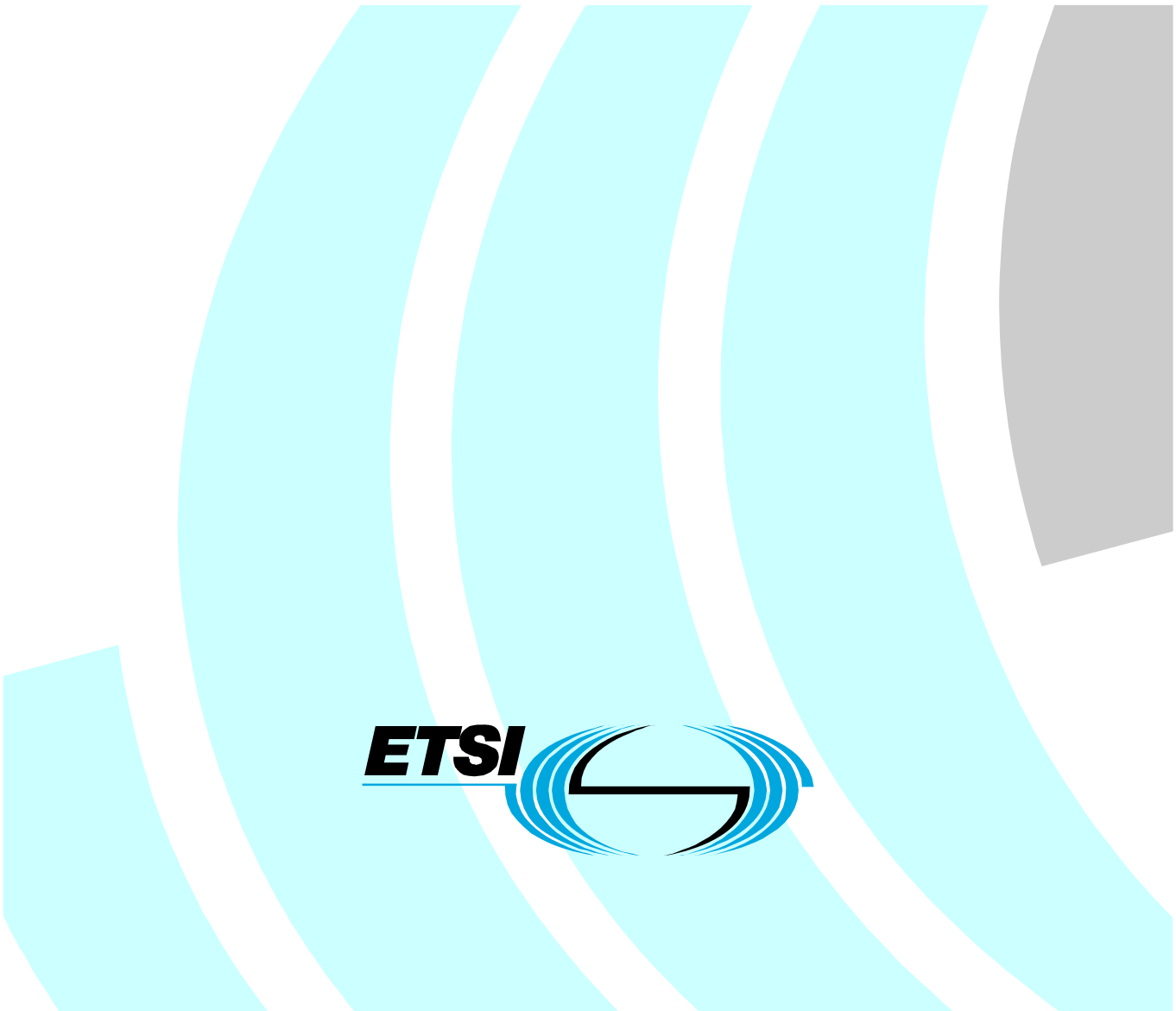
ETSI TS 102 514 V2.1.1 (2008-02)

Technical Specification

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



Reference
RTS/MTS-IPT-003[2]-IPv6-CrRqCa

Keywords
IP, IPv6, 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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2008.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™, **TIPHON**™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights 4
Foreword 4
1 Scope 5
2 References 5
2.1 Normative references 5
3 Abbreviations 6
4 Requirements Catalogue 6
4.1 Requirements extracted from TS 123 060 6
4.2 Requirements extracted from TS 123 221 8
4.3 Requirements extracted from TS 129 061 8
4.4 Requirements extracted from RFC 1981 25
4.5 Requirements extracted from RFC 2460 29
4.6 Requirements extracted from RFC 2461 72
4.7 Requirements extracted from RFC 2462 261
4.8 Requirements extracted from RFC 2463 283
4.9 Requirements extracted from RFC 2464 314
4.10 Requirements extracted from RFC 2675 318
4.11 Requirements extracted from RFC 3513 326
Annex A (informative): Duplicated requirements 355
Annex B (informative): Bibliography 357
History 358

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 purpose of the present document is to provide a catalogue of requirements extracted from the core IPv6 RFCs (see references in clause 2) and from ETSI Specifications. The catalogue follows the guidelines defined by the MTS IPv6 Testing: Methodology and Framework (see TS 102 351 in bibliography).

2 References

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.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".

[2] IETF RFC 1981: "Path MTU Discovery for IP version 6".

[3] IETF RFC 2373: "IP Version 6 Addressing Architecture".

[4] IETF RFC 2402: "IP Authentication Header".

[5] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[6] IETF RFC 2461: "Neighbor Discovery for IP Version 6 (IPv6)".

[7] IETF RFC 2462: "IPv6 Stateless Address Autoconfiguration".

[8] IETF RFC 2463: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification".

[9] IETF RFC 2464: "Transmission of IPv6 Packets over Ethernet Networks".

[10] IETF RFC 2675: "IPv6 Jumbograms".

[11] IETF RFC 3513: "Internet Protocol Version 6 (IPv6) Addressing Architecture".

[12] ETSI TS 123 060: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description; Stage 2 (3GPP TS 23.060)".

[13] ETSI TS 123 221: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Architectural requirements (3GPP TS 23.221)".

[14] ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228)".

[15] ETSI TS 129 061: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) (3GPP TS 29.061)".

3 Abbreviations

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

ICMP	Internet Control Message Protocol
IE	Information Element
MTU	Maximum Transmission Unit
ND	Neighbor Discovery
PDP	Packet Data Protocol
PMTU	Path MTU
TCP	Transfer Control Protocol
UDP	User Datagram Protocol

4 Requirements Catalogue

The requirements below have been extracted from IETF RFCs 1981 [2], 2460 [5], 2461 [6], 2462 [7], 2463 [8], 2464 [9], 2675 [10], 3513[11]) and ETSI specifications TS 123 060 [12], TS 123 221 [13], TS 123 228 [14], TS 129 061 [15]).

4.1 Requirements extracted from TS 123 060

RQ_000_7003 Configure Address
TS 123 060 9.2.1.1 MANDATORY
Applies to: Host
Context:
An IPv6 Mobile Station is performing either stateless or stateful address autoconfiguration
Requirement:
An IPv6 Mobile Station SHALL use the interface identifier provided by the Gateway GPRS Support Node to configure its link-local address
Specification Text:
To ensure that the link-local address generated by the MS does not collide with the link-local address of the GGSN, the GGSN shall provide an interface identifier (see RFC 2462 [69]) to the MS and the MS shall use this interface identifier to configure its link-local address. This is applicable for both stateful and stateless IPv6 address autoconfiguration. In case of stateless address autoconfiguration however, the MS can choose any interface identifier to generate addresses other than link-local, without involving the network. In particular, the SGSN and the GGSN are not updated with the actual address used by the MS, as the prefix alone identifies the PDP context.

RQ_000_7004 Detect Duplicate Address (DAD)
TS 123 060 9.2.1.1 OPTIONAL
Applies to: Host
Context:
An IPv6 Mobile Station is performing stateless address autoconfiguration using a prefix advertised by a Gateway BPRS Support Node in a PDP context.
Requirement:
The IPv6 Mobile Station MAY omit duplicate address detection.
Specification Text:
Because any prefix that the GGSN advertises in a PDP context is unique within the scope of the prefix (i.e. site-local or global), there is no need for the MS to perform Duplicate Address Detection for this IPv6 address. Therefore, the GGSN shall silently discard Neighbor Solicitation messages that the MS may send to perform Duplicate Address Detection. It is possible for the MS to perform Neighbor Unreachability Detection towards the GGSN, as defined in RFC 2461[71]; therefore if the GGSN receives a Neighbor Solicitation as part of this procedure, the GGSN shall provide a Neighbor Advertisement as described in RFC 2461.

RQ_000_7005 Detect Duplicate Address (DAD)
TS 123 060 9.2.1.1 MANDATORY
Applies to: Router
Context:
An IPv6 Mobile Station is performing stateless address autoconfiguration using a prefix advertised by a Gateway BPRS Support Node in a PDP context.
Requirement:
The IPv6 Gateway GPRS Support NODE SHALL silently discard any Neighbor Solicitation messages sent by the IPv6 Mobile Station.
Specification Text:
Because any prefix that the GGSN advertises in a PDP context is unique within the scope of the prefix (i.e. site-local or global), there is no need for the MS to perform Duplicate Address Detection for this IPv6 address. Therefore, the GGSN shall **silently discard Neighbor Solicitation messages that the MS may send to perform Duplicate Address Detection.** .

RQ_000_7006 Stateless Autoconfiguration
TS 123 060 9.2.1.1 MANDATORY
Applies to: Router
Context:
An IPv6 Mobile Station has sent an "Activate PDP Context Request" to its Serving GPRS Support Node
Requirement:
The IPv6 Gateway GPRS Support Node SHALL NOT advertise the same prefix on more than one PDP context on a given APN or set of APNs, within the same addressing scope.
Specification Text:
The GGSN sends a Router Advertisement message. The Router Advertisement messages shall contain the same prefix as the one provided in step 2. **A given prefix shall not be advertised on more than one PDP context on a given APN, or set of APNs, within the same addressing scope.** The GGSN shall be configured to advertise only one prefix per PDP context

After the MS has received the Router Advertisement message, it constructs its full IPv6 address by concatenating the interface identifier received in step 3, or a locally generated interface identifier, and the prefix received in the Router Advertisement. **If the Router Advertisement contains more than one prefix option, the MS shall only consider the first one and silently discard the others**.

RQ_000_7007 Stateless Autoconfiguration
TS 123 060 9.2.1.1 MANDATORY
Applies to: Host
Context:
An IPv6 Mobile Station receives a Router Advertisement message which contains more than one prefix.
Requirement:
The IPv6 Mobile Station SHALL use the first prefix and silently discard the others.
Specification Text:
The GGSN sends a Router Advertisement message. The Router Advertisement messages shall contain the same prefix as the one provided in step 2. **A given prefix shall not be advertised on more than one PDP context on a given APN, or set of APNs, within the same addressing scope.** The GGSN shall be configured to advertise only one prefix per PDP context

After the MS has received the Router Advertisement message, it constructs its full IPv6 address by concatenating the interface identifier received in step 3, or a locally generated interface identifier, and the prefix received in the Router Advertisement. **If the Router Advertisement contains more than one prefix option, the MS shall only consider the first one and silently discard the others**.

RQ_000_7009 Startup Router Advertisement Behavior
TS 123 060 9.2.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 Gateway GPRS Support Node shall automatically and periodically send Router Advertisement messages towards the Mobile Station after a PDP context of type IPv6 is activated
Specification Text:
IPv6 stateful address autoconfiguration uses the standard External PDN Address Allocation procedure, as described in TS 29.061. The GGSN informs the MS that it shall perform stateful address autoconfiguration by means of the Router Advertisements, as defined in RFC 2461. For this purpose, **the GGSN shall automatically and periodically send Router Advertisement messages towards the MS after a PDP context of type IPv6 is activated.** The use of stateless or stateful address autoconfiguration is configured per APN.

4.2 Requirements extracted from TS 123 221

RQ_000_7010 3GPP UE supports IPv6
TS 123 221 5.6 MANDATORY
Applies to: Host
Context:

Requirement:
A 3GPP User Equipment supporting IPv6 SHALL comply with the Basic IP group of specifications as defined in RFC3316.
Specification Text:
The set of IPv6 functionality a 3GPP UE will require is dependent on the services (IMS, Packet Streaming etc.) it will use.

As a minimum, a 3GPP UE shall comply with the Basic IP group of specifications as defined in RFC3316. This IPv6 functionality is sufficient to provide compatibility towards IPv6 entities external to 3GPP.

A 3GPP UE shall follow the recommendations for the IP Security set of functions in RFC3316 when a specific service requires such functions.

According to the procedures defined in TS 23.060, when a UE is assigned an IPv6 prefix, it can change the global IPv6 address it is currently using via the mechanism defined in RFC 3041, or similar means, without updating the PS domain. Any application that requires full IP address knowledge shall provide a mechanism to get the latest IPv6 address when the IPv6 address in the UE has been changed. An example of such means is defined in TS 23.228.

Note: RFC3316 does not make any recommendations on preferred transition and interoperability mechanisms between IPv4 and IPv6.

4.3 Requirements extracted from TS 129 061

RQ_000_7000 Configure Address
TS 129 061 11.2.1.3 MANDATORY
Applies to: Host
Context:
An IPv6 Mobile Station which is capable of both stateless and stateful autoconfiguration.
Requirement:
The IPv6 Mobile Station SHALL use stateless autoconfiguration to configure the address and stateful autoconfiguration to configure additional parameters only.
Specification Text:
Stateful and Stateless Autoconfiguration may also co-exist. In that case, the MS shall use Stateless to configure the address and Stateful to configure additional parameters only. The MS shall not use Stateless and Stateful Address Autoconfiguration simultaneously since GPRS only supports one prefix per PDP.

RQ_000_7001 Configure Address
TS 129 061 11.2.1.3 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 Mobile Station SHALL NOT use both stateless and stateful autoconfiguration simultaneously.
Specification Text:
Stateful and Stateless Autoconfiguration may also co-exist. In that case, the MS shall use Stateless to configure the address and Stateful to configure additional parameters only. **The MS shall not use Stateless and Stateful Address Autoconfiguration simultaneously since GPRS only supports one prefix per PDP Context**

RQ_000_7002 Configure Address
TS 129 061 11.2.1.3 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 Mobile Station SHALL support stateless address autoconfiguration.
Specification Text:
For MS, IPv6 Stateless Address Autoconfiguration is mandatory, and IPv6 Stateful Address Autoconfiguration is optional.

RQ_000_7008 Startup Router Advertisement Behavior
TS 129 061 11.2.1.3.2 OPTIONAL
Applies to: Router
Context:

Requirement:
AN IPv6 Gateway GPRS Support Node MAY omit the randomisation of the period between sending Router Advertisements.
Specification Text:
The handling of Router Advertisements shall be consistent with what is specified in RFC 2461 [44]. For the MS-GGSN link however, some specific handling shall apply. **The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link.** Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

RQ_000_7011 Configure Address
TS 129 061 11.2.1.3 OPTIONAL
Applies to: Host
Context:

Requirement:
An IPv6 Mobile Station MAY support stateful address autoconfiguration.
Specification Text:
For MS, IPv6 Stateless Address Autoconfiguration is mandatory, and **IPv6 Stateful Address Autoconfiguration is optional**.

RQ_000_7012 MaxRtrAdvInterval
TS 129 061 11.2.1.3.4 MANDATORY
Applies to: Router
Context:

Requirement:
The default value of the configurable timer, MaxRtrAdvInterval in a 3GPP IPv6 router shall be 21,600s (6 hours).

Specification Text:
For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 and RFC 2461), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. **The values specified hereafter are specific to GPRS and supersede those specified in RFC 2461.**

MaxRtrAdvInterval

Shall have a default value of 21 600 s (6 h).

MinRtrAdvInterval

Shall have a default value of 0,75 × MaxRtrAdvInterval i.e.16 200 s (4,5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 s.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

RQ_000_7013 MinRtrAdvInterval
TS 129 061 11.2.1.3.4 MANDATORY
Applies to: Router
Context:

Requirement:
The default value of the configurable timer, MinRtrAdvInterval in a 3GPP IPv6 router SHALL be 0.75 x MaxRtrAdvInterval (4,5 hours).

Specification Text:
For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 and RFC 2461), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. **The values specified hereafter are specific to GPRS and supersede those specified in RFC 2461.**

MaxRtrAdvInterval

Shall have a default value of 21 600 s (6 h).

MinRtrAdvInterval

Shall have a default value of 0,75 × MaxRtrAdvInterval i.e.16 200 s (4,5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 s.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

RQ_000_7014 RA Prefix Option
TS 129 061 11.2.1.3.4 MANDATORY
Applies to: Router
Context:

Requirement:
The default value of the configurable timer, AdvValidLifetime in a 3GPP IPv6 router SHALL be 0xFFFFFFFFH

Specification Text:
For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 and RFC 2461), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. **The values specified hereafter are specific to GPRS and supersede those specified in RFC 2461.**

MaxRtrAdvInterval

Shall have a default value of 21 600 s (6 h).

MinRtrAdvInterval

Shall have a default value of 0,75 × MaxRtrAdvInterval i.e.16 200 s (4,5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 s.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

RQ_000_7015 RA Prefix Option
TS 129 061 11.2.1.3.4 MANDATORY
Applies to: Router
Context:

Requirement:
The default value of the configurable timer, AdvPreferredLifetime in a 3GPP IPv6 router SHALL be 0xFFFFFFFFH

Specification Text:
For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 and RFC 2461), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. **The values specified hereafter are specific to GPRS and supersede those specified in RFC 2461.**

MaxRtrAdvInterval

Shall have a default value of 21 600 s (6 h).

MinRtrAdvInterval

Shall have a default value of 0,75 × MaxRtrAdvInterval i.e.16 200 s (4,5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 s.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

RQ_000_7016 ND Protocol Constants and Default Values
TS 129 061 11.2.1.3.4 OPTIONAL
Applies to: Router
Context:

Requirement:
The IPv6 router "constant" MAX_INITIAL_RTR_ADVERT_INTERVAL MAY be treated as a variable in a 3GPP router.

Specification Text:
For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 and RFC 2461), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. The values specified hereafter are specific to GPRS and supersede those specified in RFC 2461.

MaxRtrAdvInterval

Shall have a default value of 21 600 s (6 h).

MinRtrAdvInterval

Shall have a default value of 0,75 × MaxRtrAdvInterval i.e.16 200 s (4,5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 s.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

RQ_000_7017 ND Protocol Constants and Default Values
TS 129 061 11.2.1.3.4 MANDATORY
Applies to: Router
Context:

Requirement:
The MAX_INITIAL_RTR_ADVERTISEMENTS SHALL be configured to have a value such that it does not overload the radio interface while still allowing the Mobile Station to complete its configuration in a reasonable delay.

Specification Text:
For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 and RFC 2461), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. The values specified hereafter are specific to GPRS and supersede those specified in RFC 2461.

MaxRtrAdvInterval

Shall have a default value of 21 600 s (6 h).

MinRtrAdvInterval

Shall have a default value of 0,75 × MaxRtrAdvInterval i.e.16 200 s (4,5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF.
The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 s.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

RQ_000_7019 Configure Address
TS 129 061 11.2.1.3.1 MANDATORY
Applies to: Router
Context:

Requirement:
As part of the IPv6 PDP Context Activation, an IPv6 Gateway GPRS Support Node SHALL provide a dynamic IPv6 address to a Mobile Station using either stateless or stateful address autoconfiguration.
Specification Text:
The GGSN provides the MS with an IPv6 Prefix belonging to the Intranet/ISP addressing space. **A dynamic IPv6 address shall be given using either stateless or stateful address autoconfiguration.** This IPv6 address is used for packet forwarding within the packet domain and for packet forwarding on the Intranet/ISP

RQ_000_7021 Configure Address
TS 129 061 11.2.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 Mobile Station SHALL use either stateless or stateful address autoconfiguration to assign an IPv6 address to itself.
Specification Text:
The MS is given an address or IPv6 Prefix belonging to the operator addressing space. The address or IPv6 Prefix is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address or IPv6 Prefix is used for packet forwarding between the Internet and the GGSN and within the packet domain. **With IPv6, either Stateless or Stateful Address Autoconfiguration shall be used to assign an IPv6 address to the MS.** These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space. The use of stateful or stateless is configured per APN.

RQ_000_7022 Neighbor Discovery
TS 129 061 11.2.1.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 Gateway GPRS Support Node SHALL comply with the principles of RFC 2461 for sending Router Advertisements.
Specification Text:
The selection between Stateful and Stateless Autoconfiguration is dictated by **the Router Advertisements sent by the GGSN as described in the corresponding subclauses below and according to the principles defined in RFC 2461** and RFC 2462.

RQ_000_7023 Stateless Autoconfiguration
TS 129 061 11.2.1.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 Gateway GPRS Support Node SHALL comply with the principles of RFC 2462 for stateless address autoconfiguration.
Specification Text:
The selection between Stateful and Stateless Autoconfiguration is dictated by **the Router Advertisements sent by the GGSN as described in the corresponding subclauses below and according to the principles defined in RFC 2461 and RFC 2462.**

RQ_000_7024 Form Link-local Address
TS 129 061 11.2.1.3.1 MANDATORY
Applies to: Host
Context:
An IPv6 Mobile Terminal receives an Interface Identifier during IPv6 PDP context Activation.
Requirement:
The Mobile Terminal SHALL use the received Interface Identifier to create a link-local address for IPv6 address autoconfiguration.
Specification Text:
...The MT finalises the IPV6CP negotiation by sending an IPV6CP Configure-Ack message to the TE with the appropriate options included, e.g. Interface-Identifier. **The Interface-Identifier shall be used in the TE to create a link-local address to be able to perform the IPv6 address autoconfiguration**

RQ_000_7030 Stateless Autoconfiguration
TS 129 061 11.2.1.3.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 Mobile Station has completed PDP context activation and has started stateless address autoconfiguration.
Requirement:
The IPv6 Mobile Station SHALL use the interface identifier provided by the Gateway GPRS Support Node to configure its link-local address.
Specification Text:
After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface-Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373.

Before the MS can communicate with other hosts or MSes on the Intranet/ISP, the MS must obtain an IPv6 Global or Site-Local Unicast Address. The simplest way is the IPv6 Stateless Address Autoconfiguration procedure described below and in 3GPP TS 23.060 [3]. The procedure is consistent with RFC 2462.

The procedure below takes place through signalling in the user plane. It is done on the link between the MS and the GGSN. From the MS perspective the GGSN is now the first router on the link.

RQ_000_7031 Stateless Autoconfiguration
TS 129 061 11.2.1.3.2 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 Mobile Station has completed PDP context activation and has started stateless address autoconfiguration.
Requirement:
The IPv6 Mobile Station SHOULD use IPv6 Stateless Address Autoconfiguration to obtain an IPv6 Global or Site-Local Unicast address.
Specification Text:
After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface-Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373.

Before the MS can communicate with other hosts or MSes on the Intranet/ISP, the MS must obtain an IPv6 Global or Site-Local Unicast Address. The simplest way is the IPv6 Stateless Address Autoconfiguration procedure described below and in 3GPP TS 23.060 [3]. The procedure is consistent with RFC 2462.

The procedure below takes place through signalling in the user plane. It is done on the link between the MS and the GGSN. From the MS perspective the GGSN is now the first router on the link.

RQ_000_7032 Startup Router Advertisement Behavior
TS 129 061 11.2.1.3.2 MANDATORY
Applies to: Router
Context:
An IPv6 Gateway GPRS Support Node has sent a Create PDP Context Response message to complete the PDP context activation procedure.
Requirement:
The IPv6 Gateway GPRS Support Node shall send Router Advertisements periodically on the new link to the Mobile Station established by the PDP Context.
Specification Text:
After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.

To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M flag cleared in the Router Advertisement messages. An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS. The O-flag may be set though, since it does not result in additional addresses being acquired (see below).

The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

The handling of Router Advertisements shall be consistent with what is specified in RFC 2461. For the MS-GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

RQ_000_7033 Stateless Autoconfiguration
TS 129 061 11.2.1.3.2 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 Gateway GPRS Support Node SHALL send Router Advertisements with the M-flag cleared to zero if it needs to indicate to any Mobile Station that stateless address autoconfiguration shall be performed.
Specification Text:
After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.

To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M flag cleared in the Router Advertisement messages. An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS. The O-flag may be set though, since it does not result in additional addresses being acquired (see below).

The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

The handling of Router Advertisements shall be consistent with what is specified in RFC 2461. For the MS-GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

RQ_000_7034 Simultaneous Stateless and Stateful Autoconfiguration
TS 129 061 11.2.1.3.2 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 Mobile Station SHALL NOT perform stateless and stateful address autoconfiguration simultaneously.
Specification Text:
After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.

To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M flag cleared in the Router Advertisement messages. **An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS.** The O-flag may be set though, since it does not result in additional addresses being acquired (see below).

The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

The handling of Router Advertisements shall be consistent with what is specified in RFC 2461. For the MS-GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

RQ_000_7035 Use of O-Flag
TS 129 061 11.2.1.3.2 MANDATORY
Applies to: Host
Context:
An IPv6 Mobile Station receives a Router advertisement message with M-flag cleared to zero and the O-flag set to one.
Requirement:
The IPv6 Mobile Station SHALL only perform stateless autoconfiguration for one IPv6 address.
Specification Text:
After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.

To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M flag cleared in the Router Advertisement messages. An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS. **The O-flag may be set though, since it does not result in additional addresses being acquired** (see below).

The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

The handling of Router Advertisements shall be consistent with what is specified in RFC 2461. For the MS-GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

RQ_000_7036 Stateful Autoconfiguration

TS 129 061 11.2.1.3.3 MANDATORY

Applies to: Router

Context:

Implementation (GGSN) is generating a Router Advertisement message for Stateful address autoconfiguration

Requirement:

An IPv6 Gateway GPRS Support Node SHALL send Router Advertisements without any Prefix-Information option and with the M-flag set to one if it needs to indicate to any Mobile Station that stateful address autoconfiguration shall be performed.

Specification Text:

After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately. This shall be consistent with what is specified in RFC 2461. For the MS-GGSN link however, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN").

To indicate to the MS that Stateful Address Autoconfiguration shall be performed, the Router Advertisements shall not contain any Prefix-Information option and the M-flag ("Managed Address Configuration Flag") shall be set.

RQ_000_7038 RA Prefix Option

TS 129 061 11.2.1.3.1 MANDATORY

Applies to: Router

Context:

Requirement:

An IPv6 Gateway GPRS Support Node's internal IPv6 prefix pool SHALL be configurable and structured per Access Point Name.

Specification Text:

IPv6 Prefixes in a GGSN internal Prefix pool shall be configurable and structured per APN.

RQ_000_7042 Stateless Autoconfiguration

TS 129 061 11.2.1.3.2 MANDATORY

Applies to: Router

Context:

An IPv6 Gateway GPRS Support Node receives a valid Router Solicitation.

Requirement:

The IPv6 Gateway GPRS Support Node SHALL send a Router Advertisement to the source of the Router Solicitation immediately with the Prefix field in the Prefix Information Option set to the same single Prefix as the one previously sent in the Create PDP Context Response, the A-Flag set to one (1), the L-Flag set to zero (0) and the Prefix Lifetime set to infinity.

Specification Text:

After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. **The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.**

To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M flag cleared in the Router Advertisement messages. An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS. The O-flag may be set though, since it does not result in additional addresses being acquired (see below).

The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

The handling of Router Advertisements shall be consistent with what is specified in RFC 2461. For the MS-GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

RQ_000_7047 Startup Router Advertisement Behavior

TS 129 061 11.2.1.3.2 MANDATORY

Applies to: Router

Context:

Requirement:

The handling of Router Advertisements by an IPv6 Gateway GPRS Support Node SHALL be consistent with the procedures specified in IETF RFC 2461

Specification Text:

After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.

To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M flag cleared in the Router Advertisement messages. An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS. The O-flag may be set though, since it does not result in additional addresses being acquired (see below).

The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

The handling of Router Advertisements shall be consistent with what is specified in RFC 2461. For the MS-GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

RQ_000_7048 Unicast Address

TS 129 061 11.2.1.3.2 OPTIONAL

Applies to: Host

Context:

Requirement:

When creating a global or site-local unicast address, an IPv6 Mobile Station MAY use the Interface Identifier received during the IPv6 PDP Context Activation phase

Specification Text:

When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the value of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix is unique. Interface-Identifiers shall in any case be 64-bit long.

Since the GGSN guarantees that the Prefix is unique, the MS does not need to perform any Duplicate Address Detection on addresses it creates. That is, the 'DupAddrDetectTransmits' variable in the MS should have a value of zero. If the MS finds more than one Prefix in the Router Advertisement message, it shall only consider the first one and silently discard the others. The GGSN shall not generate any globally unique IPv6 addresses for itself using the Prefix assigned to the MS in the Router Advertisement.

If the O-flag ("Other stateful configuration flag") was set in the Router Advertisement, the MS may start a DHCP session to retrieve additional configuration parameters. See subclause 13.2.2 "Other configuration by the Intranet or ISP". If the MS is not DHCP capable, the O-flag may be ignored.

RQ_000_7050 Unicast Address
TS 129 061 11.2.1.3.2 MANDATORY
Applies to: Host
Context:

Requirement:
When creating a Global or Site-Local Unicast address, an IPv6 Mobile Station SHALL use an Interface-Identifier that is 64-bits long.
Specification Text:
When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the value of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix is unique. **Interface-Identifiers shall in any case be 64-bit long**.

Since the GGSN guarantees that the Prefix is unique, the MS does not need to perform any Duplicate Address Detection on addresses it creates. That is, the 'DupAddrDetectTransmits' variable in the MS should have a value of zero. If the MS finds more than one Prefix in the Router Advertisement message, it shall only consider the first one and silently discard the others. The GGSN shall not generate any globally unique IPv6 addresses for itself using the Prefix assigned to the MS in the Router Advertisement.

If the O-flag ("Other stateful configuration flag") was set in the Router Advertisement, the MS may start a DHCP session to retrieve additional configuration parameters. See subclause 13.2.2 "Other configuration by the Intranet or ISP". If the MS is not DHCP capable, the O-flag may be ignored.

RQ_000_7051 Detect Duplicate Address (DAD)
TS 129 061 11.2.1.3.2 RECOMMENDED
Applies to: Host
Context:

Requirement:
An IPv6 Mobile Station does not need to perform any Duplicate Address Detection on addresses it creates.
Specification Text:
When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the value of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix is unique. Interface-Identifiers shall in any case be 64-bit long.

Since the GGSN guarantees that the Prefix is unique, the MS does not need to perform any Duplicate Address Detection on addresses it creates. That is, the 'DupAddrDetectTransmits' variable in the MS should have a value of zero. If the MS finds more than one Prefix in the Router Advertisement message, it shall only consider the first one and silently discard the others. The GGSN shall not generate any globally unique IPv6 addresses for itself using the Prefix assigned to the MS in the Router Advertisement.

If the O-flag ("Other stateful configuration flag") was set in the Router Advertisement, the MS may start a DHCP session to retrieve additional configuration parameters. See subclause 13.2.2 "Other configuration by the Intranet or ISP". If the MS is not DHCP capable, the O-flag may be ignored.

RQ_000_7053 Configure Address
TS 129 061 11.2.1.3.2 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 Gateway GPRS Support Node SHALL NOT generate any globally unique IPv6 addresses for itself using a Prefix assigned to any MS in Router Advertisement messages.
Specification Text:
When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the value of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix is unique. Interface-Identifiers shall in any case be 64-bit long.

Since the GGSN guarantees that the Prefix is unique, the MS does not need to perform any Duplicate Address Detection on addresses it creates. That is, the 'DupAddrDetectTransmits' variable in the MS should have a value of zero. If the MS finds more than one Prefix in the Router Advertisement message, it shall only consider the first one and silently discard the others. **The GGSN shall not generate any globally unique IPv6 addresses for itself using the Prefix assigned to the MS in the Router Advertisement.**

If the O-flag ("Other stateful configuration flag") was set in the Router Advertisement, the MS may start a DHCP session to retrieve additional configuration parameters. See subclause 13.2.2 "Other configuration by the Intranet or ISP". If the MS is not DHCP capable, the O-flag may be ignored.

RQ_000_7054 Use of O-Flag
TS 129 061 11.2.1.3.2 OPTIONAL
Applies to: Host
Context:
An IPv6 Mobile Station receives a Router Advertisement in which the O-flag ("Other stateful configuration flag") is set to one (1).
Requirement:
The IPv6 Mobile Station MAY start a DHCP session to retrieve additional configuration parameters.
Specification Text:
When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the value of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix is unique. Interface-Identifiers shall in any case be 64-bit long.

Since the GGSN guarantees that the Prefix is unique, the MS does not need to perform any Duplicate Address Detection on addresses it creates. That is, the 'DupAddrDetectTransmits' variable in the MS should have a value of zero. If the MS finds more than one Prefix in the Router Advertisement message, it shall only consider the first one and silently discard the others. The GGSN shall not generate any globally unique IPv6 addresses for itself using the Prefix assigned to the MS in the Router Advertisement.

If the O-flag ("Other stateful configuration flag") was set in the Router Advertisement, the MS may start a DHCP session to retrieve additional configuration parameters. See subclause 13.2.2 "Other configuration by the Intranet or ISP". If the MS is not DHCP capable, the O-flag may be ignored.

RQ_000_7056 Stateful Autoconfiguration
TS 129 061 11.2.1.3.3 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 Mobile Station SHALL use the IPv6 Interface-Identifier, as provided by the gateway GPRS Support Node during IPv6 PDP Context Activation, to create its IPv6 Link-Local Unicast Address according to the procedures specified in RFC 2373.
Specification Text:
After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373

RQ_000_7057 Stateful Autoconfiguration
TS 129 061 11.2.1.3.3 MANDATORY
Applies to: Host
Context:
An Ipv6 Mobile Station which is capable of performing stateful address autoconfiguration receives a Router Advertisement with the M-flag set to one.
Requirement:
The IPv6 Mobile Station SHALL start a DHCPv6 configuration to request an IPv6 address.
Specification Text:
When the MS has received a Router Advertisement with the M-flag set, it shall start a DHCPv6 configuration as described in subclause "Address allocation using DHCPv6" including a request for an IPv6 address.

RQ_000_7058 3GPP Startup Router Behavior
TS 129 061 11.2.1.3.4 MANDATORY
Applies to: Router
Context:

Requirement:
Unless specifically stated otherwise in TS 129 061 or other 3GPP specifications, an IPv6 Gateway GPRS Support Node SHALL behave as a IPv6 router and be consistent with the RFCs specifying Stateless and Stateful Address Autoconfiguration procedures.
Specification Text:
For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 [29] and RFC 2461 [44]), unless stated otherwise in this or other 3GPP specifications.

RQ_000_7059 Simultaneous Stateless and Stateful Autoconfiguration
TS 129 061 13a.2.1 OPTIONAL
Applies to: Host
Context:

Requirement:
An IPv6 Mobile Station MAY simultaneously use stateless address autoconfiguration for configuring its IPv6 address and stateful autoconfiguration for configuring IMS specific parameters.
Specification Text:
When the "M-flag" is cleared, the "O- flag" shall be set in IPv6 Router Advertisement messages sent by the GGSN for APNs used for IMS services. This will trigger a DHCP capable MS to start a DHCPv6 session to retrieve server addresses and other configuration parameters. An MS which doesn't support DHCP will simply ignore the "O-flag". **An MS may simultaneously use stateless address autoconfiguration for configuring its IPv6 address and stateful autoconfiguration for configuring IMS specific parameters**.

RQ_000_7999 Configure Address
TS 129 061 11.2.1.3.1 MANDATORY
Applies to: Router
Context:
An IPv6 Gateway GPRS Support Node receives a Create PDP Context Request from an Access Point Name that is configured for stateful address autoconfiguration
Requirement:
The IPv6 Gateway GPRS Support Node SHALL return an IPv6 address in the PDP Address Information Element of the Create PDP Context Response with the Prefix part set to the link-local prefix, FE80::/64.
Specification Text:
The GGSN shall in the PDP Address IE in the Create PDP Context Response return an IPv6 address composed of a Prefix and an Interface-Identifier. The Interface-Identifier may have any value and it does not need to be unique within or across APNs. It shall however not conflict with the Interface-Identifier the GGSN has selected for its own side of the MS-GGSN link. The Prefix assigned by the GGSN or the external AAA server shall be globally or site-local unique, if stateless address autoconfiguration is configured on this APN. **If, on the other hand, stateful address autoconfiguration is configured on the APN, the Prefix part of the IPv6 address returned in the PDP Address IE shall be set to the link-local prefix (FE80::/64).**

4.4 Requirements extracted from RFC 1981

RQ_000_1802 Discover PMTU
RFC1981 1 RECOMMENDED
Applies to: Router, Host
Context:

Requirement:
An IPv6 node SHOULD implement Path MTU Discovery in order to discover and take advantage of paths with PMTU greater than the IPv6 minimum link MTU.
Specification Text:
IPv6 nodes SHOULD implement Path MTU Discovery in order to discover and take advantage of paths with PMTU greater than the IPv6 minimum link MTU [RFC 2460]. A minimal IPv6 implementation (e.g., in a boot ROM) may choose to omit implementation of Path MTU Discovery.

RQ_000_1803 Discover PMTU
RFC1981 1 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MAY omit the implementation of Path MTU Discovery
Specification Text:
IPv6 nodes SHOULD implement Path MTU Discovery in order to discover and take advantage of paths with PMTU greater than the IPv6 minimum link MTU [IPv6-SPEC]. **A minimal IPv6 implementation (e.g., in a boot ROM) may choose to omit implementation of Path MTU Discovery**.

RQ_000_1806 Discover PMTU
RFC1981 3 CONDITIONAL
[if RQ_000_1098 or RQ_000_1802 then MANDATORY]
Applies to: Host, Router
Context:
An IPv6 node has not yet determined the MTU for a particular path to another node
Requirement:
The IPv6 node MUST initially send sends packets at the (known) MTU of the first hop in the path.
Specification Text:
This memo describes a technique to dynamically discover the PMTU of a path. **The basic idea is that a source node initially assumes that the PMTU of a path is the (known) MTU of the first hop in the path**. If any of the packets sent on that path are too large to be forwarded by some node along the path, that node will discard them and return ICMPv6 Packet Too Big messages [RFC 2463]. Upon receipt of such a message, the source node reduces its assumed PMTU for the path based on the MTU of the constricting hop as reported in the Packet Too Big message.

RQ_000_1808 Discover PMTU
RFC1981 3 CONDITIONAL
[if RQ_000_1806 then MANDATORY]
Applies to: Router, Host
Context:
An IPv6 node receives an ICMPv6 Packet Too Big message in response to a packet it had previously sent
Requirement:
The IPv6 node MUST reduce its assumed PMTU for the path, based on the content of the MTU field in the Packet Too Big message.
Specification Text:
This memo describes a technique to dynamically discover the PMTU of a path. The basic idea is that a source node initially assumes that the PMTU of a path is the (known) MTU of the first hop in the path. **If any of the packets sent on that path are too large to be forwarded by some node along the path, that node will discard them and return ICMPv6 Packet Too Big messages [RFC 2463]. Upon receipt of such a message, the source node reduces its assumed PMTU for the path based on the MTU of the constricting hop as reported in the Packet Too Big message**

RQ_000_1810 Discover PMTU
RFC1981 3 CONDITIONAL
[if RQ_000_1098 or RQ_000_1802 then OPTIONAL]

Applies to: Host, Router
Context:
An IPv6 node is in the process of discovering the MTU of a path to another node
Requirement:
The IPv6 node MAY end the discovery process by ceasing to send packets larger than the IPv6 minimum link MTU.
Specification Text:
The Path MTU Discovery process ends when the node's estimate of the PMTU is less than or equal to the actual PMTU. Note that several iterations of the packet-sent/Packet-Too-Big-message-received cycle may occur before the Path MTU Discovery process ends, as there may be links with smaller MTUs further along the path.

Alternatively, the node may elect to end the discovery process by ceasing to send packets larger than the IPv6 minimum link MTU.

RQ_000_1812 Discover PMTU
RFC1981 3 CONDITIONAL
[if RQ_000_1098 or RQ_000_1802 then MANDATORY]

Applies to: Host, Router
Context:
An IPv6 node has established an MTU on a path to another node
Requirement:
The IPv6 node MUST periodically but infrequently increase the PMTU during data delivery.
Specification Text:
The PMTU of a path may change over time, due to changes in the routing topology. Reductions of the PMTU are detected by Packet Too Big messages. **To detect increases in a path's PMTU, a node periodically increases its assumed PMTU. This will almost always result in packets being discarded and Packet Too Big messages being generated, because in most cases the PMTU of the path will not have changed. Therefore, attempts to detect increases in a path's PMTU should be done infrequently.**

RQ_000_1814 Multicast PMTU Discovery
RFC1981 3 CONDITIONAL
[if RQ_000_1098 or RQ_000_1802 then MANDATORY]

Applies to: Host, Router
Context:
An IPv6 node supports Path MTU discovery
Requirement:
The IPv6 node MUST support Path MTU Discovery for Multicast as well as unicast destinations.
Specification Text:
Path MTU Discovery supports multicast as well as unicast destinations. In the case of a multicast destination, copies of a packet may traverse many different paths to many different nodes. Each path may have a different PMTU, and a single multicast packet may result in multiple Packet Too Big messages, each reporting a different next-hop MTU. The minimum PMTU value across the set of paths in use determines the size of subsequent packets sent to the multicast destination.

RQ_000_1815 Multicast PMTU Discovery
RFC1981 3 CONDITIONAL
[if RQ_000_1098 or RQ_000_1802 then MANDATORY]

Applies to: Host, Router
Context:
An IPv6 node is in the process of determining the Path MTU for sending packets to a multicast address
Requirement:
The IPv6 node MUST use the minimum PMTU value determined across all members of the multicast group as the PMTU to be used when sending subsequent packets to the multicast destination.
Specification Text:
Path MTU Discovery supports multicast as well as unicast destinations. **In the case of a multicast destination, copies of a packet may traverse many different paths to many different nodes. Each path may have a different PMTU, and a single multicast packet may result in multiple Packet Too Big messages, each reporting a different next-hop MTU. The minimum PMTU value across the set of paths in use determines the size of subsequent packets sent to the multicast destination**.

RQ_000_1816 Discover PMTU
RFC1981 3 CONDITIONAL
[if RQ_000_1098 or RQ_000_1802 then MANDATORY]

Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST perform Path MTU Discovery even if the destination node appears to be attached to the same link as itself.
Specification Text:
Note that Path MTU Discovery must be performed even in cases where a node "thinks" a destination is attached to the same link as itself. In a situation such as when a neighboring router acts as proxy for some destination, the destination can to appear to be directly connected but is in fact more than one hop away.

RQ_000_1818 Discover PMTU
RFC1981 4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an ICMPv6 Packet Too Big message in response to a packet it had previously sent
Requirement:
The IPv6 node MUST reduce its assumed PMTU for the path, based on the content of the MTU field in the Packet Too Big message.
Specification Text:
After receiving a Packet Too Big message, a node MUST attempt to avoid eliciting more such messages in the near future. **The node MUST reduce the size of the packets it is sending along the path**. Using a PMTU estimate larger than the IPv6 minimum link MTU may continue to elicit Packet Too Big messages. Since each of these messages (and the dropped packets they respond to) consume network resources, the node MUST force the Path MTU Discovery process to end}}.

RQ_000_1819 Discover PMTU
RFC1981 4 CONDITIONAL
[if RQ_000_1098 or RQ_000_1802 then MANDATORY]

Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST detect a reduction in the MTU on an active path as fast as possible.
Specification Text:
Nodes using Path MTU Discovery MUST detect decreases in PMTU as fast as possible. Nodes MAY detect increases in PMTU, but because doing so requires sending packets larger than the current estimated PMTU, and because the likelihood is that the PMTU will not have increased, this MUST be done at infrequent intervals. An attempt to detect an increase (by sending a packet larger than the current estimate) MUST NOT be done less than 5 minutes after a Packet Too Big message has been received for the given path. The recommended setting for this timer is twice its minimum value (10 minutes).

RQ_000_1820 Discover PMTU
RFC1981 4 CONDITIONAL
[if RQ_000_1098 or RQ_000_1802 then OPTIONAL]

Applies to: Host, Router
Context:

Requirement:
An IPv6 node MAY implement procedures to detect an increase in the MTU on an active path.
Specification Text:
Nodes using Path MTU Discovery MUST detect decreases in PMTU as fast as possible. **Nodes MAY detect increases in PMTU, but because doing so requires sending packets larger than the current estimated PMTU, and because the likelihood is that the PMTU will not have increased, this MUST be done at infrequent intervals**. An attempt to detect an increase (by sending a packet larger than the current estimate) MUST NOT be done less than 5 minutes after a Packet Too Big message has been received for the given path. The recommended setting for this timer is twice its minimum value (10 minutes).

RQ_000_1821 Discover PMTU
RFC1981 4 CONDITIONAL
[if RQ_000_1098 or RQ_000_1802 then MANDATORY]

Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT reduce its estimate of the Path MTU below the IPv6 minimum link MTU.
Specification Text:
A node MUST NOT reduce its estimate of the Path MTU below the IPv6 minimum link MTU.

Note: A node may receive a Packet Too Big message reporting a next-hop MTU that is less than the IPv6 minimum link MTU. In that case, the node is not required to reduce the size of subsequent packets sent on the path to less than the IPv6 minimum link MTU, but rather must include a Fragment header in those packets [RFC 2360].

RQ_000_1822 Discover PMTU
RFC1981 4 CONDITIONAL
[if RQ_000_1064 and RQ_000_1808 then MANDATORY]

Applies to: Router, Host
Context:
An IPv6 node receives a Packet Too Big message reporting a next-hop MTU that is less than the IPv6 minimum link MTU.
Requirement:
The IPv6 node MUST include a Fragment header in subsequent packets sent on the path.
Specification Text:
A node MUST NOT reduce its estimate of the Path MTU below the IPv6 minimum link MTU.

Note: A node may receive a Packet Too Big message reporting a next-hop MTU that is less than the IPv6 minimum link MTU. In that case, the node is not required to reduce the size of subsequent packets sent on the path to less than the IPv6 minimum link MTU, but rather must include a Fragment header in those packets [RFC 2360].

RQ_000_1823 Discover PMTU
RFC1981 4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT increase its estimate of the Path MTU in response to the contents of a Packet Too Big message.
Specification Text:
A node MUST NOT increase its estimate of the Path MTU in response to the contents of a Packet Too Big message. A message purporting to announce an increase in the Path MTU might be a stale packet that has been floating around in the network, a false packet injected as part of a denial-of-service attack, or the result of having multiple paths to the destination, each with a different PMTU.

RQ_000_1867 Discover PMTU
RFC1981 4 CONDITIONAL
[if RQ_000_1820 then MANDATORY]

Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT attempt to detect an increase in the MTU on an active path less than 5 minutes after a Packet Too Big message has been received for the given path.
Specification Text:
Nodes using Path MTU Discovery MUST detect decreases in PMTU as fast as possible. Nodes MAY detect increases in PMTU, but because doing so requires sending packets larger than the current estimated PMTU, and because the likelihood is that the PMTU will not have increased, this MUST be done at infrequent intervals. **An attempt to detect an increase (by sending a packet larger than the current estimate) MUST NOT be done less than 5 minutes after a Packet Too Big message has been received for the given path.** The recommended setting for this timer is twice its minimum value (10 minutes).

RQ_000_1868 Discover PMTU
RFC1981 4 CONDITIONAL
[if RQ_000_1820 then RECOMMENDED]

Applies to: Router, Host
Context:

Requirement:
If an IPv6 node implements procedures to detect an increase in the MTU on an active path, these should be invoked 10 minutes after receiving a Packet Too Big message for the given path.
Specification Text:
Nodes using Path MTU Discovery MUST detect decreases in PMTU as fast as possible. Nodes MAY detect increases in PMTU, but because doing so requires sending packets larger than the current estimated PMTU, and because the likelihood is that the PMTU will not have increased, this MUST be done at infrequent intervals. **An attempt to detect an increase (by sending a packet larger than the current estimate) MUST NOT be done less than 5 minutes after a Packet Too Big message has been received for the given path. The recommended setting for this timer is twice its minimum value (10 minutes).**

4.5 Requirements extracted from RFC 2460

RQ_000_1000 Generate IPv6 Header
RFC2460 3 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node sends an IPv6 packet.
Requirement:
The IPv6 node MUST set the value of the Payload Length Field in an IPv6 Header to the packet's total length (in octets) minus the IPv6 header's length (in octets).
Specification Text:
Payload Length 16-bit unsigned integer. **Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets. (Note that any extension headers [section 4] present are considered part of the payload, i.e., included in the length count.)**

RQ_000_1001 Generate IPv6 Header
RFC2460 3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet.
Requirement:
The IPv6 node MUST set the value in the Next Header Field in an IPv6 Header to the type of header immediately following the IPv6 header as defined in IETF RFC-1700.
Specification Text:
Next Header 8-bit selector. **Identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].**

RQ_000_1002 Process Hop Limit
RFC2460 3 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet with the Hop Limit field set to a value greater than 1 and the Destination Address field set to a value that does not correspond to the address of the router.
Requirement:
The router MUST decrement the value in Hop Limit field and forward the modified packet.
Specification Text:
Hop Limit 8-bit unsigned integer. **Decremented by 1 by each node that forwards the packet**. The packet is discarded if Hop Limit is decremented to zero.

RQ_000_1003 Process Hop Limit
RFC2460 3 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet with the Hop Limit field set to a value of 1 and the Destination Address field set to a value that does not correspond to the address of the router.
Requirement:
The router MUST NOT forward the packet.
Specification Text:
Hop Limit 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. **The packet is discarded if Hop Limit is decremented to zero**.

RQ_000_1004 Process Extension Headers
RFC2460 4 -3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing extension headers other than the Hop-by-Hop Options header and with the Destination Address field in the IPv6 header set to a value that does not correspond to the address of the IPv6 node.
Requirement:
The IPv6 node MUST NOT process the extension headers.
Specification Text:
With one exception, extension headers are not examined or processed by any node along a packet's delivery path, until the packet reaches the node (or each of the set of nodes, in the case of multicast) identified in the Destination Address field of the IPv6 header. ...The exception referred to in the preceding paragraph is the Hop-by- Hop Options header, ...

RQ_000_1005 Process Extension Headers
RFC2460 4 -3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing extension headers other than the Hop-by-Hop Options header and with the Destination Address field in the IPv6 header set to a value that corresponds to the address of the IPv6 node.
Requirement:
The IPv6 node MUST processes the extension headers.
Specification Text:
With one exception, extension headers are not examined or processed by any node along a packet's delivery path, until the packet reaches the node (or each of the set of nodes, in the case of multicast) identified in the Destination Address field of the IPv6 header. ...The exception referred to in the preceding paragraph is the Hop-by- Hop Options header, ...

RQ_000_1006 Process Extension Headers
RFC2460 4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet containing several extension headers.
Requirement:
The IPv6 node MUST process the extension headers strictly in the order they appear in the packet.
Specification Text:
Therefore, **extension headers must be processed strictly in the order they appear in the packet**; a receiver must not, for example, scan through a packet looking for a particular kind of extension header and process that header prior to processing all preceding ones .

RQ_000_1007 Process Hop by Hop Header
RFC2460 4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet with a Hop-by-Hop Options header
Requirement:
The IPv6 node MUST process the extension header.
Specification Text:
The exception referred to in the preceding paragraph is the Hop-by- Hop Options header, which carries information that must be examined and processed by every node along a packet's delivery path, including the source and destination nodes. The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header. Its presence is indicated by the value zero in the Next Header field of the IPv6 header.

RQ_000_1008 Generate Hop by Hop Header
RFC2460 4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet which includes a Hop-by-Hop Options extension header.
Requirement:
The Hop-by-Hop Options extension header MUST be the first extension header following the IPv6 header.
Specification Text:
The exception referred to in the preceding paragraph is the Hop-by- Hop Options header, which carries information that must be examined and processed by every node along a packet's delivery path, including the source and destination nodes. **The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header.** Its presence is indicated by the value zero in the Next Header field of the IPv6 header.

RQ_000_1009 Generate Hop by Hop Header
RFC2460 4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node sends an IPv6 packet which includes a Hop-by-Hop Options extension header.
Requirement:
The Next Header field in the IPv6 Header MUST be set to the value zero (0).
Specification Text:
The exception referred to in the preceding paragraph is the Hop-by- Hop Options header, which carries information that must be examined and processed by every node along a packet's delivery path, including the source and destination nodes. The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header. **Its presence is indicated by the value zero in the Next Header field of the IPv6 header**.

RQ_000_1010 Process Extension Headers
RFC2460 4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet containing an extension header in which the Next Header field is set to an unrecognized value.
Requirement:
The IPv6 node MUST discard the packet
Specification Text:
If, as a result of processing a header, a node is required to proceed to the next header but the Next Header value in the current header is unrecognized by the node, it should discard the packet and send an ICMP Parameter Problem message to the source of the packet, with an ICMP Code value of 1 ("unrecognized Next Header type encountered") and the ICMP Pointer field containing the offset of the unrecognized value within the original packet. The same action should be taken if a node encounters a Next Header value of zero in any header other than an IPv6 header.

RQ_000_1011 Process Extension Headers
RFC2460 4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet containing a Next Header field set to zero in any header other than the IPv6 header.
Requirement:
The IPv6 node MUST discard the packet
Specification Text:
If, as a result of processing a header, a node is required to proceed to the next header but the Next Header value in the current header is unrecognized by the node, **it should discard the packet** and send an ICMP Parameter Problem message to the source of the packet, with an ICMP Code value of 1 ("unrecognized Next Header type encountered") and the ICMP Pointer field containing the offset of the unrecognized value within the original packet. **The same action should be taken if a node encounters a Next Header value of zero in any header other than an IPv6 header**.

RQ_000_1013 Generate Extension Headers
RFC2460 4.1 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 node sends an IPv6 packet containing more than one extension header.
Requirement:
The extension headers SHOULD appear in the following order:
1. IPv6 header,
2. Hop-by-Hop Options header,
3. Destination Options header,
4. Routing header,
5. Fragment header,
6. Authentication header,
7. Encapsulating Security Payload header,
8. Destination Options header,
9. upper-layer header.

Specification Text:
When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order:

IPv6 header
Hop-by-Hop Options header
Destination Options header
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header
upper-layer header

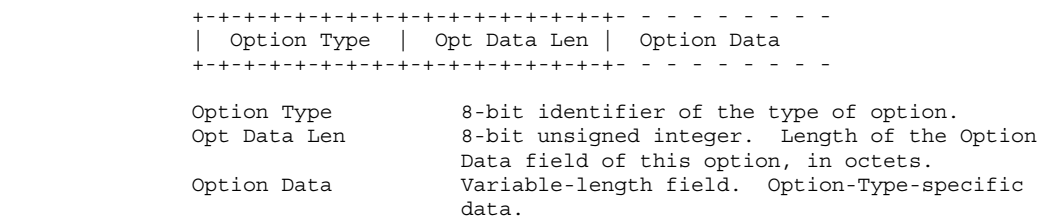
RQ_000_1014 Generate Extension Headers
RFC2460 4.1 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 node sends an IPv6 packet containing more than one extension header.
Requirement:
An IPv6 packet SHOULD NOT contain more than one instance of each extension header except for the Destination Options header
Specification Text:
Each extension header should occur at most once, except for the Destination Options header which should occur at most twice (once before a Routing header and once before the upper-layer header).

RQ_000_1015 Generate Extension Headers
RFC2460 4.1 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 node transmits a packet containing an upper-layer header which, itself, contains an IPv6 header with its own extension headers; i.e. IPv6 tunnelled over or encapsulated in IPv6.
Requirement:
The extension headers within the upper-layer header SHOULD appear in the following order:
1. IPv6 header,
2. Hop-by-Hop Options header,
3. Destination Options header,
4. Routing header, Fragment header,
5. Authentication header,
6. Encapsulating Security Payload header,
7. Destination Options header,
8. upper-layer header.

Specification Text:
If the upper-layer header is another IPv6 header (in the case of IPv6 being tunneled over or encapsulated in IPv6), it may be followed by its own extension headers, which are separately (sic) subject to the same ordering recommendations.

RQ_000_1016 Process Extension Headers
RFC2460 4.1 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a packet containing more than one extension header with duplicated extension headers and the headers not arranged in the recommended order. The Hop-by-Hop Options header is the first extension header in the packet.
Requirement:
The IPv6 node MUST accept and attempt to process extension headers (other than the Hop-by-Hop options header) in any order and occurring any number of times within the received packet.
Specification Text:
IPv6 nodes must accept and attempt to process extension headers in any order and occurring any number of times in the same packet, except for the Hop-by-Hop Options header which is restricted to appear immediately after an IPv6 header only. Nonetheless, it is strongly advised that sources of IPv6 packets adhere to the above recommended order until and unless subsequent specifications revise that recommendation.

RQ_000_1017 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a packet with a Hop-by-Hop Options header comprising a variable number of type-length-value (TLV) encoded "options".
Requirement:
The IPv6 node MUST process the options contained within the Hop-by-Hop options header strictly in the order that they appear in the header.
Specification Text:
Two of the currently-defined extension headers -- **the Hop-by-Hop Options header** and the Destination Options header -- **carry a variable number of type-length-value (TLV) encoded "options",** of the following format:



Option Type — 8-bit identifier of the type of option.
Opt Data Len — 8-bit unsigned integer. Length of the Option Data field of this option, in octets.
Option Data — Variable-length field. Option-Type-specific data.

The sequence of options within a header must be processed strictly in the order they appear in the header; a receiver must not, for example, scan through the header looking for a particular kind of option and process that option prior to processing all preceding ones.

RQ_000_1018 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing a Hop-by-Hop Options extension header in which the Option Type field is set to an unrecognized value but with its highest-order two bits set to the binary value '00'.
Requirement:
The IPv6 node MUST ignore this option and continue processing the header.
Specification Text:
The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type.

00 - skip over this option and continue processing the header.

01 - discard the packet.

10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RQ_000_1019 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing a Hop-by-Hop Options extension header in which the Option Type field is set to an unrecognized value but with its highest-order two bits set to the binary value '01'.
Requirement:
The IPv6 node discards the packet.
Specification Text:
The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type:

00 - skip over this option and continue processing the header.

01 - discard the packet.

10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RQ_000_1020 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing a Hop-by-Hop Options extension header in which the Option Type field is set to an unrecognized value but with its highest-order two bits set to the binary value '10'.
Requirement:
The IPv6 node MUST discard the packet and send an ICMP Parameter Problem message to the packet's Source Address with the Code field set to the value 2 and the Pointer field set to the offset (in octets) of the unrecognized Option Type within the packet.
Specification Text:
The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type:

00 - skip over this option and continue processing the header.

01 - discard the packet.

10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RQ_000_1021 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing a Hop-by-Hop Options extension header in which the Option Type field is set to an unrecognized value but with its highest-order two bits set to the binary value '11' and the Destination Address field does not contain a multicast address.
Requirement:
The IPv6 node MUST discard the packet and send an ICMP Parameter Problem message to the packet's Source Address with the Code field set to the value 2 and the Pointer field set to the offset (in octets) of the unrecognized Option Type within the packet.
Specification Text:
The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type:

00 - skip over this option and continue processing the header.

01 - discard the packet.

10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

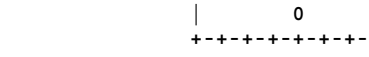
RQ_000_1022 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing both an Authentication Header and a Hop-by-Hop Options extension header with the third-highest-order bit in its Option Type field set to the binary value '1'.
Requirement:
The IPv6 node treats the entire Option Data field as zero-valued octets when verifying the packet's authenticating value.
Specification Text:
The third-highest-order bit of the Option Type specifies whether or not the Option Data of that option can change en-route to the packet's final destination. **When an Authentication header is present in the packet, for any option whose data may change en-route, its entire Option Data field must be treated as zero-valued octets when computing or verifying the packet's authenticating value.**

0 - Option Data does not change en-route

1 - Option Data may change en-route

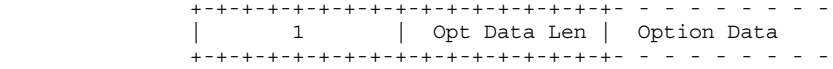
RQ_000_1028 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing a Hop-by-Hop Options extension header having its Option Type field set to zero (Pad1 option)
Requirement:
The IPv6 node MUST process the Pad1 option as a padding octet.
Specification Text:
There are two padding options which are used when necessary to align subsequent options pad out the containing header to a multiple of 8 octets in length. **These padding options must be recognized by all IPv6 implementations:**

Pad1 option (alignment requirement: none)



The Pad1 option is used to insert one octet of padding into the Options area of a header. If more than one octet of padding is required, the PadN option, described next, should be used, rather than multiple Pad1 options.

PadN option (alignment requirement: none)



The PadN option is used to insert two or more octets of padding into the Options area of a header. For N octets of padding, the Opt Data Len field contains the value N-2, and the Option Data consists of N-2 zero-valued octets.

RQ_000_1029 Generate Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node sends an IPv6 packet containing a Hop-by-Hop Options extension header which requires one octet of padding to ensure correct 8-octet alignment within the options extension header.
Requirement:
The IPv6 node MUST include an option in the Hop-by-Hop Options extension header with its Option Type field set to zero (Pad1) and with no option Data Length field and no option Data field.

Specification Text:

There are two padding options which are used when necessary to align subsequent options pad out the containing header to a multiple of 8 octets in length. These padding options must be recognized by all IPv6 implementations:

Pad1 option (alignment requirement: none)

The Pad1 option is used to insert one octet of padding into the Options area of a header. If more than one octet of padding is required, the PadN option, described next, should be used, rather than multiple Pad1 options.

RQ_000_1030 Generate Extension Header Options

RFC2460 4.2 RECOMMENDED

Applies to: Router, Host

Context:

An IPv6 node sends an IPv6 packet containing a Hop-by-Hop Options extension header which requires more than one octet of padding to ensure correct 8-octet alignment within the options extension header.

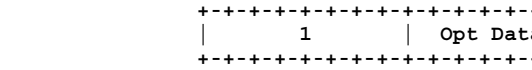
Requirement:

The IPv6 node SHOULD include an option in the Hop-by-Hop Options extension header with its Option Type field set to the value 1 (PadN), its Option Data Length field set to a value two less than the required number of padding bytes and its Option Data field containing that number of zero-valued octets.

Specification Text:

The Pad1 option is used to insert one octet of padding into the Options area of a header. **If more than one octet of padding is required, the PadN ion, described next, should be used, rather than multiple Pad1 options.**

PadN option (alignment requirement: none)



The PadN option is used to insert two or more octets of padding into the Options area of a header. For N octets of padding, the Opt Data Len field contains the value N-2, and the Option Data consists of N-2 zero-valued octets.

RQ_000_1032 Generate Hop by Hop Header

RFC2460 4.3 MANDATORY

Applies to: Host, Router

Context:

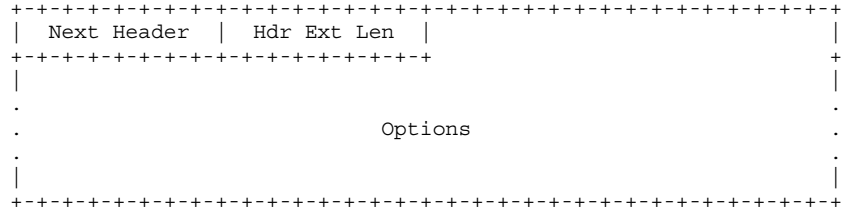
An IPv6 node sends an IPv6 packet containing a Hop-by-Hop Options extension header.

Requirement:

The IPv6 node MUST set the value of the Next Header Field in the Hop-by-Hop Options header to the value associated with the type of the header immediately following the Hop-by-Hop Options header (as defined in RFC-1700 and RFC-2460).

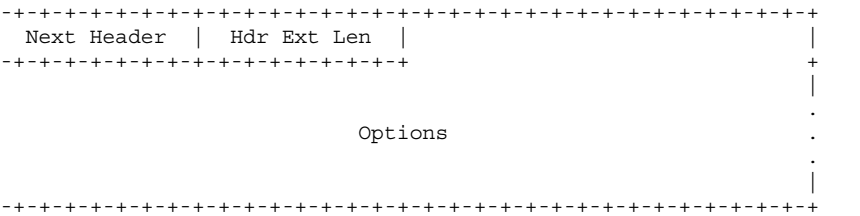
Specification Text:

The Hop-by-Hop Options header is used to carry optional information that must be examined by every node along a packet's delivery path. The Hop-by-Hop Options header is identified by a Next Header value of 0 in the IPv6 header, and has the following format:



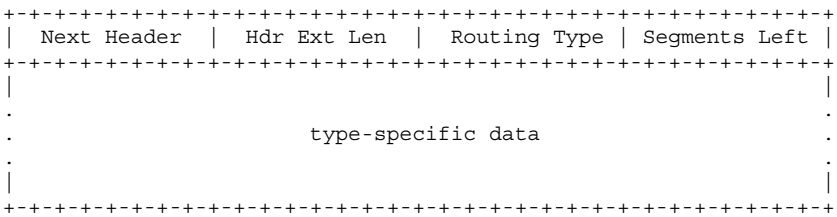
Next Header **8-bit selector. Identifies the type of header immediately following the Hop-by-Hop Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].**
Hdr Ext Len 8-bit unsigned integer. Length of the Hop-by-Hop Options header in 8-octet units, not including the first 8 octets.
Options Variable-length field, of length such that the complete Hop-by-Hop Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options, as described in section 4.2.

RQ_000_1033 Generate Hop by Hop Header
RFC2460 4.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet containing a Hop-by-Hop Options extension header.
Requirement:
The IPv6 node MUST set the value of the Hdr Ext Len Field in the Hop-by-Hop Options header to the length of the header in 8-octet units, not including the first 8 octets.
Specification Text:
The Hop-by-Hop Options header is used to carry optional information that must be examined by every node along a packet's delivery path. The Hop-by-Hop Options header is identified by a Next Header value of 0 in the IPv6 header, and has the following format:

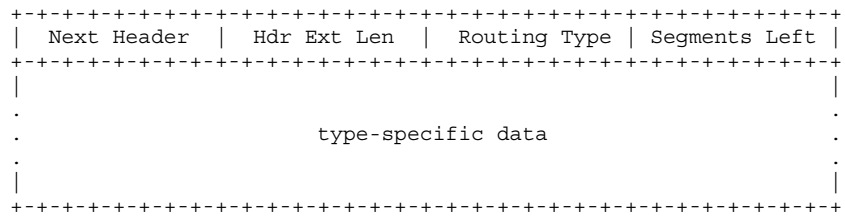


Next Header 8-bit selector. Identifies the type of header immediately following the Hop-by-Hop Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len **8-bit unsigned integer. Length of the Hop-by-Hop Options header in 8-octet units, not including the first 8 octets.**
Options Variable-length field, of length such that the complete Hop-by-Hop Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options, as described in section 4.2.

RQ_000_1035 Generate Routing Header
RFC2460 4.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet containing a Routing extension header.
Requirement:
The IPv6 node MUST set the appropriate Next Header field (either in the IPv6 Header or in the extension header immediately preceding the Routing extension header) to the value forty-three (43).
Specification Text:
The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination. This function is very similar to IPv4's Loose Source and Record Route option. **The Routing header is identified by a Next Header value of 43 in the immediately preceding header**, and has the following format:

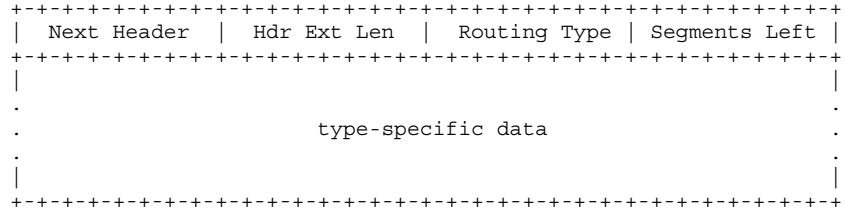


RQ_000_1036 Generate Routing Header
RFC2460 4.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet containing a Routing header.
Requirement:
The IPv6 node MUST set the value of the Next Header Field in the Routing header to the value associated with the type of the header immediately following the Routing header (as defined in RFC-1700 and RFC-2460).
Specification Text:
The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination. This function is very similar to IPv4's Loose Source and Record Route option. The Routing header is identified by a Next Header value of 43 in the immediately preceding header, and has the following format:



Next Header	**8-bit selector. Identifies the type of header immediately following the Routing header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].**
Hdr Ext Len	8-bit unsigned integer. Length of the Routing header in 8-octet units, not including the first 8 octets.
Routing Type	8-bit identifier of a particular Routing header variant.
Segments Left	8-bit unsigned integer. Number of route segments remaining, i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination.
type-specific data	Variable-length field, of format determined by the Routing Type, and of length such that the complete Routing header is an integer multiple of 8 octets long.

RQ_000_1037 Generate Routing Header
RFC2460 4.4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node sends an IPv6 packet containing a Routing header.
Requirement:
The IPv6 node MUST set the Hdr Ext Len Field in the Routing header to a value representing the length, in 8-octet units, of the header, not including the first 8 octets.
Specification Text:
The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination. This function is very similar to IPv4's Loose Source and Record Route option. The Routing header is identified by a Next Header value of 43 in the immediately preceding header, and has the following format:



Next Header	8-bit selector. Identifies the type of header immediately following the Routing header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	**8-bit unsigned integer. Length of the Routing header in 8-octet units, not including the first 8 octets.**
Routing Type	8-bit identifier of a particular Routing header variant.
Segments Left	8-bit unsigned integer. Number of route segments remaining, i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination.
type-specific data	Variable-length field, of format determined by the Routing Type, and of length such that the complete Routing header is an integer multiple of 8 octets long.

RQ_000_1038 Generate Routing Header

RFC2460 4.4 MANDATORY

Applies to: Router, Host

Context:

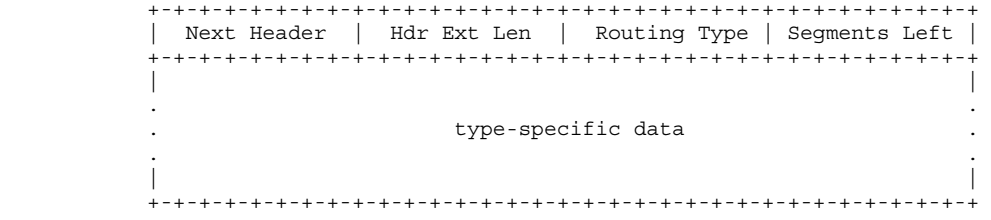
An IPv6 node sends an IPv6 packet containing a Routing header.

Requirement:

The IPv6 node MUST set the Segments Left field in the Routing header to the number of explicitly listed intermediate nodes still to be visited before reaching the final destination.

Specification Text:

The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination. This function is very similar to IPv4's Loose Source and Record Route option. The Routing header is identified by a Next Header value of 43 in the immediately preceding header, and has the following format:



Next Header	8-bit selector. Identifies the type of header immediately following the Routing header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	8-bit unsigned integer. Length of the Routing header in 8-octet units, not including the first 8 octets.
Routing Type	8-bit identifier of a particular Routing header variant.
Segments Left	**8-bit unsigned integer. Number of route segments remaining, i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination.**
type-specific data	Variable-length field, of format determined by the Routing Type, and of length such that the complete Routing header is an integer multiple of 8 octets long.

RQ_000_1040 Process Routing Header
RFC2460 4.4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet containing a Routing header with its Routing Type field set to an unrecognizable value and its Segments Left field set to the value zero.
Requirement:
The IPv6 node MUST ignore the Routing header and processes the next header in the packet whose type is identified by the Next Header field in the Routing header.
Specification Text:
If, while processing a received packet, a node encounters a Routing header with an unrecognized Routing Type value, the required behavior of the node depends on the value of the Segments Left field, as follows:

If Segments Left is zero, the node must ignore the Routing header and proceed to process the next header in the packet, whose type is identified by the Next Header field in the Routing header.

If Segments Left is non-zero, the node must discard the packet and send an ICMP Parameter Problem, Code 0, message to the packet's Source Address, pointing to the unrecognized Routing Type.

RQ_000_1041 Process Routing Header
RFC2460 4.4 MANDATORY
Applies to: Router
Context:
An IPv6 node receives an IPv6 packet containing a Routing header with its Routing Type field set to an unrecognizable value and its Segments Left field set to a non-zero value.
Requirement:
The IPv6 node MUST discard the packet and send an ICMP Parameter Problem message to the packet's Source Address with the Code field set to zero (0) and its Pointer field set to the offset (in octets) from the start of the packet to the unrecognized Routing Type.
Specification Text:
If, while processing a received packet, a node encounters a Routing header with an unrecognized Routing Type value, the required behavior of the node depends on the value of the Segments Left field, as follows:

If Segments Left is zero, the node must ignore the Routing header and proceed to process the next header in the packet, whose type is identified by the Next Header field in the Routing header.

If Segments Left is non-zero, the node must discard the packet and send an ICMP Parameter Problem, Code 0, message to the packet's Source Address, pointing to the unrecognized Routing Type.

RQ_000_1042 Process Routing Header
RFC2460 4.4 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet containing a Routing header indicating that the packet is to be forwarded onto a link whose link MTU is less than the size of the packet.
Requirement:
The IPv6 router MUST discard the packet and send an ICMP Packet Too Big message to the packet's Source Address.
Specification Text:
If, after processing a Routing header of a received packet, an intermediate node determines that the packet is to be forwarded onto a link whose link MTU is less than the size of the packet, the node must discard the packet and send an ICMP Packet Too Big message to the packet's Source Address.

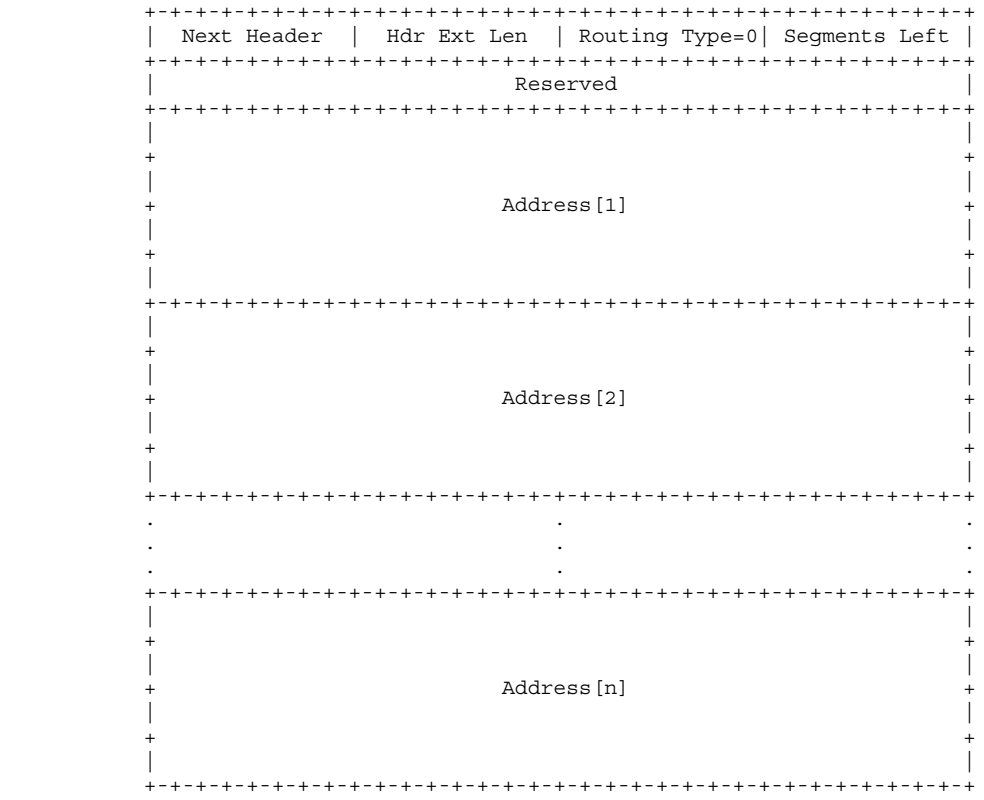
RQ_000_1044 Process Extension Headers
RFC2460 4 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing an extension header in which the Next Header field is set to an unrecognized value.
Requirement:
The IPv6 node SHOULD send an ICMP Parameter Problem message to the source of the packet, with an ICMP Code value of 1 ("unrecognized Next Header type encountered") and the ICMP Pointer field containing the offset to the unrecognized value within the original packet.
Specification Text:
If, as a result of processing a header, a node is required to proceed to the next header but the Next Header value in the current header is unrecognized by the node, it should discard the packet **and send an ICMP Parameter Problem message to the source of the packet, with an ICMP Code value of 1 ("unrecognized Next Header type encountered") and the ICMP Pointer field containing the offset of the unrecognized value within the original packet**. The same action should be taken if a node encounters a Next Header value of zero in any header other than an IPv6 header.

RQ_000_1045 Process Extension Headers
RFC2460 4 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet containing a Next Header field set to zero in any header other than the IPv6 header
Requirement:
The implementation SHOULD send an ICMP Parameter Problem message to the source of the packet, with an ICMP Code value of 1 ("unrecognized Next Header type encountered") and the ICMP Pointer field containing the offset of the unrecognized value within the original packet.
Specification Text:
If, as a result of processing a header, a node is required to proceed to the next header but the Next Header value in the current header is unrecognized by the node, it should discard the packet and **send an ICMP Parameter Problem message to the source of the packet, with an ICMP Code value of 1 ("unrecognized Next Header type encountered") and the ICMP Pointer field containing the offset of the unrecognized value within the original packet. The same action should be taken if a node encounters a Next Header value of zero in any header other than an IPv6 header**.

RQ_000_1046 Process Routing Header
RFC2460 4.4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a packet containing a Routing header with its Routing Type field set to zero (0).
Requirement:
The node MUST ignore the contents of the Reserved Field in octets 5 to 8 of the Routing header.

Specification Text:

The Type 0 Routing header has the following format:



Next Header	8-bit selector. Identifies the type of header immediately following the Routing header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	8-bit unsigned integer. Length of the Routing header in 8-octet units, not including the first 8 octets. For the Type 0 Routing header, Hdr Ext Len is equal to two times the number of addresses in the header.
Routing Type	0.
Segments Left	8-bit unsigned integer. Number of route segments remaining, i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination.
Reserved	**32-bit reserved field. Initialized to zero for transmission; ignored on reception.**
Address[1..n]	Vector of 128-bit addresses, numbered 1 to n.

RQ_000_1047 Generate Routing Header

RFC2460 4.4 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node sends a packet containing a Routing header with its Routing Type field set to zero (0).

Requirement:

The IPv6 node MUST NOT set any of the Address fields in the Routing header to a Multicast addresses.

Specification Text:

Multicast addresses must not appear in a Routing header of Type 0, or in the IPv6 Destination Address field of a packet carrying a Routing header of Type 0.

RQ_000_1048 Generate Routing Header
RFC2460 4.4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node sends a packet containing a Routing header with its Routing Type field set to zero (0).
Requirement:
The IPv6 node MUST NOT set the IPv6 Destination Address field in the IPv6 header to a Multicast addresses.
Specification Text:
Multicast addresses must not appear in a Routing header of Type 0, **or in the IPv6 Destination Address field of a packet carrying a Routing header of Type 0**.

RQ_000_1049 Process Routing Header
RFC2460 4.4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a packet containing a Routing extension header and the Destination Address field in the IPv6 Header is not set to the address of the IPv6 node.
Requirement:
The IPv6 node MUST NOT process the Routing Header.
Specification Text:
A Routing header is not examined or processed until it reaches the node identified in the Destination Address field of the IPv6 header.

RQ_000_1051 Process Routing Header
RFC2460 4.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing a Routing extension header in which the Routing Type field is set to zero (0) and the Segments Left Field is also set to zero (0).
Requirement:
The IPv6 node MUST ignore all fields in the Routing extension header except for Next Header field.
Specification Text:
A Routing header is not examined or processed until it reaches the node identified in the Destination Address field of the IPv6 header. In that node, dispatching on the Next Header field of the immediately preceding header causes the Routing header module to be invoked, which, **in the case of Routing Type 0, performs the following algorithm:**

```
 if Segments Left = 0 {
    proceed to process the next header in the packet, whose type is
    identified by the Next Header field in the Routing header

 }
 else if Hdr Ext Len is odd {
       send an ICMP Parameter Problem, Code 0, message to the Source
       Address, pointing to the Hdr Ext Len field, and discard the packet
 }
 else {
    compute n, the number of addresses in the Routing header, by
    dividing Hdr Ext Len by 2
    if Segments Left is greater than n {
       send an ICMP Parameter Problem, Code 0, message to the Source
       Address, pointing to the Segments Left field, and discard the packet
    }
    else {
       decrement Segments Left by 1;
       compute i, the index of the next address to be visited in
       the address vector, by subtracting Segments Left from n
       if Address [i] or the IPv6 Destination Address is multicast {
          discard the packet
       }
       else {
          swap the IPv6 Destination Address and Address[i]
          if the IPv6 Hop Limit is less than or equal to 1 {
             send an ICMP Time Exceeded -- Hop Limit Exceeded in
             Transit message to the Source Address and discard the packet
          }
          else {
```

```
            decrement the Hop Limit by 1
            resubmit the packet to the IPv6 module for transmission
            to the new destination
         }
      }
   }
}
```

RQ_000_1052 Process Routing Header

RFC2460 4.4 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives an IPv6 packet containing a Routing extension header in which the Routing Type field is set to zero (0), the Segments Left Field is set to a value greater than zero (0) and the Hdr Ext Len field is set to an odd (not even) value.

Requirement:

The IPv6 node MUST discard the packet and send an ICMP Parameter Problem message to the packet's Source Address with the Code field set to the value 0 and the Pointer field set to the offset (in octets) of the Hdr Ext Len field within the packet.

Specification Text:

A Routing header is not examined or processed until it reaches the node identified in the Destination Address field of the IPv6 header. In that node, dispatching on the Next Header field of the immediately preceding header causes the Routing header module to be invoked, which, **in the case of Routing Type 0, performs the following algorithm**:

```
if Segments Left = 0 {
   proceed to process the next header in the packet, whose type is
   identified by the Next Header field in the Routing header
}
else if Hdr Ext Len is odd {
      send an ICMP Parameter Problem, Code 0, message to the Source
      Address, pointing to the Hdr Ext Len field, and discard the packet
}
else {
   compute n, the number of addresses in the Routing header, by
   dividing Hdr Ext Len by 2
   if Segments Left is greater than n {
      send an ICMP Parameter Problem, Code 0, message to the Source
      Address, pointing to the Segments Left field, and discard the packet
   }
   else {
      decrement Segments Left by 1;
      compute i, the index of the next address to be visited in
      the address vector, by subtracting Segments Left from n
      if Address [i] or the IPv6 Destination Address is multicast {
         discard the packet
      }
      else {
         swap the IPv6 Destination Address and Address[i]
         if the IPv6 Hop Limit is less than or equal to 1 {
            send an ICMP Time Exceeded -- Hop Limit Exceeded in
            Transit message to the Source Address and discard the packet
         }
         else {
            decrement the Hop Limit by 1
            resubmit the packet to the IPv6 module for transmission
            to the new destination
         }
      }
   }
}
```

RQ_000_1053 Process Routing Header

RFC2460 4.4 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives an IPv6 packet containing a Routing extension header in which the Routing Type field is set to zero (0), the Segments Left Field is set to a value greater than the number of addresses in the Routing Header and the Hdr Ext Len field is set to even value.

Requirement:

The IPv6 node MUST discard the packet and send an ICMP Parameter Problem message to the packet's Source Address with the Code field set to the value 0 and the Pointer field set to the offset (in octets) of the Segments Left field within the packet.

Specification Text:

A Routing header is not examined or processed until it reaches the node identified in the Destination Address field of the IPv6 header. In that node, dispatching on the Next Header field of the immediately preceding header causes the Routing header module to be invoked, which, **in the case of Routing Type 0, performs the following algorithm**:

```
if Segments Left = 0 {
   proceed to process the next header in the packet, whose type is
   identified by the Next Header field in the Routing header
}
else if Hdr Ext Len is odd {
      send an ICMP Parameter Problem, Code 0, message to the Source
      Address, pointing to the Hdr Ext Len field, and discard the packet
}
else {
   compute n, the number of addresses in the Routing header, by
   dividing Hdr Ext Len by 2
   if Segments Left is greater than n {
      send an ICMP Parameter Problem, Code 0, message to the Source
      Address, pointing to the Segments Left field, and discard the packet
   }
   else {
      decrement Segments Left by 1;
      compute i, the index of the next address to be visited in
      the address vector, by subtracting Segments Left from n
      if Address [i] or the IPv6 Destination Address is multicast {
         discard the packet
      }
      else {
         swap the IPv6 Destination Address and Address[i]
         if the IPv6 Hop Limit is less than or equal to 1 {
            send an ICMP Time Exceeded -- Hop Limit Exceeded in
            Transit message to the Source Address and discard the packet
         }
         else {
            decrement the Hop Limit by 1
            resubmit the packet to the IPv6 module for transmission
            to the new destination
         }
      }
   }
}
```

RQ_000_1054 Generate Extension Headers

RFC2460 4.1 RECOMMENDED

Applies to: Host, Router

Context:

An IPv6 node sends an IPv6 packet containing more than one extension header.

Requirement:

An IPv6 packet SHOULD NOT contain more than two instances of the Destination Options header (once before a Routing header and once before the upper-layer header).

Specification Text:

Each extension header should occur at most once, except for **the Destination Options header which should occur at most twice (once before a Routing header and once before the upper-layer header)**.

RQ_000_1055 Process Routing Header

RFC2460 4.4 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives an IPv6 packet containing a Routing extension header in which the Routing Type field is set to zero (0), the Segments Left Field is set to a value greater than zero (0) but not greater than the number of addresses in the Routing Header, the Hdr Ext Len field is set to even value and the next address to be visited is set to a multicast address.

Requirement:

The IPv6 node MUST discard the packet.

Specification Text:

A Routing header is not examined or processed until it reaches the node identified in the Destination Address field of the IPv6 header. In that node, dispatching on the Next Header field of the immediately preceding header causes the Routing header module to be invoked, which**, in the case of Routing Type 0, performs the following algorithm**:

```
 if Segments Left = 0 {
    proceed to process the next header in the packet, whose type is
    identified by the Next Header field in the Routing header
 }
 else if Hdr Ext Len is odd {
       send an ICMP Parameter Problem, Code 0, message to the Source
       Address, pointing to the Hdr Ext Len field, and discard the packet
 }
 else {
    compute n, the number of addresses in the Routing header, by
    dividing Hdr Ext Len by 2
    if Segments Left is greater than n {
       send an ICMP Parameter Problem, Code 0, message to the Source
       Address, pointing to the Segments Left field, and discard the packet
    }
    else {
       decrement Segments Left by 1;
       compute i, the index of the next address to be visited in
       the address vector, by subtracting Segments Left from n
       if Address [i] or the IPv6 Destination Address is multicast {
          discard the packet
       }
       else {
          swap the IPv6 Destination Address and Address[i]
          if the IPv6 Hop Limit is less than or equal to 1 {
             send an ICMP Time Exceeded -- Hop Limit Exceeded in
             Transit message to the Source Address and discard the packet
          }
          else {
             decrement the Hop Limit by 1
             resubmit the packet to the IPv6 module for transmission
             to the new destination
          }
       }
    }
 }
```

RQ_000_1056 Process Routing Header

RFC2460 4.4 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives an IPv6 packet containing a Routing extension header in which the Routing Type field is set to zero (0), the Segments Left Field is set to a value greater than zero (0) but not greater than the number of addresses in the Routing Header, the Hdr Ext Len field is set to even value and the Destination Address field in the IPv6 Header is set to a multicast address.

Requirement:

The IPv6 node MUST discard the packet.

Specification Text:

A Routing header is not examined or processed until it reaches the node identified in the Destination Address field of the IPv6 header. In that node, dispatching on the Next Header field of the immediately preceding header causes the Routing header module to be invoked, which**, in the case of Routing Type 0, performs the following algorithm**:

```
 if Segments Left = 0 {
    proceed to process the next header in the packet, whose type is
    identified by the Next Header field in the Routing header
 }
 else if Hdr Ext Len is odd {
       send an ICMP Parameter Problem, Code 0, message to the Source
       Address, pointing to the Hdr Ext Len field, and discard the packet
 }
 else {
    compute n, the number of addresses in the Routing header, by
    dividing Hdr Ext Len by 2
    if Segments Left is greater than n {
       send an ICMP Parameter Problem, Code 0, message to the Source
       Address, pointing to the Segments Left field, and discard the packet
    }
```

```
    else {
       decrement Segments Left by 1;
       compute i, the index of the next address to be visited in
       the address vector, by subtracting Segments Left from n
       if Address [i] or the IPv6 Destination Address is multicast {
          discard the packet
       }
       else {
          swap the IPv6 Destination Address and Address[i]
          if the IPv6 Hop Limit is less than or equal to 1 {
             send an ICMP Time Exceeded -- Hop Limit Exceeded in
             Transit message to the Source Address and discard the packet
          }
          else {
             decrement the Hop Limit by 1
             resubmit the packet to the IPv6 module for transmission
             to the new destination
          }
       }
    }
 }
```

RQ_000_1057 Process Extension Header Options

RFC2460 4.2 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a packet containing a Destination Options header comprising a variable number of type-length-value (TLV) encoded "options".

Requirement:

The IPv6 node MUST process the options contained within the Destination Options header strictly in the order that they appear in the header.

Specification Text:

Two of the currently-defined extension headers -- the Hop-by-Hop Options header and **the Destination Options header -- carry a variable number of type-length-value (TLV) encoded "options",** of the following format:

```
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
   |  Option Type  |  Opt Data Len |  Option Data
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -

   Option Type          8-bit identifier of the type of option.
   Opt Data Len         8-bit unsigned integer.  Length of the Option
                        Data field of this option, in octets.
   Option Data          Variable-length field.  Option-Type-specific
                        data.
```

The sequence of options within a header must be processed strictly in the order they appear in the header; a receiver must not, for example, scan through the header looking for a particular kind of option and process that option prior to processing all preceding ones.

RQ_000_1058 Process Routing Header

RFC2460 4.4 MANDATORY

Applies to: Router, Host

Context:

An IPv6 node receives an IPv6 packet containing a Routing extension header in which the Routing Type field is set to zero (0), the Segments Left Field is set to a value greater than zero (0) but not greater than the number of addresses in the Routing Header, the Hdr Ext Len field is set to even value, neither the next address to be visited (in the Routing Header) nor the Destination Address field (in the IPv6 Header) is set to a multicast address and the Hop Limit field in the IPv6 Header is set to a value less than or equal to 1.

Requirement:

The IPv6 node MUST discard the packet and send an ICMP Time Exceeded message to the packet's Source Address with the Code field set to the value zero (0) -- Hop Limit Exceeded in Transit.

Specification Text:

A Routing header is not examined or processed until it reaches the node identified in the Destination Address field of the IPv6 header. In that node, dispatching on the Next Header field of the immediately preceding header causes the Routing header module to be invoked, which, **in the case of Routing Type 0, performs the following algorithm**:

```
 if Segments Left = 0 {
    proceed to process the next header in the packet, whose type is
    identified by the Next Header field in the Routing header
 }
```

```
else if Hdr Ext Len is odd {
      send an ICMP Parameter Problem, Code 0, message to the Source
      Address, pointing to the Hdr Ext Len field, and discard the packet
}
else {
   compute n, the number of addresses in the Routing header, by
   dividing Hdr Ext Len by 2
   if Segments Left is greater than n {
      send an ICMP Parameter Problem, Code 0, message to the Source
      Address, pointing to the Segments Left field, and discard the packet
   }
   else {
      decrement Segments Left by 1;
      compute i, the index of the next address to be visited in
      the address vector, by subtracting Segments Left from n
      if Address [i] or the IPv6 Destination Address is multicast {
         discard the packet
      }
      else {
         swap the IPv6 Destination Address and Address[i]
         if the IPv6 Hop Limit is less than or equal to 1 {
            send an ICMP Time Exceeded -- Hop Limit Exceeded in
            Transit message to the Source Address and discard the packet
         }
         else {
            decrement the Hop Limit by 1
            resubmit the packet to the IPv6 module for transmission
            to the new destination
         }
      }
   }
}
```

RQ_000_1059 Process Routing Header

RFC2460 4.4 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives an IPv6 packet containing a Routing extension header in which the Routing Type field is set to zero (0), the Segments Left Field is set to a value greater than zero (0) but not greater than the number of addresses in the Routing Header, the Hdr Ext Len field is set to even value, neither the next address to be visited (in the Routing Header) nor the Destination Address field (in the IPv6 Header) is set to a multicast address and the Hop Limit field in the IPv6 Header is set to a value greater than 1.

Requirement:

The IPv6 node MUST decrement Segments Left field in the Routing extension header, swap the Destination Address in the IPv6 Header and next address to be visited in the Routing Header, decrement the Hop Limit in the IPv6 Header and forward the packet to the new Destination Address.

Specification Text:

A Routing header is not examined or processed until it reaches the node identified in the Destination Address field of the IPv6 header. In that node, dispatching on the Next Header field of the immediately preceding header causes the Routing header module to be invoked, which, **in the case of Routing Type 0, performs the following algorithm**:

```
if Segments Left = 0 {
   proceed to process the next header in the packet, whose type is
   identified by the Next Header field in the Routing header
}
else if Hdr Ext Len is odd {
      send an ICMP Parameter Problem, Code 0, message to the Source
      Address, pointing to the Hdr Ext Len field, and discard the packet
}
else {
   compute n, the number of addresses in the Routing header, by
   dividing Hdr Ext Len by 2
   if Segments Left is greater than n {
      send an ICMP Parameter Problem, Code 0, message to the Source
      Address, pointing to the Segments Left field, and discard the packet
   }
   else {
      decrement Segments Left by 1;
      compute i, the index of the next address to be visited in
      the address vector, by subtracting Segments Left from n
      if Address [i] or the IPv6 Destination Address is multicast {
         discard the packet
```

```
        }
        else {
           swap the IPv6 Destination Address and Address[i]
           if the IPv6 Hop Limit is less than or equal to 1 {
              send an ICMP Time Exceeded -- Hop Limit Exceeded in
              Transit message to the Source Address and discard the packet
           }
           else {
              decrement the Hop Limit by 1
              resubmit the packet to the IPv6 module for transmission
              to the new destination
           }
        }
     }
  }
```

RQ_000_1060 Process Extension Header Options

RFC2460 4.2 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives an IPv6 packet containing a Destination Options extension header in which the Option Type field is set to an unrecognized value but with its highest-order two bits set to the binary value '00'.

Requirement:

The IPv6 node MUST ignore this option and continue processing the header.

Specification Text:

The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type.

00 - skip over this option and continue processing the header.

01 - discard the packet.

10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RQ_000_1061 Process Extension Header Options

RFC2460 4.2 MANDATORY

Applies to: Router, Host

Context:

An IPv6 node receives an IPv6 packet containing a Destination Options extension header in which the Option Type field is set to an unrecognized value but with its highest-order two bits set to the binary value '01'.

Requirement:

The IPv6 node MUST discard the packet.

Specification Text:

The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type:

00 - skip over this option and continue processing the header.

01 - discard the packet.

10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RQ_000_1062 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet containing a Destination Options extension header in which the Option Type field is set to an unrecognized value but with its highest-order two bits set to the binary value '10'.
Requirement:
The IPv6 node MUST discard the packet and send an ICMP Parameter Problem message to the packet's Source Address with the Code field set to the value 2 and the Pointer field set to the offset (in octets) of the unrecognized Option Type within the packet.
Specification Text:
The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type:

00 - skip over this option and continue processing the header.

01 - discard the packet.

10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RQ_000_1063 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing a Destination Options extension header in which the Option Type field is set to an unrecognized value but with its highest-order two bits set to the binary value '11' and the Destination Address field does not contain a multicast address.
Requirement:
The IPv6 node MUST discard the packet and send an ICMP Parameter Problem message to the packet's Source Address with the Code field set to the value 2 and the Pointer field set to the offset (in octets) of the unrecognized Option Type within the packet.
Specification Text:
The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type:

00 - skip over this option and continue processing the header.

01 - discard the packet.

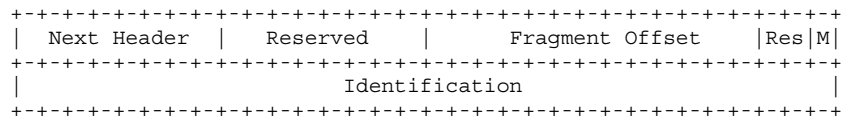
10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RQ_000_1064 Generate Fragment Packets
RFC2460 5 OPTIONAL
Applies to: Host
Context:
An IPv6 host sends an IPv6 packet which is larger than the MTU on the path between the host and the packet's destination.
Requirement:
The IPv6 host MAY fragment the packet using the Fragment header.
Specification Text:
In order to send a packet larger than a path's MTU, a node may use the IPv6 Fragment header to fragment the packet at the source and have it reassembled at the destination(s). However, the use of such fragmentation is discouraged in any application that is able to adjust its packets to fit the measured path MTU (i.e., down to 1280 octets).

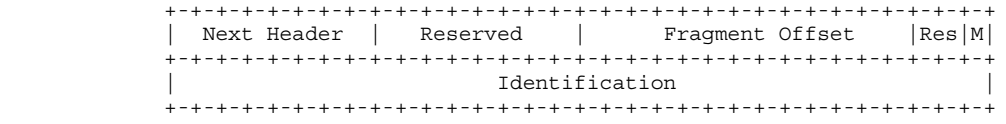
RQ_000_1065 Generate Fragment Packets
RFC2460 5 RECOMMENDED
Applies to: Host
Context:
An IPv6 host sends an IPv6 packet which is larger than the MTU on the path between the host and the packet's destination.
Requirement:
The IPv6 host SHOULD adjust the packet size to fit the path MTU.
Specification Text:
In order to send a packet larger than a path's MTU, a node may use the IPv6 Fragment header to fragment the packet at the source and have it reassembled at the destination(s). **However, the use of such fragmentation is discouraged in any application that is able to adjust its packets to fit the measured path MTU (i.e., down to 1280 octets)**.

RQ_000_1067 Generate Fragment Packets
RFC2460 4.5 CONDITIONAL
[if RQ_000_1064 then MANDATORY]
Applies to: Host
Context:
An IPv6 host sends an IPv6 packet containing a Fragment header.
Requirement:
The IPv6 host MUST set the Next Header field in the header preceding the Fragment header to the value forty-four (44)
Specification Text:
The Fragment header is used by an IPv6 source to send a packet larger than would fit in the path MTU to its destination. (Note: unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path -- see section 5.) **The Fragment header is identified by a Next Header value of 44 in the immediately preceding header**, and has the following format:



RQ_000_1068 Generate Fragment Packets
RFC2460 4.5 CONDITIONAL
[if RQ_000_1064 then MANDATORY]
Applies to: Host
Context:
An IPv6 host sends an IPv6 packet containing a Fragment header.
Requirement:
The IPv6 host MUST set the value in the Next Header Field in the Fragment header to the initial header type of the Fragmentable Part of the original packet.

Specification Text:



Next Header **8-bit selector. Identifies the initial header type of the Fragmentable Part of the original packet** (defined below). Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].

Reserved 8-bit reserved field. Initialized to zero for transmission; ignored on reception.

Fragment Offset 13-bit unsigned integer. The offset, in 8-octet units, of the data following this header, relative to the start of the Fragmentable Part of the original packet.

Res 2-bit reserved field. Initialized to zero for transmission; ignored on reception.

M flag 1 = more fragments; 0 = last fragment.

Identification 32 bits. See description below.

RQ_000_1069 Process Fragment Packets

RFC2460 4.5 MANDATORY

Applies to: Host

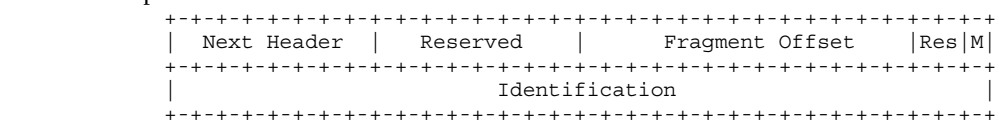
Context:

An IPv6 host receives an IPv6 packet containing a Fragment header

Requirement:

The IPv6 host MUST ignore the value of the Reserved Field and the Res field in the Fragment Header.

Specification Text:



Next Header 8-bit selector. Identifies the initial header type of the Fragmentable Part of the original packet (defined below). Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].

Reserved **8-bit reserved field. Initialized to zero for transmission; ignored on reception**.

Fragment Offset 13-bit unsigned integer. The offset, in 8-octet units, of the data following this header, relative to the start of the Fragmentable Part of the original packet.

Res **2-bit reserved field. Initialized to zero for transmission; ignored on reception**.

M flag 1 = more fragments; 0 = last fragment.

Identification 32 bits. See description below.

RQ_000_1070 Generate Fragment Packets

RFC2460 4.5 CONDITIONAL

[if RQ_000_1064 then MANDATORY]

Applies to: Host

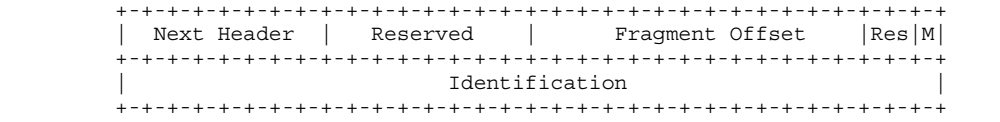
Context:

An IPv6 host sends an IPv6 packet containing a Fragment header.

Requirement:

The IPv6 host MUST set the value in the Fragment Offset field to the offset, in 8-octet units, of the data following this header, relative to the start of the fragmentable part of the original packet.

Specification Text:



```
Next Header          8-bit selector.  Identifies the initial header
                     type of the Fragmentable Part of the original
                     packet (defined below).  Uses the same values as
                     the IPv4 Protocol field [RFC-1700 et seq.].

Reserved             8-bit reserved field.  Initialized to zero for
                     transmission; ignored on reception.

Fragment Offset      13-bit unsigned integer.  The offset, in 8-octet
                     units, of the data following this header,
                     relative to the start of the Fragmentable Part
                     of the original packet.

Res                  2-bit reserved field.  Initialized to zero for
                     transmission; ignored on reception.

M flag               1 = more fragments; 0 = last fragment.

Identification       32 bits.  See description below.
```

RQ_000_1071 Generate Fragment Packets

RFC2460 4.5 CONDITIONAL

[if RQ_000_1064 then MANDATORY]

Applies to: Host

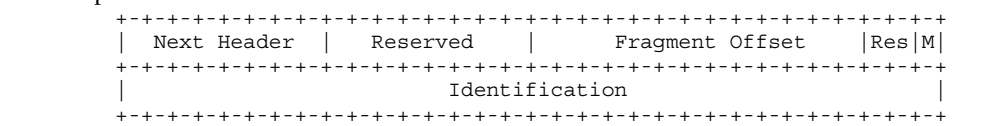
Context:

An IPv6 host sends an IPv6 packet containing a packet fragment which is not the final fragment.

Requirement:

The IPv6 host MUST set the M Flag in the Fragment header to the value 1.

Specification Text:



```
Next Header          8-bit selector.  Identifies the initial header
                     type of the Fragmentable Part of the original
                     packet (defined below).  Uses the same values as
                     the IPv4 Protocol field [RFC-1700 et seq.].

Reserved             8-bit reserved field.  Initialized to zero for
                     transmission; ignored on reception.

Fragment Offset      13-bit unsigned integer.  The offset, in 8-octet
                     units, of the data following this header,
                     relative to the start of the Fragmentable Part
                     of the original packet.

Res                  2-bit reserved field.  Initialized to zero for
                     transmission; ignored on reception.

M flag               1 = more fragments; 0 = last fragment.

Identification       32 bits.  See description below.
```

RQ_000_1072 Generate Fragment Packets

RFC2460 4.5 CONDITIONAL

[if RQ_000_1064 then MANDATORY]

Applies to: Host

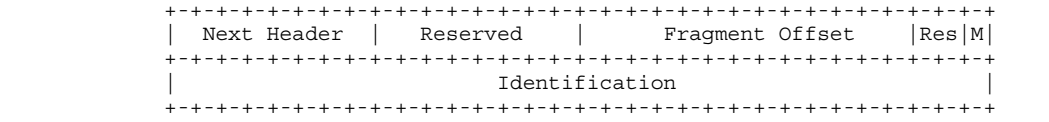
Context:

An IPv6 host sends an IPv6 packet containing a the final fragment of a fragmented packet.

Requirement:

The IPv6 host MUST set the M Flag in the Fragment header to the value zero (0).

Specification Text:



Next Header — 8-bit selector. Identifies the initial header type of the Fragmentable Part of the original packet (defined below). Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].

Reserved — 8-bit reserved field. Initialized to zero for transmission; ignored on reception.

Fragment Offset — 13-bit unsigned integer. The offset, in 8-octet units, of the data following this header, relative to the start of the Fragmentable Part of the original packet.

Res — 2-bit reserved field. Initialized to zero for transmission; ignored on reception.

M flag — 1 = more fragments; 0 = last fragment.

Identification — 32 bits. See description below.

RQ_000_1073 Generate Fragment Packets

RFC2460 4.5 CONDITIONAL
[if RQ_000_1064 then MANDATORY]

Applies to: Host

Context:

An IPv6 host sends an IPv6 packet containing a Fragment extension header.

Requirement:

The IPv6 host MUST set a value in the Identification field of the Fragment header which is different from that for any other fragmented packet sent recently with the same Source Address and final Destination Address.

Specification Text:

For every packet that is to be fragmented, the source node generates an Identification value. **The Identification must be different than that of any other fragmented packet sent recently* with the same Source Address and Destination Address**. If a Routing header is present, the Destination Address of concern is that of the final destination.

* "recently" means within the maximum likely lifetime of a packet, including transit time from source to destination and time spent awaiting reassembly with other fragments of the same packet. However, it is not required that a source node know the maximum packet lifetime. Rather, it is assumed that the requirement can be met by maintaining the Identification value as a simple, 32-bit, "wrap-around" counter, incremented each time a packet must be fragmented. It is an implementation choice whether to maintain a single counter for the node or multiple counters, e.g., one for each of the node's possible source addresses, or one for each active (source address, destination address) combination.

RQ_000_1077 Generate Extension Header Options

RFC2460 4.2 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node sends an IPv6 packet containing both an Authentication Header and a Hop-by-Hop Options extension header with the third-highest-order bit in its Option Type field set to the binary value '1'.

Requirement:

The IPv6 node treats the entire Option Data field as zero-valued octets when computing the packet's authenticating value.

Specification Text:

The third-highest-order bit of the Option Type specifies whether or not the Option Data of that option can change en-route to the packet's final destination. **When an Authentication header is present in the packet, for any option whose data may change en-route, its entire Option Data field must be treated as zero-valued octets when computing or verifying the packet's authenticating value.**

0 - Option Data does not change en-route

1 - Option Data may change en-route

RQ_000_1078 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing both an Authentication Header and a Destination Options extension header with the third-highest-order bit in its Option Type field set to the binary value '1'.
Requirement:
The IPv6 node treats the entire Option Data field as zero-valued octets when verifying the packet's authenticating value.
Specification Text:
The third-highest-order bit of the Option Type specifies whether or not the Option Data of that option can change en-route to the packet's final destination. **When an Authentication header is present in the packet, for any option whose data may change en-route, its entire Option Data field must be treated as zero-valued octets when computing or verifying the packet's authenticating value.**

0 - Option Data does not change en-route

1 - Option Data may change en-route

RQ_000_1079 Generate Fragment Packets
RFC2460 4.5 MANDATORY
Applies to: Host
Context:
An IPv6 host sends an IPv6 packet that is larger than the MTU on the path between itself and the packet's destination.
Requirement:
The IPv6 host MUST NOT fragment the IPv6 header or any extension headers that are likely to be processed by nodes en route to the destination.
Specification Text:
The initial, large, unfragmented packet is referred to as the "original packet", and it is considered to consist of two parts, as illustrated:

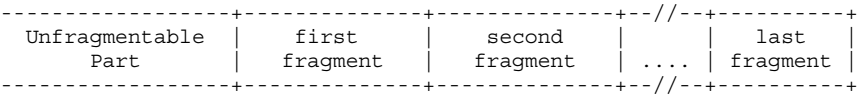
original packet:

The Unfragmentable Part consists of the IPv6 header plus any extension headers that must be processed by nodes en route to the destination, that is, all headers up to and including the Routing header if present, else the Hop-by-Hop Options header if present, else no extension headers.

The Fragmentable Part consists of the rest of the packet, that is, any extension headers that need be processed only by the final destination node(s), plus the upper-layer header and data.

The Fragmentable Part of the original packet is divided into fragments, each, except possibly the last ("rightmost") one, being an integer multiple of 8 octets long. The fragments are transmitted in separate "fragment packets" as illustrated:

original packet:



RQ_000_1080 Generate Fragment Packets
RFC2460 4.5 CONDITIONAL
[if RQ_000_1064 then MANDATORY]

Applies to: Host
Context:
An IPv6 host sends an IPv6 packet that is larger than the MTU on the path between itself and the packet's destination.
Requirement:
The IPv6 host MUST select the lengths of fragments such that the resulting fragment packets fit within the MTU of the path to the original packet's destination
Specification Text:
Each fragment packet is composed of:

(1) The Unfragmentable Part of the original packet, with the Payload Length of the original IPv6 header changed to contain the length of this fragment packet only (excluding the length of the IPv6 header itself), and the Next Header field of the last header of the Unfragmentable Part changed to 44.

(2) A Fragment header containing:

The Next Header value that identifies the first header of the Fragmentable Part of the original packet.

A Fragment Offset containing the offset of the fragment, in 8-octet units, relative to the start of the Fragmentable Part of the original packet. The Fragment Offset of the first ("leftmost") fragment is 0.

An M flag value of 0 if the fragment is the last ("rightmost") one, else an M flag value of 1.

The Identification value generated for the original packet.

(3) The fragment itself.

The lengths of the fragments must be chosen such that the resulting fragment packets fit within the MTU of the path to the packets' destination(s).

RQ_000_1081 Generate Fragment Packets
RFC2460 4.5 CONDITIONAL
[if RQ_000_1064 then MANDATORY]

Applies to: Host
Context:
An IPv6 host sends an IPv6 packet that is larger than the MTU on the path between itself and the packet's destination.
Requirement:
The IPv6 host MUST construct each fragment packet as follows:

(1) The Unfragmentable Part of the original packet
(2) A Fragment header
(3) The fragment itself.

Specification Text:
Each fragment packet is composed of:

(1) The Unfragmentable Part of the original packet, with the Payload Length of the original IPv6 header changed to contain the length of this fragment packet only (excluding the length of the IPv6 header itself), and the Next Header field of the last header of the Unfragmentable Part changed to 44.

(2) A Fragment header containing:

The Next Header value that identifies the first header of the Fragmentable Part of the original packet.

A Fragment Offset containing the offset of the fragment, in 8-octet units, relative to the start of the Fragmentable Part of the original packet. The Fragment Offset of the first ("leftmost") fragment is 0.

An M flag value of 0 if the fragment is the last ("rightmost") one, else an M flag value of 1.

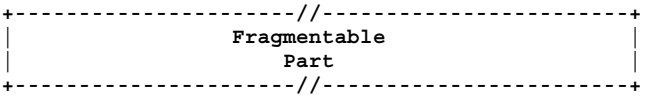
The Identification value generated for the original packet.

(3) The fragment itself.

The lengths of the fragments must be chosen such that the resulting fragment packets fit within the MTU of the path to the packets' destination(s).

RQ_000_1082 Process Fragment Packets
RFC2460 4.5 -10 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a series of IPv6 packets in each of which the Source Address field is set to the same value and the Destination Address field is set to the same value and each contains a Fragment extension header with the same value set in the Fragment Identification field
Requirement:
The IPv6 host MUST reassemble the packet fragments into their original, unfragmented form
Specification Text:
At the destination, fragment packets are reassembled into their original, unfragmented form, as illustrated:

reassembled original packet:



The following rules govern reassembly:

An original packet is reassembled only from fragment packets that have the same Source Address, Destination Address, and Fragment Identification.

The Unfragmentable Part of the reassembled packet consists of all headers up to, but not including, the Fragment header of the first fragment packet (that is, the packet whose Fragment Offset is zero), with the following two changes:

The Next Header field of the last header of the Unfragmentable Part is obtained from the Next Header field of the first fragment's Fragment header.

The Payload Length of the reassembled packet is computed from the length of the Unfragmentable Part and the length and offset of the last fragment. For example, a formula for computing the Payload Length of the reassembled original packet is:

```
PL.orig = PL.first - FL.first - 8 + (8 * FO.last) + FL.last

where
PL.orig  = Payload Length field of reassembled packet.
PL.first = Payload Length field of first fragment packet.
FL.first = length of fragment following Fragment header of
           first fragment packet.
FO.last  = Fragment Offset field of Fragment header of
           last fragment packet.
FL.last  = length of fragment following Fragment header of
           last fragment packet.
```

The Fragmentable Part of the reassembled packet is constructed from the fragments following the Fragment headers in each of the fragment packets. The length of each fragment is computed by subtracting from the packet's Payload Length the length of the headers between the IPv6 header and fragment itself; its relative position in Fragmentable Part is computed from its Fragment Offset value.

The Fragment header is not present in the final, reassembled packet.

RQ_000_1083 Process Fragment Packets
RFC2460 4.5 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a series of IPv6 packets in each of which the Source Address field is set to the same value and the Destination Address field is set to the same value and each contains a Fragment extension header with the same value set in the Fragment Identification field. Insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet.
Requirement:
The IPv6 host MUST abandon the reassembly of that packet and discard all the fragments that have been received for that packet.

Specification Text:

The following error conditions may arise when reassembling fragmented packets:

If insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded. If the first fragment (i.e., the one with a Fragment Offset of zero) has been received, an ICMP Time Exceeded -- Fragment Reassembly Time Exceeded message should be sent to the source of that fragment.

If the length of a fragment, as derived from the fragment packet's Payload Length field, is not a multiple of 8 octets and the M flag of that fragment is 1, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Payload Length field of the fragment packet.

If the length and offset of a fragment are such that the Payload Length of the packet reassembled from that fragment would exceed 65,535 octets, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Fragment Offset field of the fragment packet.

RQ_000_1084 Process Fragment Packets

RFC2460 4.5 RECOMMENDED

Applies to: Host

Context:

An IPv6 host receives a series of IPv6 packets in each of which the Source Address field is set to the same value and the Destination Address field is set to the same value and each contains a Fragment extension header with the same value set in the Fragment Identification field. Insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet but the first fragment packet (i.e., the one with a Fragment Offset of zero) is present in the set of received fragments.

Requirement:

The IPv6 host SHOULD send an ICMP Time Exceeded message with the Code field set to 1 (Fragment Reassembly Time Exceeded) to the Source Address set in the packet containing the first fragment.

Specification Text:

The following error conditions may arise when reassembling fragmented packets:

If insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded. If the first fragment (i.e., the one with a Fragment Offset of zero) has been received, an ICMP Time Exceeded -- Fragment Reassembly Time Exceeded message should be sent to the source of that fragment.

If the length of a fragment, as derived from the fragment packet's Payload Length field, is not a multiple of 8 octets and the M flag of that fragment is 1, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Payload Length field of the fragment packet.

If the length and offset of a fragment are such that the Payload Length of the packet reassembled from that fragment would exceed 65,535 octets, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Fragment Offset field of the fragment packet.

RQ_000_1085 Process Fragment Packets
RFC2460 4.5 MANDATORY
Applies to: Host
Context:
An IPv6 host receives an IPv6 packet containing a Fragment extension header in which the M-Flag is set to the value 1 but the length of the fragment itself is not a multiple of 8 octets.
Requirement:
The IPv6 host MUST discard the fragment.
Specification Text:
The following error conditions may arise when reassembling fragmented packets:

If insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded. If the first fragment (i.e., the one with a Fragment Offset of zero) has been received, an ICMP Time Exceeded -- Fragment Reassembly Time Exceeded message should be sent to the source of that fragment.

If the length of a fragment, as derived from the fragment packet's Payload Length field, is not a multiple of 8 octets and the M flag of that fragment is 1, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Payload Length field of the fragment packet.

If the length and offset of a fragment are such that the Payload Length of the packet reassembled from that fragment would exceed 65,535 octets, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Fragment Offset field of the fragment packet.

RQ_000_1086 Process Fragment Packets
RFC2460 4.5 MANDATORY
Applies to: Host
Context:
An IPv6 host receives an IPv6 packet containing a Fragment extension header and the value set in the Packet Length field within the IPv6 header when combined with the value set in the Fragment Offset field of the Fragment header would result in the Payload Length of the reassembled packet exceeding 65,535 octets.
Requirement:
The IPv6 host MUST discard fragment packet.
Specification Text:
The following error conditions may arise when reassembling fragmented packets:

If insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded. If the first fragment (i.e., the one with a Fragment Offset of zero) has been received, an ICMP Time Exceeded -- Fragment Reassembly Time Exceeded message should be sent to the source of that fragment.

If the length of a fragment, as derived from the fragment packet's Payload Length field, is not a multiple of 8 octets and the M flag of that fragment is 1, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Payload Length field of the fragment packet.

If the length and offset of a fragment are such that the Payload Length of the packet reassembled from that fragment would exceed 65,535 octets, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Fragment Offset field of the fragment packet.

RQ_000_1087 Process Fragment Packets
RFC2460 4.5 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a series of IPv6 packets in each of which the Source Address field is set to the same value and the Destination Address field is set to the same value and each contains a Fragment extension header with the same value set in the Fragment Identification field . However, the number and content of the headers preceding the Fragment header of different fragments of the same original packet differ.
Requirement:
The IPv6 host MUST processes the headers that precede the Fragment header in each fragment packet prior to queueing the fragments for reassembly.
Specification Text:
The following conditions are not expected to occur, but are not considered errors if they do:

The number and content of the headers preceding the Fragment header of different fragments of the same original packet may differ. Whatever headers are present, preceding the Fragment header in each fragment packet, are processed when the packets arrive, prior to queueing the fragments for reassembly. Only those headers in the Offset zero fragment packet are retained in the reassembled packet.

The Next Header values in the Fragment headers of different fragments of the same original packet may differ. Only the value from the Offset zero fragment packet is used for reassembly.

RQ_000_1088 Process Fragment Packets
RFC2460 4.5 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a series of IPv6 packets in each of which the Source Address field is set to the same value and the Destination Address field is set to the same value and each contains a Fragment extension header with the same value set in the Fragment Identification field . However, the Next Header values in the Fragment headers of different fragments of the same original packet differ.
Requirement:
The IPv6 host MUST include in the reassembled packet only the Next Header value that was received in the Offset zero fragment packet.
Specification Text:
The following conditions are not expected to occur, but are not considered errors if they do:

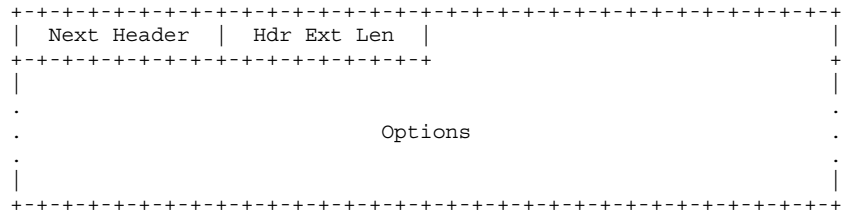
The number and content of the headers preceding the Fragment header of different fragments of the same original packet may differ. Whatever headers are present, preceding the Fragment header in each fragment packet, are processed when the packets arrive, prior to queueing the fragments for reassembly. Only those headers in the Offset zero fragment packet are retained in the reassembled packet.

The Next Header values in the Fragment headers of different fragments of the same original packet may differ. Only the value from the Offset zero fragment packet is used for reassembly.

RQ_000_1089 Generate Destination Options Header
RFC2460 4.6 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet containing a Destination Options extension header.
Requirement:
The IPv6 node MUST set the appropriate Next Header field (either in the IPv6 Header or in the extension header immediately preceding the Destination Options extension header) to the value sixty (60).

Specification Text:

The Destination Options header is used to carry optional information that need be examined only by a packet's destination node(s). **The Destination Options header is identified by a Next Header value of 60 in the immediately preceding header**, and has the following format:



Next Header	8-bit selector. Identifies the type of header immediately following the Destination Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Hdr Ext Len	8-bit unsigned integer. Length of the Destination Options header in 8-octet units, not including the first 8 octets.
Options	Variable-length field, of length such that the complete Destination Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options, as described in section 4.2.

RQ_000_1090 Generate Destination Options Header

RFC2460 4.6 MANDATORY

Applies to: Host, Router

Context:

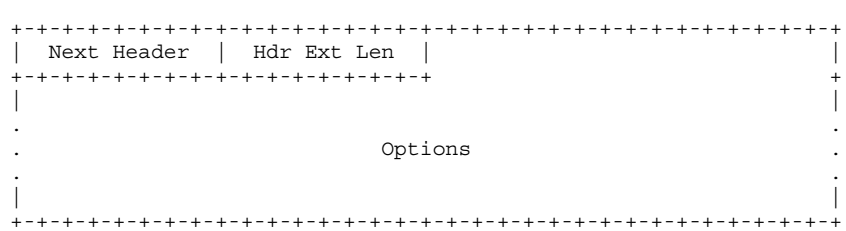
An IPv6 node sends an IPv6 packet containing a Destination Options header.

Requirement:

The IPv6 node MUST set the value of the Next Header Field in the Destination Options header to the value associated with the type of the header immediately following the Destinations Options header (as defined in RFC-1700 and RFC-2460).

Specification Text:

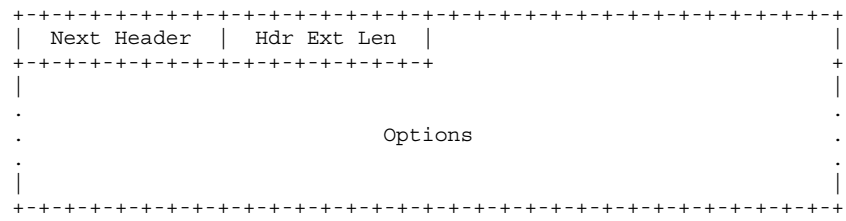
The Destination Options header is used to carry optional information that need be examined only by a packet's destination node(s). The Destination Options header is identified by a Next Header value of 60 in the immediately preceding header, and has the following format:



Next Header	**8-bit selector. Identifies the type of header immediately following the Destination Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].**
Hdr Ext Len	8-bit unsigned integer. Length of the Destination Options header in 8-octet units, not including the first 8 octets.
Options	Variable-length field, of length such that the complete Destination Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options, as described in section 4.2.

RQ_000_1091 Generate Destination Options Header
RFC2460 4.6 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet containing a Destination Options header.
Requirement:

The IPv6 node MUST set the value of the Hdr Ext Len field in the Destination Options header to the length of the header in 8-octet units, not including the first 8 octets
Specification Text:
The Destination Options header is used to carry optional information that need be examined only by a packet's destination node(s). The Destination Options header is identified by a Next Header value of 60 in the immediately preceding header, and has the following format:



Next Header 8-bit selector. Identifies the type of header immediately following the Destination Options header. Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].

Hdr Ext Len **8-bit unsigned integer. Length of the Destination Options header in 8-octet units, not including the first 8 octets**.

Options Variable-length field, of length such that the complete Destination Options header is an integer multiple of 8 octets long. Contains one or more TLV-encoded options, as described in section 4.2.

RQ_000_1092 Generate Extension Headers
RFC2460 4.7 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet
Requirement:
The IPv6 node MUST set the value 59 in the Next Header field of the final header in the IPv6 packet
Specification Text:
The value 59 in the Next Header field of an IPv6 header or any extension header indicates that there is nothing following that header. If the Payload Length field of the IPv6 header indicates the presence of octets past the end of a header whose Next Header field contains 59, those octets must be ignored, and passed on unchanged if the packet is forwarded.

RQ_000_1093 Process Extension Headers
RFC2460 4.7 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet in which the value fifty-nine (59) is set into either the IPv6 header or an extension header.
Requirement:
The IPv6 node MUST ignore and, if forwarding the packet, pass on unchanged, the octets beyond the end of the header whose Next Header field contains 59.
Specification Text:
The value 59 in the Next Header field of an IPv6 header or any extension header indicates that there is nothing following that header. **If the Payload Length field of the IPv6 header indicates the presence of octets past the end of a header whose Next Header field contains 59, those octets must be ignored, and passed on unchanged if the packet is forwarded**.

RQ_000_1095 Determine Default MTU
RFC2460 5 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST be able to transmit an IPv6 packet of 1280 octets without fragmentation
Specification Text:
IPv6 requires that every link in the internet have an MTU of 1280 octets or greater. On any link that cannot convey a 1280-octet packet in one piece, link-specific fragmentation and reassembly must be provided at a layer below IPv6.

Links that have a configurable MTU (for example, PPP links [RFC- 1661]) must be configured to have an MTU of at least 1280 octets; it is recommended that they be configured with an MTU of 1500 octets or greater, to accommodate possible encapsulations (i.e., tunneling) without incurring IPv6-layer fragmentation.

RQ_000_1096 Determine Default MTU
RFC2460 5 RECOMMENDED
Applies to: Host
Context:

Requirement:
An IPv6 host SHOULD be able to transmit an IPv6 packet of 1500 octets or greater without fragmentation
Specification Text:
IPv6 requires that every link in the internet have an MTU of 1280 octets or greater. On any link that cannot convey a 1280-octet packet in one piece, link-specific fragmentation and reassembly must be provided at a layer below IPv6.

Links that have a configurable MTU (for example, PPP links [RFC- 1661]) must be configured to have an MTU of at least 1280 octets; **it is recommended that they be configured with an MTU of 1500 octets or greater, to accommodate possible encapsulations (i.e., tunneling) without incurring IPv6-layer fragmentation**.

RQ_000_1097 Process IPv6 Packet
RFC2460 5 MANDATORY
Applies to: Router, Host
Context:

Requirement:
On each link to which it is attached, an IPv6 host MUST be able to accept IPv6 packets up to the size of the MTU of the link.
Specification Text:
From each link to which a node is directly attached, the node must be able to accept packets as large as that link's MTU.

RQ_000_1098 Discover PMTU
RFC2460 5 RECOMMENDED
Applies to: Router, Host
Context:

Requirement:
An IPv6 node SHOULD implement Path MTU Discovery as specified in IETF RFC-1661.
Specification Text:
It is strongly recommended that IPv6 nodes implement Path MTU Discovery [RFC-1981], in order to discover and take advantage of path MTUs greater than 1280 octets. However, a minimal IPv6 implementation (e.g., in a boot ROM) may simply restrict itself to sending packets no larger than 1280 octets, and omit implementation of Path MTU Discovery.

RQ_000_1100 Process Fragment Packets
RFC2460 5 MANDATORY
Applies to: Host
Context:
An IPv6 host receives the fragment packets of an original packet of 1500 octets or less.
Requirement:
The IPv6 host MUST reassemble the fragments into the original unfragmented packet.
Specification Text:
A node must be able to accept a fragmented packet that, after reassembly, is as large as 1500 octets.

RQ_000_1101 Process Fragment Packets
RFC2460 5 OPTIONAL
Applies to: Host
Context:
An IPv6 host receives the fragment packets of an original packet of greater than 1500 octets.
Requirement:
The IPv6 host MAY reassemble the fragments into the original unfragmented packet.
Specification Text:
A node is permitted to accept fragmented packets that reassemble to more than 1500 octets.

RQ_000_1103 Generate Fragment Packets
RFC2460 5 CONDITIONAL
[if RQ_000_1064 then MANDATORY]
Applies to: Host
Context:
Having sent an IPv6 packet to an IPv4 destination, an IPv6 host receives an ICMP "Packet Too Big" message.
Requirement:
The IPv6 host MUST include a Fragment header in subsequent packets with a suitable Identification value to use in resulting IPv4 fragments.
Specification Text:
In response to an IPv6 packet that is sent to an IPv4 destination (i.e., a packet that undergoes translation from IPv6 to IPv4), the originating IPv6 node may receive an ICMP Packet Too Big message reporting a Next-Hop MTU less than 1280. In that case, **the IPv6 node is not required to reduce the size of subsequent packets to less than 1280, but must include a Fragment header in those packets so that the IPv6-to-IPv4 translating router can obtain a suitable Identification value to use in resulting IPv4 fragments**. Note that this means the payload may have to be reduced to 1232 octets (1280 minus 40 for the IPv6 header and 8 for the Fragment header), and smaller still if additional extension headers are used.

RQ_000_1106 Generate Flow Label
RFC2460 6 OPTIONAL
Applies to: Host
Context:

Requirement:
An IPv6 host MAY use the Flow Label field in the IPv6 header to identify sequences of packets which require special handling by the IPv6 routers along the path to the destination.
Specification Text:
The 20-bit Flow Label field in the IPv6 header may be used by a source to label sequences of packets for which it requests special handling by the IPv6 routers, such as non-default quality of service or "real-time" service. This aspect of IPv6 is, at the time of writing, still experimental and subject to change as the requirements for flow support in the Internet become clearer.

RQ_000_1107 Generate Flow Label
RFC2460 6 MANDATORY
Applies to: Host
Context:
An IPv6 host that does not support the functions of the Flow Label sends a packet.
Requirement:
The IPv6 host MUST set the Flow Label field in the IPv6 header to zero (0).
Specification Text:
Hosts or routers that do not support the functions of the Flow Label field are required to set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

RQ_000_1108 Process Flow Label
RFC2460 6 MANDATORY
Applies to: Router
Context:
An IPv6 router that does not support the functions of the Flow Label field receives a packet.
Requirement:
The IPv6 Router MUST pass on the packet with the Flow Label field unchanged.
Specification Text:
Hosts or routers that do not support the functions of the Flow Label field are required to set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

RQ_000_1109 Process Flow Label
RFC2460 6 MANDATORY
Applies to: Host
Context:
An IPv6 host that does not support the functions of the Flow Label receives an IPv6 packet.
Requirement:
The IPv6 host MUST ignore the contents Flow Label field.
Specification Text:
Hosts or routers that do not support the functions of the Flow Label field are required to set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

RQ_000_1119 Process Traffic Class
RFC2460 7 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet.
Requirement:
The IPv6 node SHOULD ignore and leave unchanged any bits of the Traffic Class field in the IPv6 header for which it does not support a specific use.
Specification Text:
Nodes should ignore and leave unchanged any bits of the Traffic Class field for which they do not support a specific use.

RQ_000_1122 Process Checksum
RFC2460 8.1 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing an encapsulated UDP packet which has its UDP checksum field set to zero (0).
Requirement:
The IPv6 node MUST discard the UDP packet.
Specification Text:
- Unlike IPv4, when UDP packets are originated by an IPv6 node, the UDP checksum is not optional. That is, whenever originating a UDP packet, an IPv6 node must compute a UDP checksum over the packet and the pseudo-header, and, if that computation yields a result of zero, it must be changed to hex FFFF for placement in the UDP header. **IPv6 receivers must discard UDP packets containing a zero checksum**, and should log the error.

RQ_000_1123 Process Checksum
RFC2460 8.1, 5 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet containing an encapsulated UDP packet which has its UDP checksum field set to zero (0).
Requirement:
The IPv6 node SHOULD record the event in its error log.
Specification Text:
- Unlike IPv4, when UDP packets are originated by an IPv6 node, the UDP checksum is not optional. That is, whenever originating a UDP packet, an IPv6 node must compute a UDP checksum over the packet and the pseudo-header, and, if that computation yields a result of zero, it must be changed to hex FFFF for placement in the UDP header. **IPv6 receivers** must discard UDP packets containing a zero checksum, **and should log the error**.

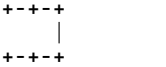
RQ_000_1132 Generate Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet containing both an Authentication Header and a Destination Options extension header with the third-highest-order bit in its Option Type field set to the binary value '1'.
Requirement:
The IPv6 node MUST treat the entire Option Data field as zero-valued octets when computing the packet's authenticating value.
Specification Text:
The third-highest-order bit of the Option Type specifies whether or not the Option Data of that option can change en-route to the packet's final destination. **When an Authentication header is present in the packet, for any option whose data may change en-route, its entire Option Data field must be treated as zero-valued octets when computing or verifying the packet's authenticating value.**

0 - Option Data does not change en-route

1 - Option Data may change en-route

RQ_000_1133 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing a Destination Options extension header having its Option Type field set to zero (Pad1 option)
Requirement:
The IPv6 node MUST process the Pad1 option as a padding octet.
Specification Text:
There are two padding options which are used when necessary to align subsequent options pad out the containing header to a multiple of 8 octets in length. These padding options must be recognized by all IPv6 implementations:

Pad1 option (alignment requirement: none)



The Pad1 option is used to insert one octet of padding into the Options area of a header. If more than one octet of padding is required, the PadN option, described next, should be used, rather than multiple Pad1 options.

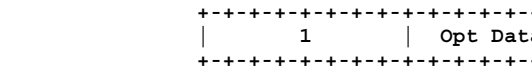
RQ_000_1134 Generate Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet containing a Destination Options extension header which requires one octet of padding to ensure correct 8-octet alignment within the options extension header.
Requirement:
The IPv6 node MUST include an option in the Hop-by-Hop Options extension header with its Option Type field set to zero (Pad1) and with no option Data Length field and no option Data field.
Specification Text:
There are two padding options which are used when necessary to align subsequent options pad out the containing header to a multiple of 8 octets in length. These padding options must be recognized by all IPv6 implementations:

Pad1 option (alignment requirement: none)

The Pad1 option is used to insert one octet of padding into the Options area of a header. If more than one octet of padding is required, the PadN option, described next, should be used, rather than multiple Pad1 options.

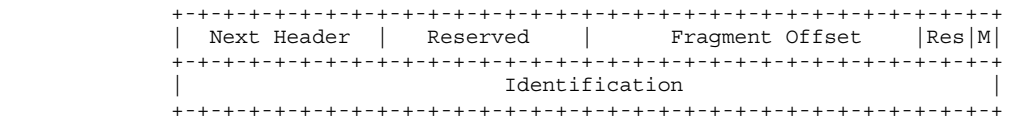
RQ_000_1135 Generate Extension Header Options
RFC2460 4.2 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node sends an IPv6 packet containing a Destination Options extension header which requires more than one octet of padding to ensure correct 8-octet alignment within the options extension header.
Requirement:
The IPv6 node SHOULD include an option in the Destination Options extension header with its Option Type field set to the value 1 (PadN), its Option Data Length field set to a value two less than the required number of padding bytes and its Option Data field containing that number of zero-valued octets.
Specification Text:
The Pad1 option is used to insert one octet of padding into the Options area of a header. **If more than one octet of padding is required, the PadN ion, described next, should be used, rather than multiple Pad1 options.**

PadN option (alignment requirement: none)



The PadN option is used to insert two or more octets of padding into the Options area of a header. For N octets of padding, the Opt Data Len field contains the value N-2, and the Option Data consists of N-2 zero-valued octets.

RQ_000_1136 Process Extension Headers
RFC2460 4.5 MANDATORY
Applies to: Host
Context:
An IPv6 host sends an IPv6 packet containing a Fragment header
Requirement:
The IPv6 host MUST set the value in both the Reserved field and the Res field to zero (0).
Specification Text:



Next Header	8-bit selector. Identifies the initial header type of the Fragmentable Part of the original packet (defined below). Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Reserved	**8-bit reserved field. Initialized to zero for transmission; ignored on reception.**
Fragment Offset	13-bit unsigned integer. The offset, in 8-octet units, of the data following this header, relative to the start of the Fragmentable Part of the original packet.
Res	**2-bit reserved field. Initialized to zero for transmission; ignored on reception.**
M flag	1 = more fragments; 0 = last fragment.
Identification	32 bits. See description below.

RQ_000_1137 Process Extension Headers
RFC2460 4.5 OPTIONAL
Applies to: Host
Context:
An IPv6 host sends an IPv6 packet that is larger than the MTU on the path between itself and the packet's destination.
Requirement:
The IPv6 host MAY any extension headers that need to be processed only by the final destination node(s) plus the upper-layer header and data.
Specification Text:
The initial, large, unfragmented packet is referred to as the "original packet", and it is considered to consist of two parts, as illustrated:

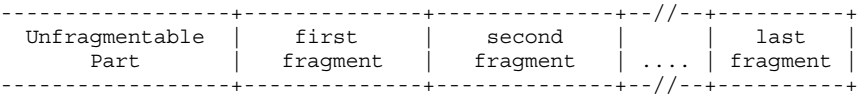
original packet:

The Unfragmentable Part consists of the IPv6 header plus any extension headers that must be processed by nodes en route to the destination, that is, all headers up to and including the Routing header if present, else the Hop-by-Hop Options header if present, else no extension headers.

The Fragmentable Part consists of the rest of the packet, that is, any extension headers that need be processed only by the final destination node(s), plus the upper-layer header and data.

The Fragmentable Part of the original packet is divided into fragments, each, except possibly the last ("rightmost") one, being an integer multiple of 8 octets long. The fragments are transmitted in separate "fragment packets" as illustrated:

original packet:



RQ_000_1138 Process Fragment Packets
RFC2460 4.5 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a series of IPv6 packets in each of which the Source Address field is set to the same value and the Destination Address field is set to the same value and each contains a Fragment extension header with the same value set in the Fragment Identification field . However, the number and content of the headers preceding the Fragment header of different fragments of the same original packet differ.
Requirement:
The IPv6 host MUST include in the reassembled packet only those headers that were received in the Offset zero fragment packet.

Specification Text:
The following conditions are not expected to occur, but are not considered errors if they do:

The number and content of the headers preceding the Fragment header of different fragments of the same original packet may differ. Whatever headers are present, preceding the Fragment header in each fragment packet, are processed when the packets arrive, prior to queueing the fragments for reassembly. **Only those headers in the Offset zero fragment packet are retained in the reassembled packet**.

The Next Header values in the Fragment headers of different fragments of the same original packet may differ. Only the value from the Offset zero fragment packet is used for reassembly.

RQ_000_9003 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet containing a Hop-by-Hop Options extension header in which the Option Type field is set to an unrecognized value but with its highest-order two bits set to the binary value '11' and the Destination Address field contains a multicast address.
Requirement:
The IPv6 node MUST discard the packet.
Specification Text:
The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type:

00 - skip over this option and continue processing the header.

01 - discard the packet.

10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

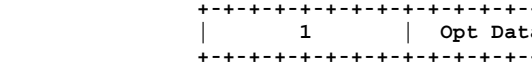
11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RQ_000_9004 Process Extension Header Options
RFC2460 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet containing a Hop-by-Hop Options extension header having its Option Type field set to one (PadN option)
Requirement:
The IPv6 node MUST process the PadN option as a padding octets.
Specification Text:
There are two padding options which are used when necessary to align subsequent options pad out the containing header to a multiple of 8 octets in length. **These padding options must be recognized by all IPv6 implementations:**

Pad1 option (alignment requirement: none)

The Pad1 option is used to insert one octet of padding into the Options area of a header. If more than one octet of padding is required, the PadN option, described next, should be used, rather than multiple Pad1 options.

PadN option (alignment requirement: none)



The PadN option is used to insert two or more octets of padding into the Options area of a header. For N octets of padding, the Opt Data Len field contains the value N-2, and the Option Data consists of N-2 zero-valued octets.

RQ_000_9006 Process Fragment Packets
RFC2460 4.5, 41 RECOMMENDED
Applies to: Host
Context:
An IPv6 host receives an IPv6 packet containing a Fragment extension header in which the M-Flag is set to the value 1 but the length of the fragment itself is not a multiple of 8 octets.
Requirement:
The IPv6 host SHOULD send an ICMP Parameter Problem message to the Source Address of the fragment with the Code field set to the value zero (0) and the Pointer field set to the offset (in octets) of the Payload Length field within the fragment packet.
Specification Text:
The following error conditions may arise when reassembling fragmented packets:

If insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded. If the first fragment (i.e., the one with a Fragment Offset of zero) has been received, an ICMP Time Exceeded -- Fragment Reassembly Time Exceeded message should be sent to the source of that fragment.

If the length of a fragment, as derived from the fragment packet's Payload Length field, is not a multiple of 8 octets and the M flag of that fragment is 1, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Payload Length field of the fragment packet.

If the length and offset of a fragment are such that the Payload Length of the packet reassembled from that fragment would exceed 65,535 octets, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Fragment Offset field of the fragment packet.

RQ_000_9007 Process Fragment Packets
RFC2460 4.5 RECOMMENDED
Applies to: Host
Context:
An IPv6 host receives an IPv6 packet containing a Fragment extension header and the value set in the Packet Length field within the IPv6 header when combined with the value set in the Fragment Offset field of the Fragment header would result in the Payload Length of the reassembled packet exceeding 65,535 octets.
Requirement:
The IPv6 host SHOULD send an ICMP Parameter Problem message to the Source Address of the fragment with the Code field set to the value zero (0) and the Pointer field set to the offset (in octets) of the Fragment Offset field within the fragment packet.
Specification Text:
The following error conditions may arise when reassembling fragmented packets:

If insufficient fragments are received to complete reassembly of a packet within 60 seconds of the reception of the first-arriving fragment of that packet, reassembly of that packet must be abandoned and all the fragments that have been received for that packet must be discarded. If the first fragment (i.e., the one with a Fragment Offset of zero) has been received, an ICMP Time Exceeded -- Fragment Reassembly Time Exceeded message should be sent to the source of that fragment.

If the length of a fragment, as derived from the fragment packet's Payload Length field, is not a multiple of 8 octets and the M flag of that fragment is 1, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Payload Length field of the fragment packet.

If the length and offset of a fragment are such that the Payload Length of the packet reassembled from that fragment would exceed 65,535 octets, then that fragment must be discarded and an ICMP Parameter Problem, Code 0, message should be sent to the source of the fragment, pointing to the Fragment Offset field of the fragment packet.

4.6 Requirements extracted from RFC 2461

RQ_000_8101 Discover Neighbor by Redirect Message
RFC2461 2.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST consider an IPv6 address to be on-link if it receives a the address in the Target Address filed of a Redirect message.
Specification Text:

on-link - an address that is assigned to an interface on a specified link. A node considers an address to be on-link if:

- it is covered by one of the link's prefixes, or

- **a neighboring router specifies the address as the target of a Redirect message,** or

- a Neighbor Advertisement message is received for the (target) address, or

- any Neighbor Discovery message is received from the address.

RQ_000_8102 Discover Neighbor by NA
RFC2461 2.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST consider an IPv6 address to be on-link if it receives a the address in the Target Address filed of a Neighbor Advertisement message.
Specification Text:

on-link - an address that is assigned to an interface on a specified link. A node considers an address to be on-link if:

- it is covered by one of the link's prefixes, or

- a neighboring router specifies the address as the target of a Redirect message, or

- **a Neighbor Advertisement message is received for the (target) address,** or

- any Neighbor Discovery message is received from the address.

RQ_000_8103 Neighbor Discovery
RFC2461 2.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST consider an IPv6 address to be on-link if it receives any Neighbor Discovery message from that address.
Specification Text:

on-link - an address that is assigned to an interface on a specified link. A node considers an address to be on-link if:

- it is covered by one of the link's prefixes, or

- a neighboring router specifies the address as the target of a Redirect message, or

- a Neighbor Advertisement message is received for the (target) address, or

- **any Neighbor Discovery message is received from the address.**

RQ_000_8107 Form Link-local Address
RFC2461 2.3 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST ensure that each of its interfaces have a link-local address assigned to it.
Specification Text:
link-local address
- a unicast address having link-only scope that can be used to reach neighbors. **All interfaces on routers MUST have a link-local address.** Also, RFC 2462 requires that interfaces on hosts have a link-local address.

RQ_000_8108 Form Link-local Address
RFC2461 2.3 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST ensure that each of its interfaces have a link-local address assigned to it.
Specification Text:
link-local address
- a unicast address having link-only scope that can be used to reach neighbors. All interfaces on routers MUST have a link-local address. **Also, RFC 2462 requires that interfaces on hosts have a link-local address.**

RQ_000_8111 Generate Router Advertisement
RFC2461 3 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST periodically send Router advertisement messages to each of its multicast-capable links

Specification Text:
On multicast-capable links, each router periodically multicasts a Router Advertisement packet announcing its availability. A host receives Router Advertisements from all routers, building a list of default routers. Routers generate Router Advertisements frequently enough that hosts will learn of their presence within a few minutes, but not frequently enough to rely on an absence of advertisements to detect router failure; a separate Neighbor Unreachability Detection algorithm provides failure detection.

RQ_000_8112 Router Processing of RS
RFC2461 3 MANDATORY
Applies to: Router
Context:
An IPv6 router receives a Router Solicitation message.
Requirement:
The IPv6 router MUST send a Router Advertisement message to indicate its presence together with various link and Internet parameters.
Specification Text:
Router Advertisement: Routers advertise their presence together with various link and Internet parameters either periodically, **or in response to a Router Solicitation message.** Router Advertisements contain prefixes that are used for on-link determination and/or address configuration, a suggested hop limit value, etc.

RQ_000_8113 Generate NS for Address Resolution
RFC2461 3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST send a Neighbor Solicitation message in order to determine the link-layer address of a neighboring node.
Specification Text:
Neighbor Solicitation: **Sent by a node to determine the link-layer address of a neighbor**, or to verify that a neighbor is still reachable via a cached link-layer address. Neighbor Solicitations are also used for Duplicate Address Detection.

RQ_000_8114 Generate NS for Address Resolution
RFC2461 3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST send a Neighbor Solicitation message in order to verify that a neighboring node is still reachable on a known link-layer address.
Specification Text:
Neighbor Solicitation: **Sent by a node** to determine the link-layer address of a neighbor, or **to verify that a neighbor is still reachable via a cached link-layer address**. Neighbor Solicitations are also used for Duplicate Address Detection.

RQ_000_8115 Process Neighbor Solicitation
RFC2461 3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a Neighbor Solicitation message.
Requirement:
The IPv6 node MUST send a Neighbor Advertisement message in response.
Specification Text:
Neighbor Advertisement: **A response to a Neighbor Solicitation message.** A node may also send unsolicited Neighbor Advertisements to announce a link-layer address change.

RQ_000_8116 Generate Unsolicited Neighbor Advertisement
RFC2461 3 OPTIONAL
Applies to: Host, Router
Context:
A link-layer addresses has been changed for an interface belonging to an IPv6 node
Requirement:
The IPv6 node MAY send an unsolicited Neighbor Advertisement message to announce the link-layer address change.
Specification Text:
Neighbor Advertisement: A response to a Neighbor Solicitation message. **A node may also send unsolicited Neighbor Advertisements to announce a link-layer address change.**

RQ_000_8117 Generate Redirect Message
RFC2461 3 RECOMMENDED
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet from a local host. It is not the destination node and a better first hope node exists.
Requirement:
The IPv6 router SHOULD send a Redirect message in response to the received packet informing the local host of the better first hop node for the particular destination.
Specification Text:
Redirect: **How a router informs a host of a better first-hop node to reach a particular destination.**

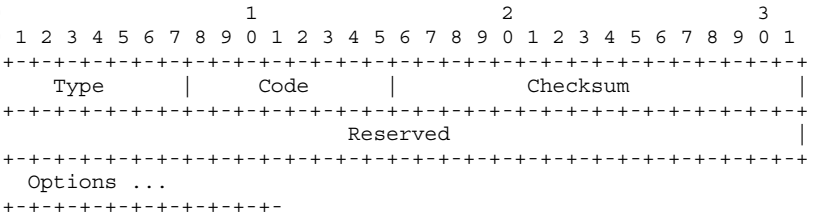
RQ_000_8118 Generate Router Advertisement
RFC2461 3 OPTIONAL
Applies to: Router
Context:

Requirement:
An IPv6 router MAY omit the source link-layer address from the options in a Router Advertisement packet.
Specification Text:
Inbound load balancing - Nodes with replicated interfaces may want to load balance the reception of incoming packets across multiple network interfaces on the same link. Such nodes have multiple link-layer addresses assigned to the same interface. For example, a single network driver could represent multiple network interface cards as a single logical interface having multiple link-layer addresses.

Load balancing is handled by allowing routers to omit the source link-layer address from Router Advertisement packets, thereby forcing neighbors to use Neighbor Solicitation messages to learn link-layer addresses of routers. Returned Neighbor Advertisement messages can then contain link-layer addresses that differ depending on who issued the solicitation.

RQ_000_8124 Generate Router Solicitation
RFC2461 4.1 OPTIONAL
Applies to: Host
Context:

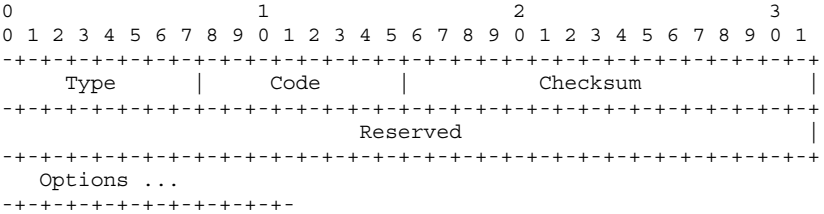
Requirement:
An IPv6 host MAY send a Router Solicitation packet at any time
Specification Text:
Hosts send Router Solicitations in order to prompt routers to generate Router Advertisements quickly.



RQ_000_8125 Generate Router Solicitation Header
RFC2461 4.1 MANDATORY
Applies to: Host
Context:

Requirement:
When constructing a Router Solicitation message, an IPv6 host MUST insert the IP address assigned to the sending interface into the Source Address field of the IPv6 Packet Header if an address has been assigned to the interface.
Specification Text:
Router Solicitation Message Format

..



IP Fields:

Source Address
An IP address assigned to the sending interface, or the unspecified address if no address is assigned to the sending interface.

Destination Address
Typically the all-routers multicast address.

Hop Limit 255

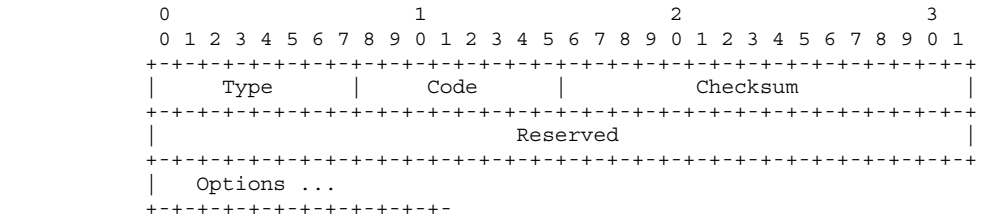
Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header.

RQ_000_8126 Generate Router Solicitation Header
RFC2461 4.1 MANDATORY
Applies to: Host
Context:

Requirement:
When constructing a Router Solicitation message, an IPv6 host MUST insert the IPv6 unspecified address (0:0:0:0:0:0:0:0) into the Source Address field of the IPv6 Packet Header if no IP address has been assigned to the sending interface.

Specification Text:
Router Solicitation Message Format

..



IP Fields:

Source Address
An IP address assigned to the sending interface, **or the unspecified address if no address is assigned to the sending interface.**

Destination Address
Typically the all-routers multicast address.

Hop Limit 255

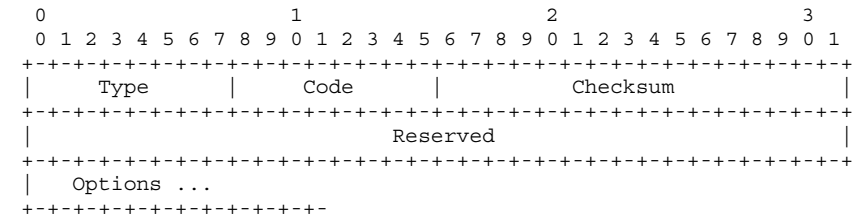
Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header.

RQ_000_8127 Generate Router Solicitation Header
RFC2461 4.1 RECOMMENDED
Applies to: Host
Context:

Requirement:
When constructing a Router Solicitation message, an IPv6 host SHOULD insert the IPv6 link-local all-routers multicast address (FF02:0:0:0:0:0:0:2) into the Destination Address field of the IPv6 Packet Header

Specification Text:
Router Solicitation Message Format

..



IP Fields:

Source Address
An IP address assigned to the sending interface, or the unspecified address if no address is assigned to the sending interface.

Destination Address
Typically the all-routers multicast address.

Hop Limit 255

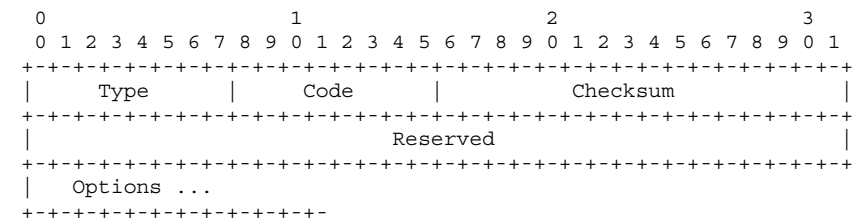
Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header.

RQ_000_8128 Generate Router Solicitation Header
RFC2461 4.1 MANDATORY
Applies to: Host
Context:

Requirement:
When constructing a Router Solicitation message, an IPv6 host MUST set Hop Limit field of the IPv6 Packet Header to the decimal value 255.

Specification Text:
Router Solicitation Message Format

..



IP Fields:

Source Address
An IP address assigned to the sending interface, or the unspecified address if no address is assigned to the sending interface.

Destination Address
Typically the all-routers multicast address.

Hop Limit 255

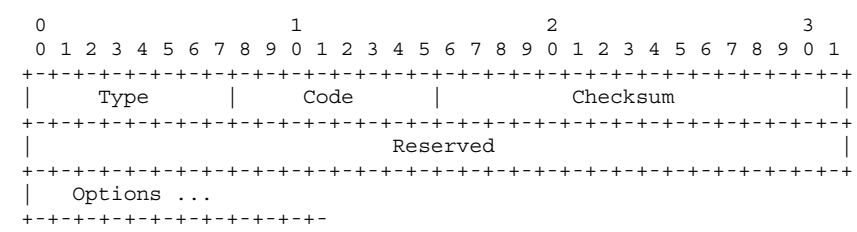
Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header.

RQ_000_8129 Generate Router Solicitation Header
RFC2461 4.1 RECOMMENDED
Applies to: Host
Context:

Requirement:
When constructing a Router Solicitation message, an IPv6 host SHOULD include an Authentication Header in the IPv6 packet if an AH-based Security Association exists between the IPv6 node and the destination address.

Specification Text:
Router Solicitation Message Format

..



IP Fields:

Source Address
An IP address assigned to the sending interface, or the unspecified address if no address is assigned to the sending interface.

Destination Address
Typically the all-routers multicast address.

Hop Limit 255

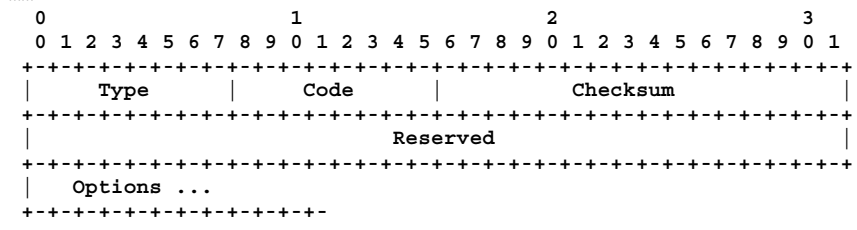
Authentication Header
If a Security Association for the IP Authentication Header exists between the sender and the destination address, then the sender SHOULD include this header.

RQ_000_8130 Generate Router Solicitation Header
RFC2461 4.1 MANDATORY
Applies to: Host
Context:

Requirement:
When constructing a Router Solicitation message, an IPv6 host MUST set the fields in the ICMPv6 packet as follows:

ICMPv6 Field	Octets	Value
Type	1	133
Code	2	0
Checksum	3 & 4	ICMPv6 packet checksum
Reserved	5 - 8	0

Specification Text:
Router Solicitation Message Format
……



……

ICMP Fields:

Type **133**

Code **0**

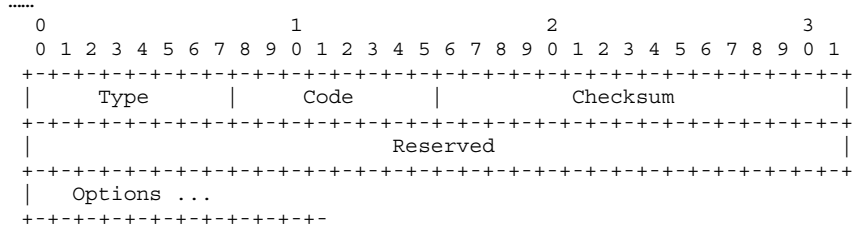
Checksum **The ICMP checksum. See [ICMPv6].**

Reserved **This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.**

RQ_000_8131 Process Router Solicitation
RFC2461 4.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST ignore any value set in the Reserved field (octets 5 to 8) in the ICMPv6 packet of a received Router Solicitation message.
Specification Text:
Router Solicitation Message Format

……



……

ICMP Fields:

Type 133

Code 0

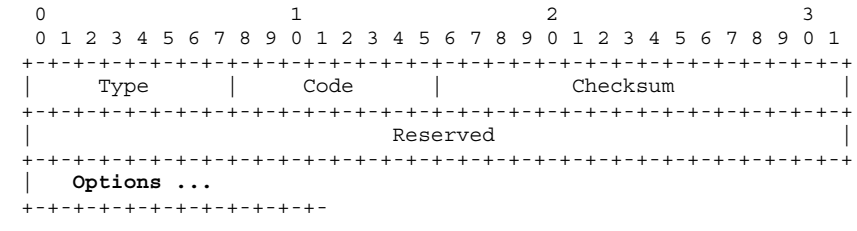
Checksum The ICMP checksum. See [ICMPv6].

Reserved **This field is unused**. It MUST be initialized to zero by the sender and **MUST be ignored by the receiver**.

RQ_000_8132 Generate RS Source Link-Layer Address Option
RFC2461 4.1 RECOMMENDED
Applies to: Host
Context:

Requirement:
When constructing a Router Solicitation message, an IPv6 host SHOULD insert the link-layer address into the Source link-layer address Options field if such a link-layer address is known.
Specification Text:
Router Solicitation Message Format

……



……

Valid Options:

Source link-layer address
The link-layer address of the sender, if known.
MUST NOT be included if the Source Address is the unspecified address. Otherwise it SHOULD be included on link layers that have addresses.

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.

RQ_000_8133 Generate RS Source Link-Layer Address Option

RFC2461 4.1 MANDATORY

Applies to: Host

Context:

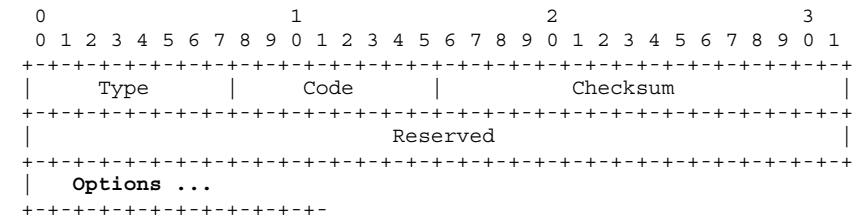
Requirement:

When constructing a Router Solicitation message, an IPv6 host MUST NOT insert an address value into the Source link-layer address Options field if the IPv6 Source Address is the Unspecified Address (0:0:0:0:0:0:0:0)

Specification Text:

Router Solicitation Message Format

……



……

Valid Options:

Source link-layer address

The link-layer address of the sender, if known. **MUST NOT be included if the Source Address is the unspecified address.** Otherwise it SHOULD be included on link layers that have addresses.

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.

RQ_000_8134 Process Router Solicitation

RFC2461 4.1 MANDATORY

Applies to: Router

Context:

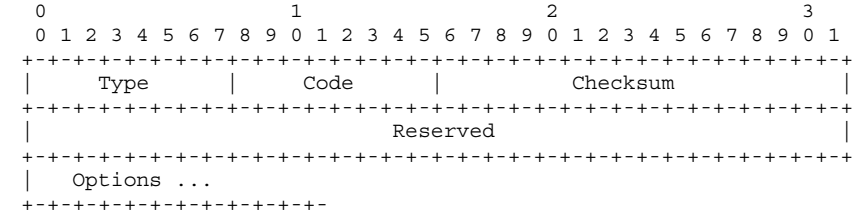
Requirement:

An IPv6 router MUST silently ignore any unrecognized value in the Options field of a received Router Solicitation message but continue to process the message.

Specification Text:

Router Solicitation Message Format

……



……

Valid Options:

Source link-layer address

The link-layer address of the sender, if known. MUST NOT be included if the Source Address is the unspecified address. Otherwise it SHOULD be included on link layers that have addresses.

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.

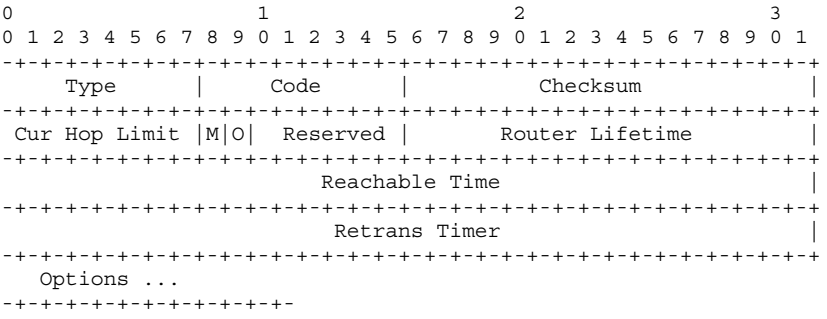
RQ_000_8135 Generate Router Advertisement
RFC2461 4.2 MANDATORY
Applies to: Router
Context:

Requirement:
When an IPv6 router transmits an unsolicited Router Advertisement message, fields in the IPv6 packet header MUST be set as follows:

IPv6 Header Field	Value
Source Address	link-local address assigned to the interface from which the message is to be sent
Destination Address	IPv6 All-Nodes Multicast Address (FF02:0:0:0:0:0:0:2)
Hop Limit	255

Specification Text:
Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or in response to a Router Solicitation.



IP Fields:

Source Address
MUST be the link-local address assigned to the interface from which this message is sent.

Destination Address
Typically the Source Address of an invoking Router Solicitation or **the all-nodes multicast address.**

Hop Limit **255**

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.

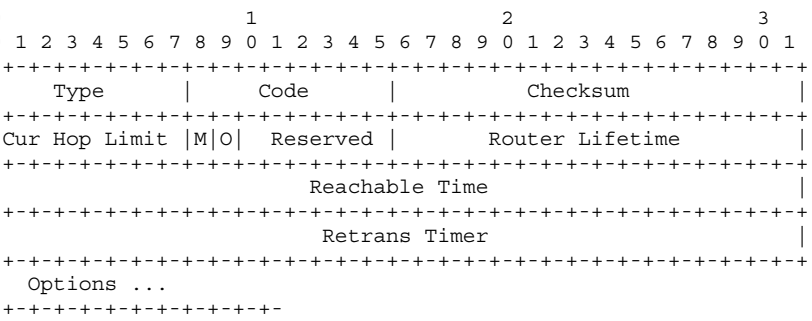
RQ_000_8136 Router Processing of RS
RFC2461 4.2 MANDATORY
Applies to: Router
Context:

Requirement:
When an IPv6 router receives a Router Solicitation message, it MUST transmit a Router Advertisement message in response with fields in the IPv6 packet header set as follows:

IPv6 Header Field	Value
Source Address	link-local address assigned to the interface from which the message is to be sent
Destination Address	Source address taken from the IPv6 packet header of the received Router Solicitation message
Hop Limit	255

Specification Text:
Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or **in response to a Router Solicitation**.



IP Fields:

Source Address
MUST be the link-local address assigned to the interface from which this message is sent.

Destination Address
Typically the Source Address of an invoking Router Solicitation or the all-nodes multicast address.

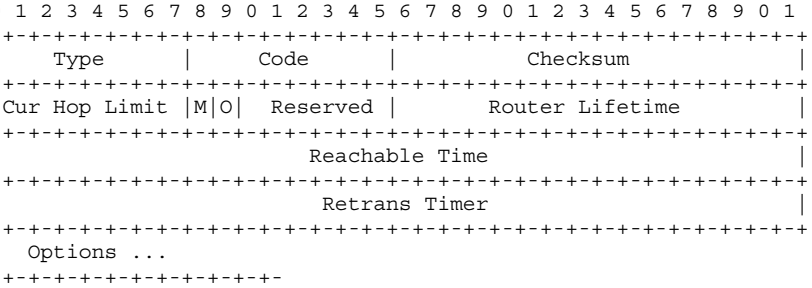
Hop Limit **255**

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.

RQ_000_8137 Form Router Advertisement Header
RFC2461 4.2 RECOMMENDED
Applies to: Router
Context:

Requirement:
When constructing a Router Advertisement message, an IPv6 router SHOULD include an Authentication Header in the IPv6 packet if an AH-based Security Association exists between the IPv6 node and the destination address.
Specification Text:
Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or in response to a Router Solicitation.



IP Fields:

Source Address
MUST be the link-local address assigned to the interface from which this message is sent.

Destination Address
Typically the Source Address of an invoking Router Solicitation or the all-nodes multicast address.

Hop Limit 255

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.

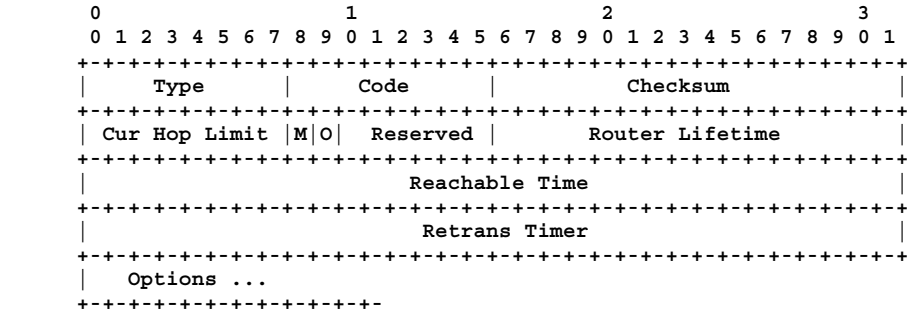
RQ_000_8138 Form Router Advertisement Header
RFC2461 4.2 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Router Solicitation message, an IPv6 host MUST set the fields in the ICMPv6 packet as follows:

ICMPv6 Field	Octets	Value
Type	1	134
Code	2	0
Checksum	3 & 4	ICMPv6 packet checksum
Cur Hop Limit	5	Value established by configuration
M flag	6[0]	1 = Receiver should use stateful address autoconfiguration
O Flag	6[1]	1 = Receiver should use stateful protocol to configure non-address information
Reserved	6[2-7]	0
Router Lifetime	7 & 8	Lifetime (seconds) associated with the router as a default router (0=Not a default router)
Reachable Time	9 - 12	Time (ms) that a receiving node should assume that the IPv6 router will be reachable after having received a reachability confirmation (0=unspecified)
Retrans Timer	13 - 16	Time (ms) to be used by a receiving node between retransmitted Neighbor Solicitation messages

Specification Text:
Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or in response to a Router Solicitation.



……
ICMP Fields:

Type 134

Code 0

Checksum The ICMP checksum. See [ICMPv6].

Cur Hop Limit 8-bit unsigned integer. The default value that should be placed in the Hop Count field of the IP header for outgoing IP packets. A value of zero means unspecified (by this router).

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 RFC 2462.

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 RFC 2462.

Reserved A 6-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Router Lifetime 16-bit unsigned integer. The lifetime associated with the default router in units of seconds. The maximum value corresponds to 18.2 hours. A Lifetime of 0 indicates that the router is not a default router and SHOULD NOT appear on the default router list. The Router Lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Options that need time limits for their information include their own lifetime fields.

Reachable Time 32-bit unsigned integer. The time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation. Used by the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router).

Retrans Timer 32-bit unsigned integer. The time, in milliseconds, between retransmitted Neighbor Solicitation messages. Used by address resolution and the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router).

RQ_000_8139 Process Field Anomalies in RA

RFC2461 4.2 MANDATORY

Applies to: Router, Host

Context:

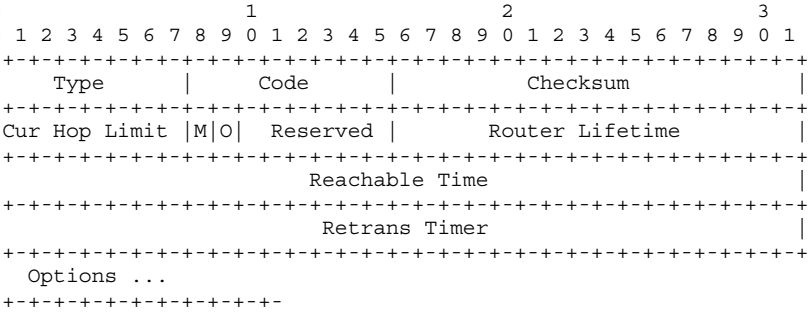
Requirement:

An IPv6 node MUST ignore the contents of the Reserved field in the ICMPv6 packet of a received Router Advertisement message.

Specification Text:

Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or in response to a Router Solicitation.



……

ICMP Fields:

Type 134

Code 0

Checksum The ICMP checksum. See [ICMPv6].

Cur Hop Limit 8-bit unsigned integer. The default value that should be placed in the Hop Count field of the IP header for outgoing IP packets. A value of zero means unspecified (by this router).

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 RFC 2462.

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 RFC 2462.

Reserved **A 6-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver**.

Router Lifetime 16-bit unsigned integer. The lifetime associated with the default router in units of seconds. The maximum value corresponds to 18.2 hours. A Lifetime of 0 indicates that the router is not a default router and SHOULD NOT appear on the default router list. The Router Lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Options that need time limits for their information include their own lifetime fields.

Reachable Time 32-bit unsigned integer. The time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation. Used by the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router).

Retrans Timer 32-bit unsigned integer. The time, in milliseconds, between retransmitted Neighbor Solicitation messages. Used by address resolution and the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router).

RQ_000_8140 Process Router Advertisement

RFC2461 4.2 RECOMMENDED

Applies to: Host

Context:

An IPv6 host receives a Router Advertisement message with the Router Lifetime field set to 0 in the ICMPv6 packet.

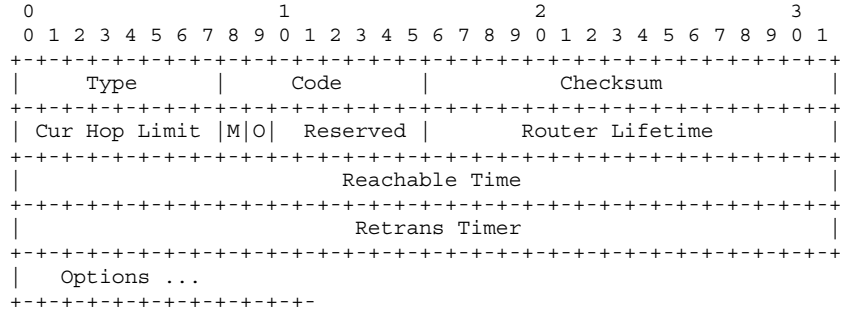
Requirement:

The IPv6 host SHOULD NOT use the advertising router as one of its default routers.

Specification Text:

Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or in response to a Router Solicitation.



……
ICMP Fields:

Type 134

Code 0

Checksum The ICMP checksum. See [ICMPv6].

Cur Hop Limit 8-bit unsigned integer. The default value that should be placed in the Hop Count field of the IP header for outgoing IP packets. A value of zero means unspecified (by this router).

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 RFC 2462.

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 RFC 2462.

Reserved A 6-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Router Lifetime
16-bit unsigned integer. The lifetime associated with the default router in units of seconds. The maximum value corresponds to 18.2 hours. **A Lifetime of 0 indicates that the router is not a default router and SHOULD NOT appear on the default router list.** The Router Lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Options that need time limits for their information include their own lifetime fields.

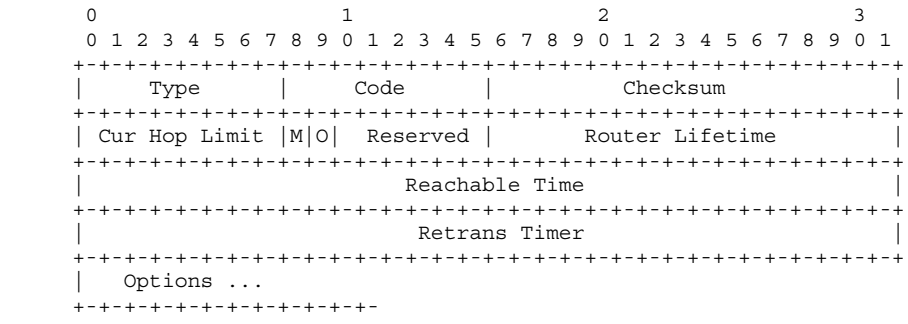
Reachable Time 32-bit unsigned integer. The time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation. Used by the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router).

Retrans Timer 32-bit unsigned integer. The time, in milliseconds, between retransmitted Neighbor Solicitation messages. Used by address resolution and the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router).

RQ_000_8141 Process Router Advertisement
RFC2461 4.2 OPTIONAL
Applies to: Router
Context:

Requirement:
An IPv6 router MAY omit the Source link-layer address option in a Router Advertisement message.
Specification Text:
Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or in response to a Router Solicitation.



……

Possible options:

Source link-layer address
The link-layer address of the interface from which the Router Advertisement is sent. Only used on link layers that have addresses. **A router MAY omit this option in order to enable inbound load sharing across multiple link-layer addresses.**

MTU
SHOULD be sent on links that have a variable MTU (as specified in the document that describes how to run IP over the particular link type). MAY be sent on other links.

Prefix Information
These options specify the prefixes that are on-link and/or are used for address autoconfiguration. A router SHOULD include all its on-link prefixes (except the link-local prefix) so that multihomed hosts have complete prefix information about on-link destinations for the links to which they attach. If complete information is lacking, a multihomed host may not be able to choose the correct outgoing interface when sending traffic to its neighbors.

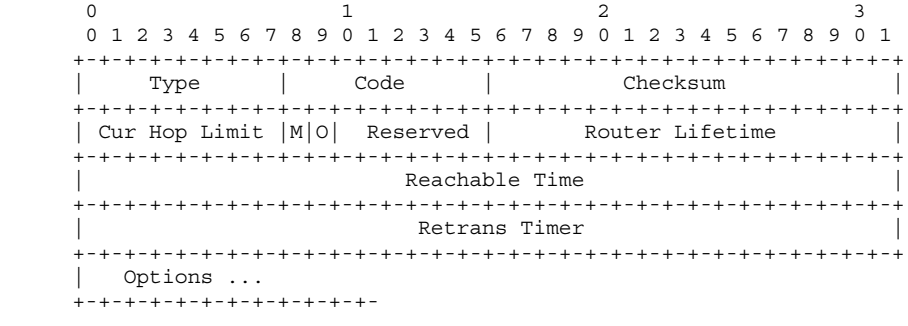
Future versions of this protocol may define new option types. Receivers MUST silently ignore any options they do not recognize and continue processing the message.

RQ_000_8142 RA MTU Option
RFC2461 4.2 RECOMMENDED
Applies to: Router
Context:

Requirement:
When constructing a Router Advertisement message to be sent on a link that is known to have a variable MTU, an IPv6 router SHOULD include the MTU option in the ICMPv6 packet.

Specification Text:
Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or in response to a Router Solicitation.



……

Possible options:

Source link-layer address
The link-layer address of the interface from which the Router Advertisement is sent. Only used on link layers that have addresses. A router MAY omit this option in order to enable inbound load sharing across multiple link-layer addresses.

MTU **SHOULD be sent on links that have a variable MTU (as specified in the document that describes how to run IP over the particular link type).** MAY be sent on other links.

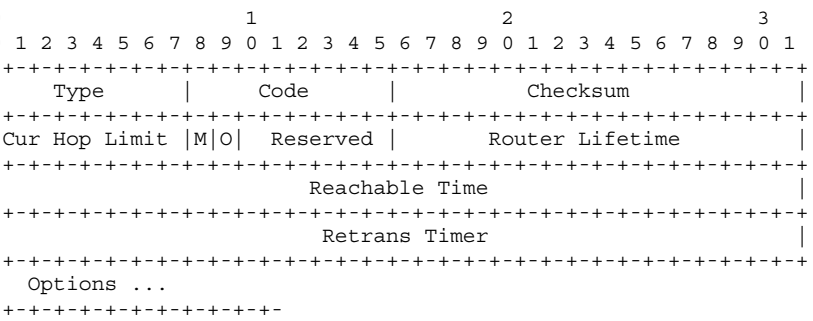
Prefix Information
These options specify the prefixes that are on-link and/or are used for address autoconfiguration. A router SHOULD include all its on-link prefixes (except the link-local prefix) so that multihomed hosts have complete prefix information about on-link destinations for the links to which they attach. If complete information is lacking, a multihomed host may not be able to choose the correct outgoing interface when sending traffic to its neighbors.

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.

RQ_000_8143 RA MTU Option
RFC2461 4.2 OPTIONAL
Applies to: Router
Context:

Requirement:
When constructing a Router Advertisement message to be sent on a link that is known to have a fixed MTU, an IPv6 router MAY include the MTU option in the ICMPv6 packet.
Specification Text:
Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or in response to a Router Solicitation.



……
Possible options:

Source link-layer address
The link-layer address of the interface from which the Router Advertisement is sent. Only used on link layers that have addresses. A router MAY omit this option in order to enable inbound load sharing across multiple link-layer addresses.

MTU SHOULD be sent on links that have a variable MTU (as specified in the document that describes how to run IP over the particular link type). **MAY be sent on other links.**

```
   Prefix Information
                 These options specify the prefixes that are on-link
                 and/or are used for address autoconfiguration.  A
                 router SHOULD include all its on-link prefixes
                 (except the link-local prefix) so that multihomed
                 hosts have complete prefix information about on-
                 link destinations for the links to which they
                 attach.  If complete information is lacking, a
                 multihomed host may not be able to choose the
                 correct outgoing interface when sending traffic to
                 its neighbors.

   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.
```

RQ_000_8144 RA Prefix Option

RFC2461 4.2 RECOMMENDED

Applies to: Router

Context:

Requirement:

```
  When constructing a Router Advertisement message, an IPv6 router SHOULD include all of its on-
  link prefixes (except the link-local prefix) in the ICMPv6 Prefix Information option field.
```

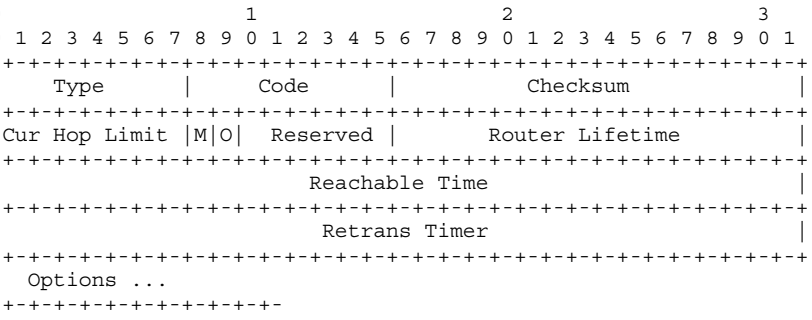
Specification Text:

```
  Router Advertisement Message Format

  Routers send out Router Advertisement message periodically, or in response to a Router
  Solicitation.

       0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |     Type      |     Code      |          Checksum             |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      | Cur Hop Limit |M|O|  Reserved |       Router Lifetime         |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         Reachable Time                        |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                          Retrans Timer                        |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |   Options ...
      +-+-+-+-+-+-+-+-+-+-
  ……
   Possible options:

     Source link-layer address
                 The link-layer address of the interface from which
                 the Router Advertisement is sent.  Only used on
                 link layers that have addresses.  A router MAY omit
                 this option in order to enable inbound load sharing
                 across multiple link-layer addresses.

     MTU         SHOULD be sent on links that have a variable MTU
                 (as specified in the document that describes how to
                 run IP over the particular link type).  MAY be sent
                 on other links.

     Prefix Information
                 These options specify the prefixes that are on-link
                 and/or are used for address autoconfiguration.  A
                 router SHOULD include all its on-link prefixes
                 (except the link-local prefix) so that multihomed
                 hosts have complete prefix information about on-
                 link destinations for the links to which they
                 attach.  If complete information is lacking, a
                 multihomed host may not be able to choose the
                 correct outgoing interface when sending traffic to
                 its neighbors.

   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.
```

RQ_000_8145 Process Option Anomalies in RA
RFC2461 4.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 router MUST silently ignore any unrecognized value in the Options fields of a received Router Advertisement message but continue to process the message.
Specification Text:
Router Advertisement Message Format

Routers send out Router Advertisement message periodically, or in response to a Router Solicitation.



……
Possible options:

Source link-layer address
The link-layer address of the interface from which the Router Advertisement is sent. Only used on link layers that have addresses. A router MAY omit this option in order to enable inbound load sharing across multiple link-layer addresses.

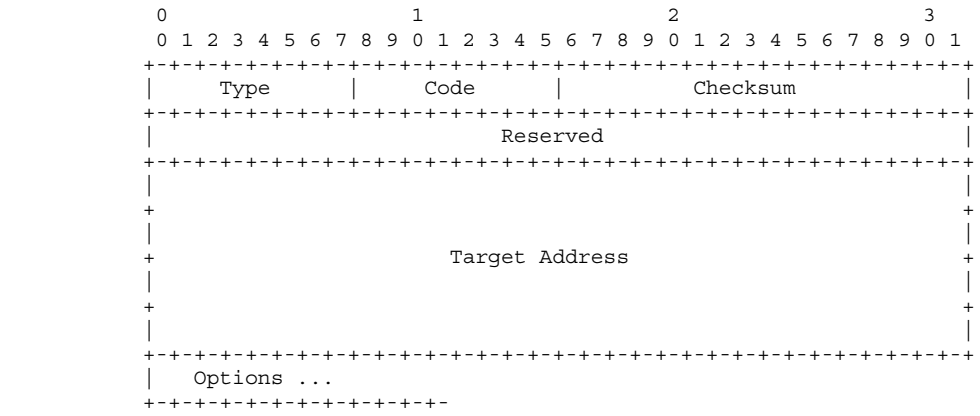
MTU
SHOULD be sent on links that have a variable MTU (as specified in the document that describes how to run IP over the particular link type). MAY be sent on other links.

Prefix Information
These options specify the prefixes that are on-link and/or are used for address autoconfiguration. A router SHOULD include all its on-link prefixes (except the link-local prefix) so that multihomed hosts have complete prefix information about on-link destinations for the links to which they attach. If complete information is lacking, a multihomed host may not be able to choose the correct outgoing interface when sending traffic to its neighbors.

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.**

RQ_000_8146 Address Resolution
RFC2461 4.3 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When using Neighbor Discovery to resolve an address, an IPv6 node MUST set the Destination Address field in the IPv6 Header of its Neighbor Solicitation message to an IPv6 Solicited Node Multicast address (FF02:0:0:0:0:1::FFXX:XXXX).
Specification Text:
Nodes send Neighbor Solicitations to request the link-layer address of a target node while also providing their own link-layer address to the target. **Neighbor Solicitations are multicast when the node needs to resolve an address** and unicast when the node seeks to verify the reachability of a neighbor.



IP Fields:

Source Address
Either an address assigned to the interface from which this message is sent or (if Duplicate Address Detection is in progress [ADDRCONF]) the unspecified address.

Destination Address
Either the solicited-node multicast address corresponding to the target address, or the target address.

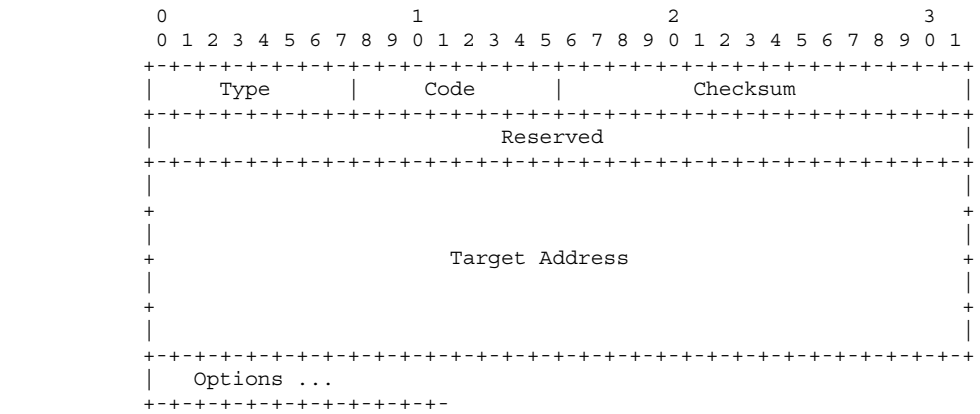
Hop Limit 255

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.

RQ_000_8147 Determine Neighbor Reachability
RFC2461 4.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When using Neighbor Discovery to determine the reachability of a neighboring node, an IPv6 node MUST set the Destination Address field in the IPv6 Header of its Neighbor Solicitation message to the address of the neighboring node.

Specification Text:
Nodes send Neighbor Solicitations to request the link-layer address of a target node while also providing their own link-layer address to the target. Neighbor Solicitations are multicast when the node needs to resolve an address and **unicast when the node seeks to verify the reachability of a neighbor.**



IP Fields:

Source Address
Either an address assigned to the interface from which this message is sent or (if Duplicate Address Detection is in progress [ADDRCONF]) the unspecified address.

Destination Address
Either the solicited-node multicast address corresponding to the target address, **or the target address.**

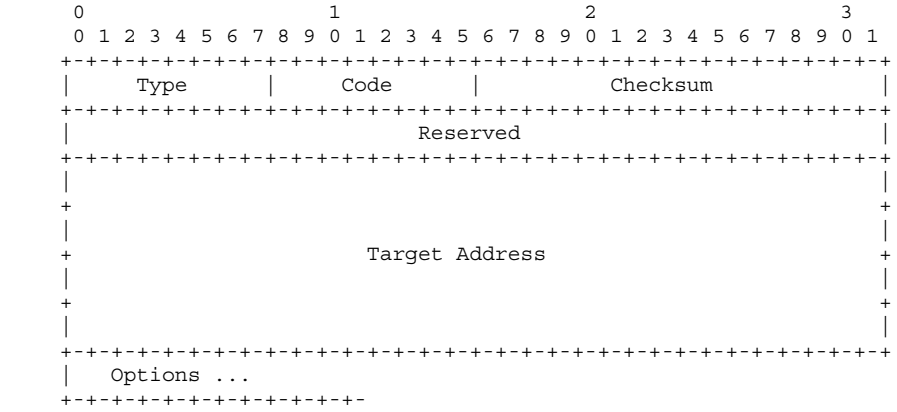
Hop Limit 255

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.

RQ_000_8148 Generate Neighbor Solicitation Header
RFC2461 4.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Solicitation message as part of the Duplicate Address Detection process, an IPv6 node MUST set the Source address field in the IPv6 Header to the IPv6 Unspecified Address (0:0:0:0:0:0:0:0).

Specification Text:
Nodes send Neighbor Solicitations to request the link-layer address of a target node while also providing their own link-layer address to the target. Neighbor Solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor.



IP Fields:

Source Address
Either an address assigned to the interface from which this message is sent or **(if Duplicate Address Detection is in progress RFC 2462) the unspecified address.**

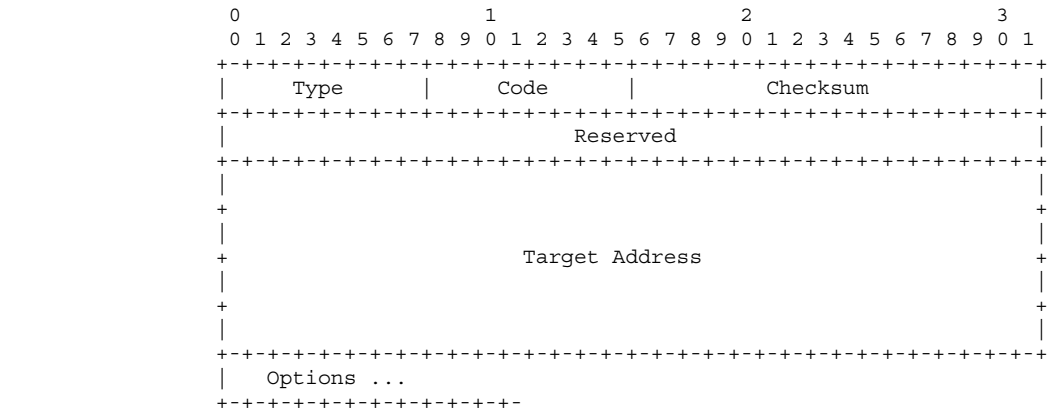
Destination Address
Either the solicited-node multicast address corresponding to the target address, or the target address.

Hop Limit 255

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.

RQ_000_8149 Generate Neighbor Solicitation Header
RFC2461 4.3 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When constructing a Neighbor Solicitation message outside the Duplicate Address Detection process, an IPv6 node MUST set the Source address field in the IPv6 Header to an IPv6 address assigned to the interface on which the message will be sent.
Specification Text:
Nodes send Neighbor Solicitations to request the link-layer address of a target node while also providing their own link-layer address to the target. Neighbor Solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor.



IP Fields:

Source Address
Either an address assigned to the interface from which this message is sent or (if Duplicate Address Detection is in progress [ADDRCONF]) the unspecified address.

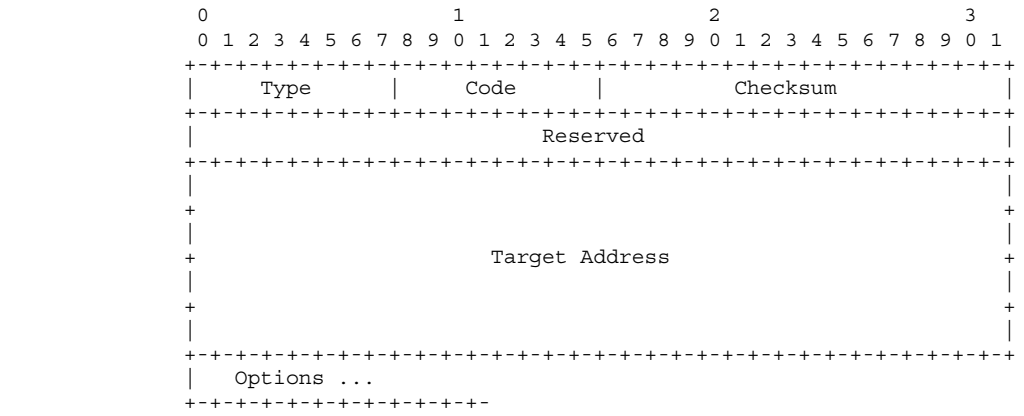
Destination Address
Either the solicited-node multicast address corresponding to the target address, or the target address.

Hop Limit 255

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.

RQ_000_8150 Generate Neighbor Solicitation Header
RFC2461 4.3 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When constructing a neighbor Solicitation message, an IPv6 node MUST set the Hop Limit field in the IPv6 Header to the decimal value 255.
Specification Text:
Nodes send Neighbor Solicitations to request the link-layer address of a target node while also providing their own link-layer address to the target. Neighbor Solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor.



IP Fields:

Source Address
Either an address assigned to the interface from which this message is sent or (if Duplicate Address Detection is in progress [ADDRCONF]) the unspecified address.

Destination Address
Either the solicited-node multicast address corresponding to the target address, or the target address.

Hop Limit **255**

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.

RQ_000_8151 Generate Neighbor Solicitation Header

RFC2461 4.3 RECOMMENDED

Applies to: Host, Router

Context:

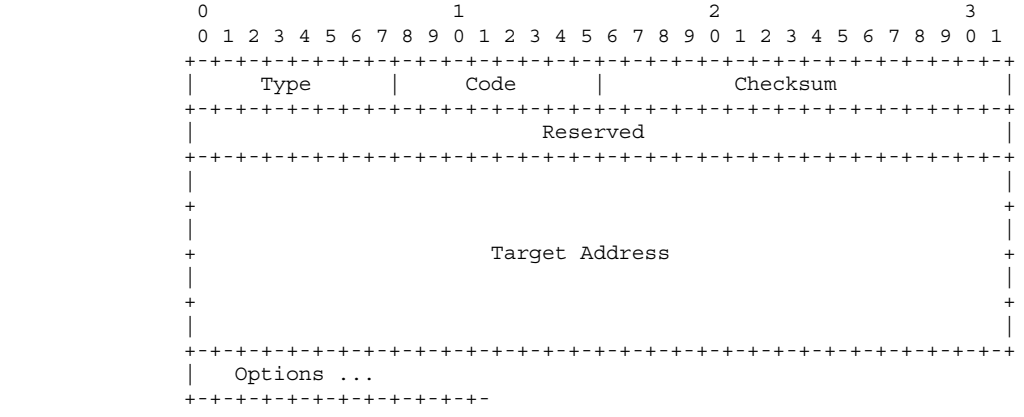
The implementation is generating a Neighbor Solicitation. A security association exists between the implementation and the destination address.

Requirement:

When constructing a Neighbor Solicitation message, an IPv6 router SHOULD include an Authentication Header in the IPv6 packet if an AH-based Security Association exists between the IPv6 node and the destination address.

Specification Text:

Nodes send Neighbor Solicitations to request the link-layer address of a target node while also providing their own link-layer address to the target. Neighbor Solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor.



```
 IP Fields:

Source Address
              Either an address assigned to the interface from
              which this message is sent or (if Duplicate Address
              Detection is in progress [ADDRCONF]) the
              unspecified address.

Destination Address
              Either the solicited-node multicast address
              corresponding to the target address, or the target
              address.

Hop Limit     255

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.
```

RQ_000_8152 Generate Neighbor Solicitation Header

RFC2461 4.3 MANDATORY

Applies to: Host, Router

Context:

Requirement:

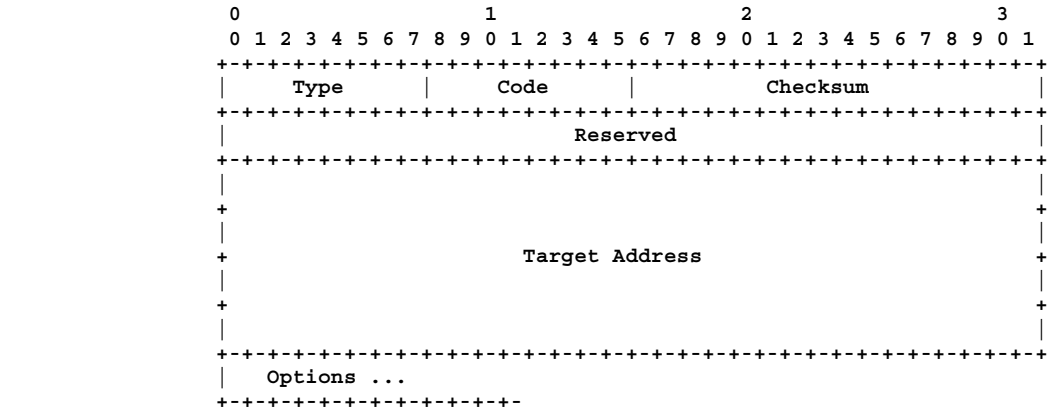
When constructing a Neighbor Solicitation message, an IPv6 host MUST set the fields in the ICMPv6 packet as follows:

ICMPv6 Field	Octets	Value
Type	1	135
Code	2	0
Checksum	3 & 4	ICMPv6 packet checksum
Reserved	5 - 8	0
Target Address	9 - 24	IP address of the target of the solicitation

Specification Text:

Neighbor Solicitation Message Format

Nodes send Neighbor Solicitations to request the link-layer address of a target node while also providing their own link-layer address to the target. Neighbor Solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor.



……

ICMP Fields:

Type 135

Code 0

Checksum The ICMP checksum. See RFC 2463.

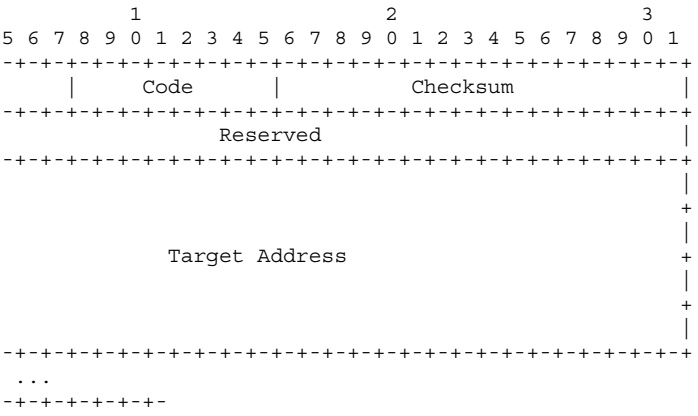
Reserved **This field is unused. It MUST be initialized to zero by the sender and** MUST be ignored by the receiver.

Target Address
The IP address of the target of the solicitation. It MUST NOT be a multicast address.

RQ_000_8153 Process Field Anomalies in NS
RFC2461 4.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ignore the contents of the Reserved field in the ICMPv6 packet of a received Neighbor Discovery message.
Specification Text:
Neighbor Solicitation Message Format

Nodes send Neighbor Solicitations to request the link-layer address of a target node while also providing their own link-layer address to the target. Neighbor Solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor.



……
ICMP Fields:

Type 135

Code 0

Checksum The ICMP checksum. See RFC 2463.

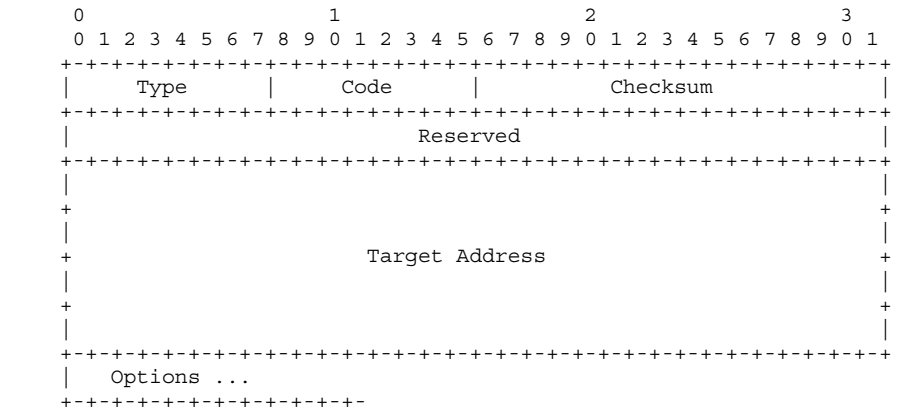
Reserved **This field is unused.** It MUST be initialized to zero by the sender **and MUST be ignored by the receiver.**

Target Address
The IP address of the target of the solicitation. It MUST NOT be a multicast address.

RQ_000_8154 Generate Neighbor Solicitation Header
RFC2461 4.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Solicitation message, an IPv6 node MUST NOT place a multicast IP address in the Target field in the ICMPv6 packet.
Specification Text:
Neighbor Solicitation Message Format

Nodes send Neighbor Solicitations to request the link-layer address of a target node while also providing their own link-layer address to the target. Neighbor Solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor.



……

ICMP Fields:

Type 135

Code 0

Checksum The ICMP checksum. See RFC 2463.

Reserved This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

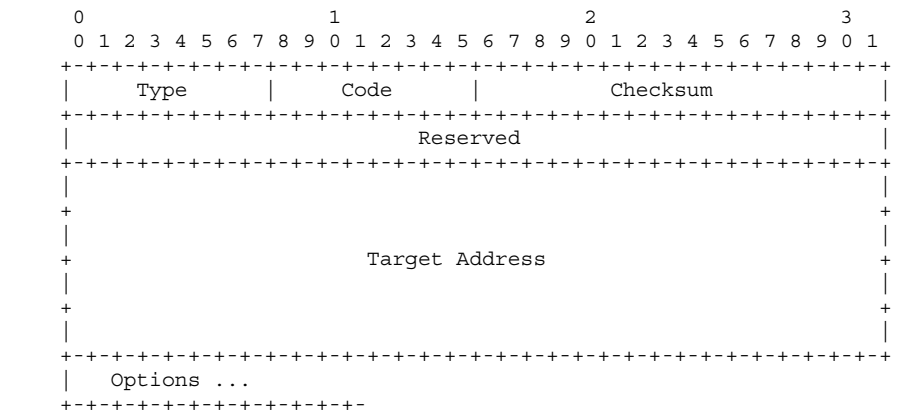
Target Address
The IP address of the target of the solicitation.
It MUST NOT be a multicast address.

RQ_000_8155 Generate Neighbor Solicitation Option
RFC2461 4.3 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When constructing a Neighbor Solicitation message, an IPv6 host MUST NOT insert an address value into the Source link-layer address Options field if the IPv6 Source Address is the Unspecified Address (0:0:0:0:0:0:0:0)

Specification Text:
Neighbor Solicitation Message Format

……



……

Possible options:

Source link-layer address
The link-layer address for the sender. MUST NOT be included when the source IP address is the unspecified address. Otherwise, on link layers that have addresses this option MUST be included in multicast solicitations and SHOULD be included in unicast solicitations.

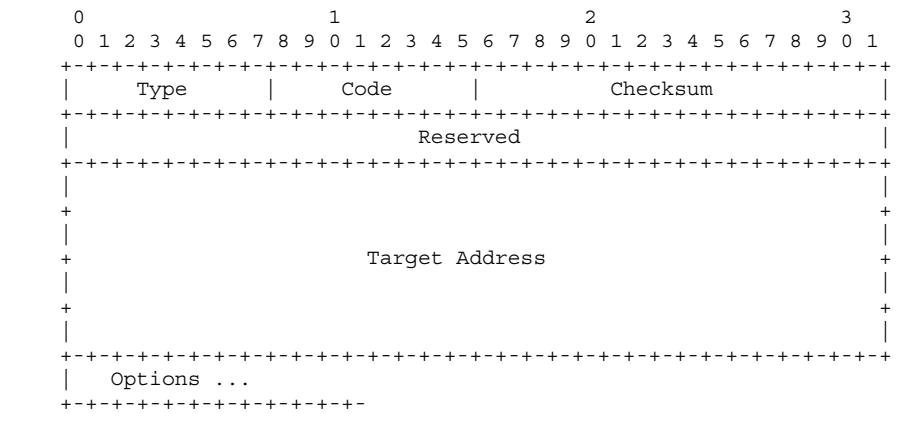
Future versions of this protocol may define new option types. Receivers MUST silently ignore any options they do not recognize and continue processing the message.

RQ_000_8156 Generate Neighbor Solicitation Option
RFC2461 4.3 MANDATORY
Applies to: Host, RoutervContext:

Requirement:
When constructing a Neighbor Solicitation message for multicast transmission over a link layer for which an address exists, an IPv6 node MUST insert the link layer address into the Source Link Layer Address option field of the message.

Specification Text:
Neighbor Solicitation Message Format

……



……

Possible options:

Source link-layer address
The link-layer address for the sender. MUST NOT be included when the source IP address is the unspecified address. Otherwise, **on link layers that have addresses this option MUST be included in multicast solicitations** and SHOULD be included in unicast solicitations.

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.

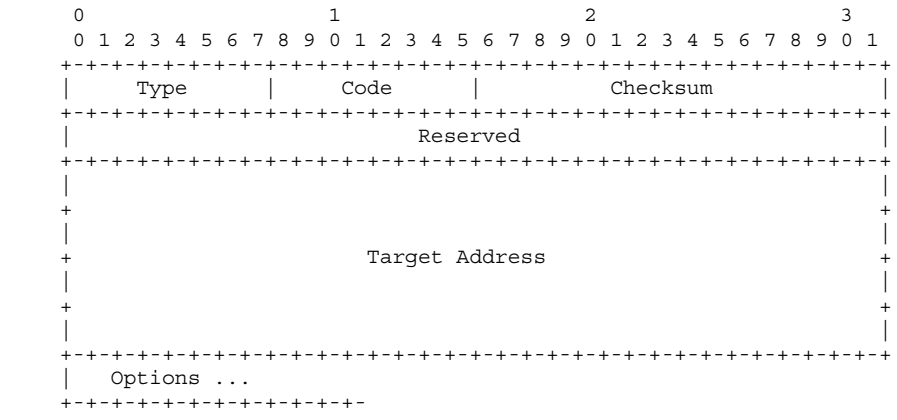
RQ_000_8157 Generate Neighbor Solicitation Option
RFC2461 4.3 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Solicitation message for unicast transmission over a link layer for which an address exists, an IPv6 node SHOULD insert the link layer address into the Source Link Layer Address option field of the message.

Specification Text:

Neighbor Solicitation Message Format

……



……

Possible options:

Source link-layer address

The link-layer address for the sender. MUST NOT be included when the source IP address is the unspecified address. Otherwise, on link layers that have addresses this option MUST be included in multicast solicitations **and SHOULD be included in unicast solicitations.**

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.

RQ_000_8158 Process Option Anomalies in NS

RFC2461 4.3 MANDATORY

Applies to: Host, Router

Context:

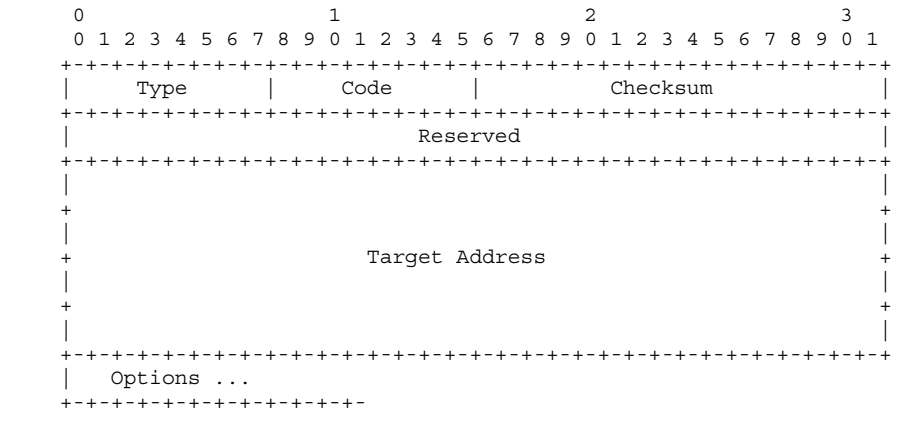
Requirement:

An IPv6 node MUST silently ignore any unrecognized value in the Options field of a received Neighbor Solicitation message but continue to process the message.

Specification Text:

Neighbor Solicitation Message Format

……



……

Possible options:

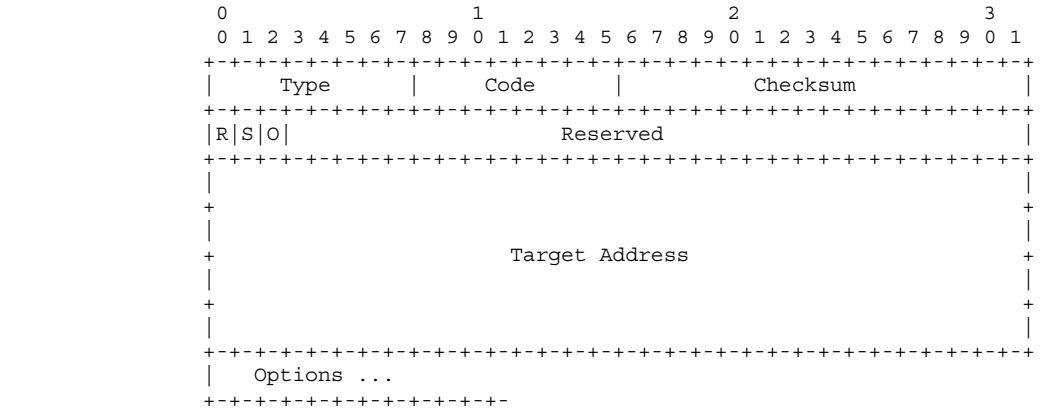
Source link-layer address

The link-layer address for the sender. MUST NOT be included when the source IP address is the unspecified address. Otherwise, on link layers that have addresses this option MUST be included in multicast solicitations and SHOULD be included in unicast solicitations.

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.

RQ_000_8159 Process Neighbor Solicitation
RFC2461 4.4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a valid Neighbor Solicitation.
Requirement:
The IPv6 node MUST send a Neighbor Advertisement message in response to the Neighbor Solicitation.
Specification Text:
Neighbor Advertisement Message Format

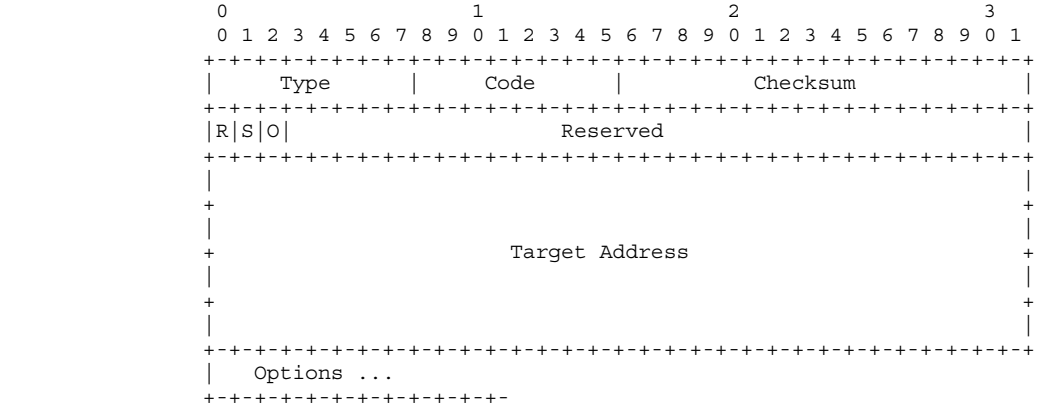
A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



RQ_000_8160 Generate Unsolicited Neighbor Advertisement
RFC2461 4.4 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MAY send an unsolicited Neighbor Advertisement message at any time.
Specification Text:
Neighbor Advertisement Message Format

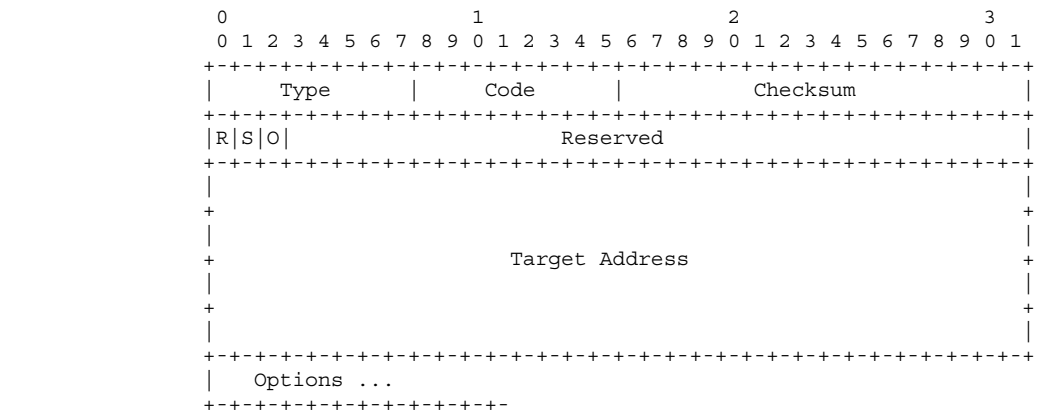
A node sends Neighbor Advertisements in response to Neighbor Solicitations and **sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly**.



RQ_000_8161 Form Neighbor Advertisement Header
RFC2461 4.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Advertisement message, an IPv6 node MUST set the Source Address field in the IPv6 packet header to an address assigned to the interface on which the advertisement is to be sent and MST set the Hop Limit field to the decimal value 255.
Specification Text:
Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



IP Fields:

Source Address
An address assigned to the interface from which the advertisement is sent.

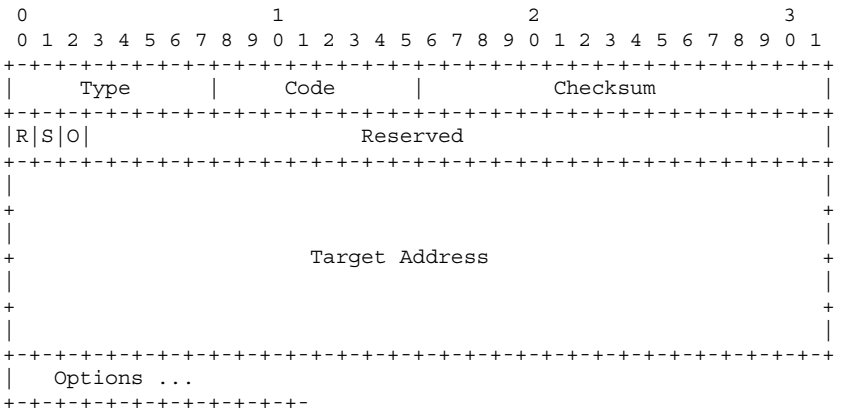
Destination Address
For solicited advertisements, the Source Address of an invoking Neighbor Solicitation or, if the solicitation's Source Address is the unspecified address, the all-nodes multicast address.

For unsolicited advertisements typically the all-nodes multicast address.

Hop Limit 255

RQ_000_8162 Generate Neighbor Advertisement
RFC2461 4.4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a valid Neighbor Solicitation message with the Source Address field in the IPv6 packet header set to a value other than the IPv6 Unspecified Address (0:0:0:0:0:0:0:0).
Requirement:
The IPv6 node MUST transmit a Neighbor Advertisement message with the Destination Address in the IPv6 packet header set to the Source Address of the invoking Neighbor Solicitation.
Specification Text:
Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



IP Fields:

Source Address
An address assigned to the interface from which the advertisement is sent.

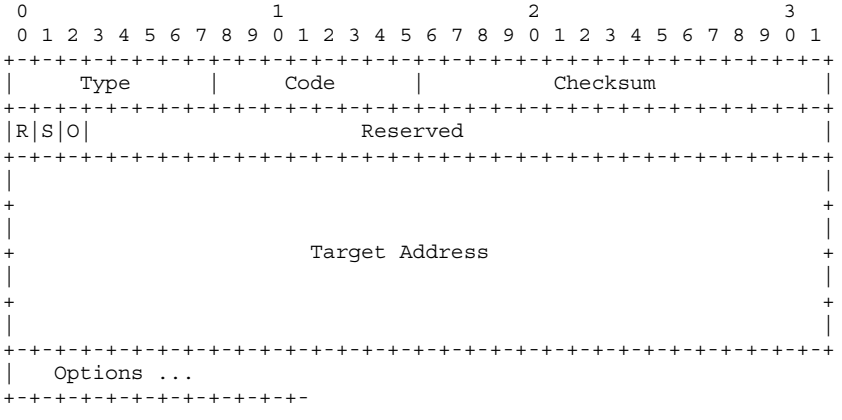
Destination Address
For solicited advertisements, the Source Address of an invoking Neighbor Solicitation or, if the solicitation's Source Address is the unspecified address, the all-nodes multicast address.

For unsolicited advertisements typically the all-nodes multicast address.

Hop Limit 255

RQ_000_8163 Generate Neighbor Advertisement
RFC2461 4.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a valid Neighbor Solicitation message with the Source Address field in the IPv6 packet header set to the IPv6 Unspecified Address (0:0:0:0:0:0:0:0).
Requirement:
The IPv6 node MUST transmit a Neighbor Advertisement message with the Destination Address in the IPv6 packet header set to the IPv6 all-nodes multicast address.
Specification Text:
Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



IP Fields:

Source Address
An address assigned to the interface from which the advertisement is sent.

Destination Address
For solicited advertisements, the Source Address of an invoking Neighbor Solicitation or, **if the solicitation's Source Address is the unspecified address, the all-nodes multicast address.**

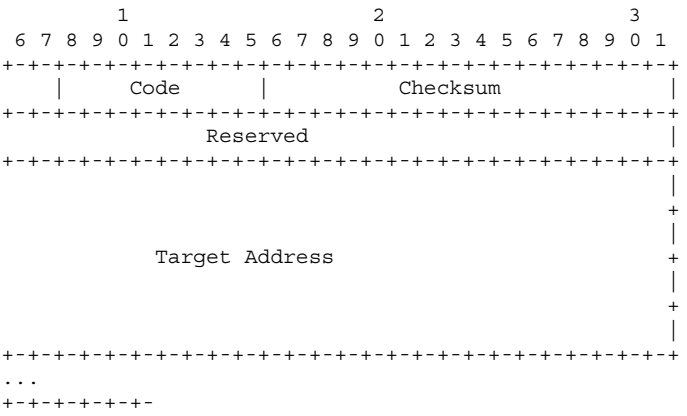
For unsolicited advertisements typically the all-nodes multicast address.

Hop Limit 255

RQ_000_8164 Form Unsolicited NA Header
RFC2461 4.4 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Advertisement message for unsolicited transmission, an IPv6 node SHOULD set the Destination Address in the IPv6 packet header to the IPv6 all-nodes multicast address.
Specification Text:
Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



IP Fields:

Source Address
An address assigned to the interface from which the advertisement is sent.

Destination Address
For solicited advertisements, the Source Address of an invoking Neighbor Solicitation or, if the solicitation's Source Address is the unspecified address, the all-nodes multicast address.

For unsolicited advertisements typically the all-nodes multicast address.

Hop Limit 255

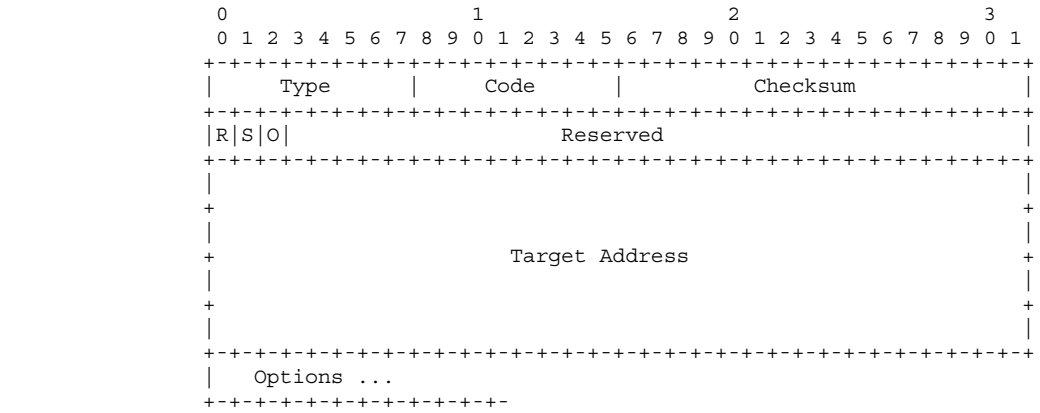
RQ_000_8165 Generate Neighbor Advertisement
RFC2461 4.4 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Advertisement message, an IPv6 router SHOULD include an Authentication Header in the IPv6 packet if an AH-based Security Association exists between the IPv6 node and the destination address.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

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.

RQ_000_8166 Form Neighbor Advertisement Header
RFC2461 4.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:

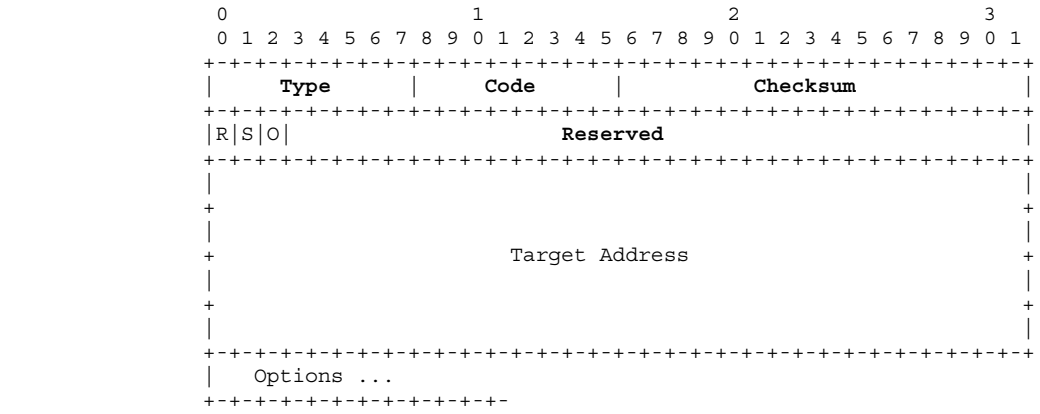
When constructing a Neighbor Solicitation message, an IPv6 host MUST set the fields in the ICMPv6 packet as follows:

ICMPv6 Field	Octets	Value
Type	1	136
Code	2	0
Checksum	3 & 4	ICMPv6 packet checksum
Reserved	5[3-7]	0
Reserved	6 - 8	0

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	**136**
Code	**0**
Checksum	**The ICMP checksum. See RFC 2463.**
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	Override flag. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8167 Process Field Anomalies in NA

RFC2461 4.4 MANDATORY

Applies to: Host, Router

Context:

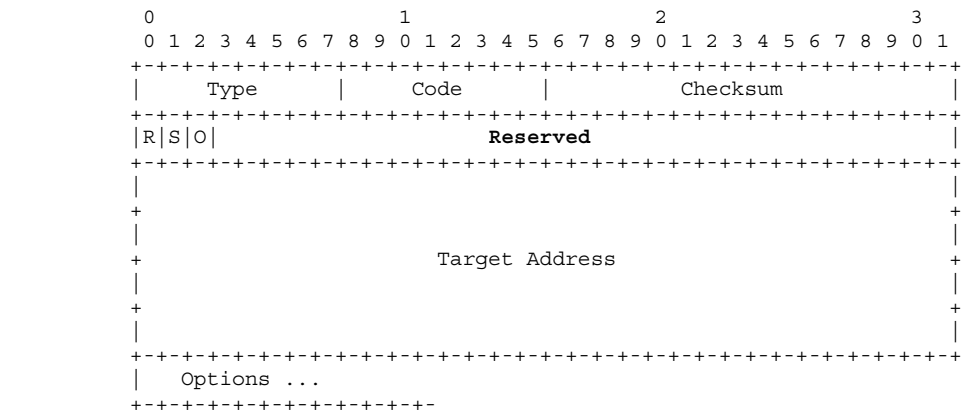
Requirement:

An IPv6 node MUST ignore the contents of the ICMPv6 Reserved field in a received Neighbor Advertisement message.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	Override flag. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	**29-bit unused field.** It MUST be initialized to zero by the sender **and MUST be ignored by the receiver**.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8168 Form Neighbor Advertisement Header

RFC2461 4.4 MANDATORY

Applies to: Host, Router

Context:

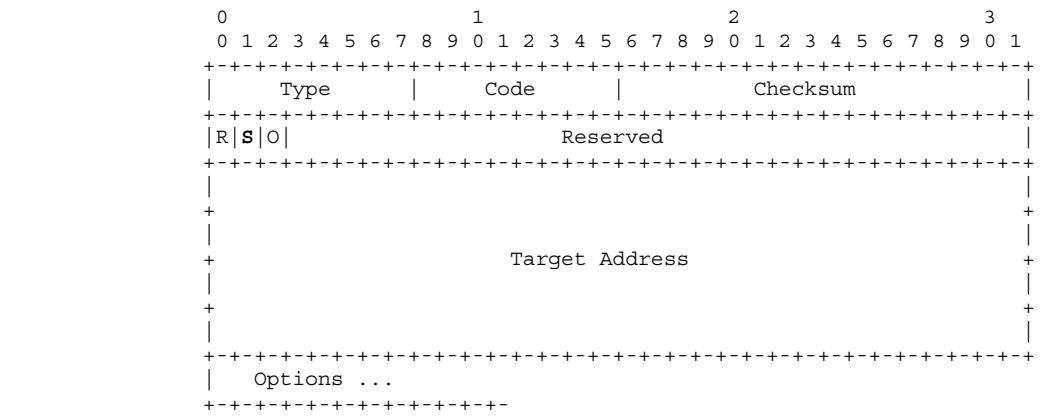
Requirement:

An IPv6 node MUST set the S-Flag (Octet 5, bit 1) to zero (0) in a Neighbor Advertisement message if the Destination Address in the IPv6 packet header contains a multicast address.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	**Solicited flag.** When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. **It MUST NOT be set in multicast advertisements** or in unsolicited unicast advertisements.
O	Override flag. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8169 Form Unsolicited NA Header

RFC2461 4.4 MANDATORY

Applies to: Host, Router

Context:

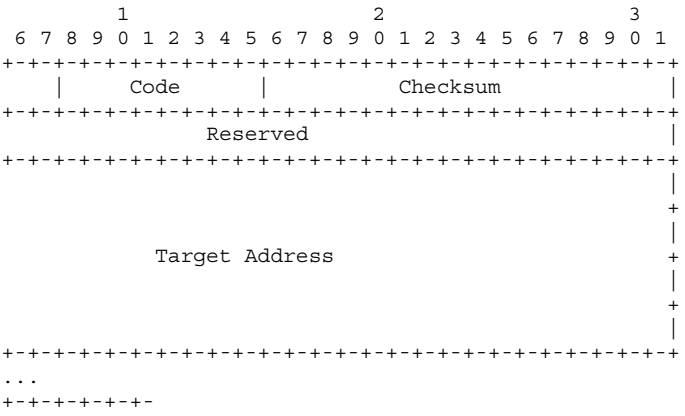
Requirement:

An IPv6 node MUST set the S-Flag (Octet 5, bit 1) to zero (0) in an unsolicited Neighbor Advertisement message if the Destination Address in the IPv6 packet header contains a unicast address.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	**Solicited flag.** When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. **It MUST NOT be set** in multicast advertisements **or in unsolicited unicast advertisements.**
O	Override flag. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8170 Process Neighbor Advertisement

RFC2461 4.4 RECOMMENDED

Applies to: Host, Router

Context:

An IPv6 node receives a Neighbor Advertisement message with the O-Flag (octet 5, bit 2) set to one (1)

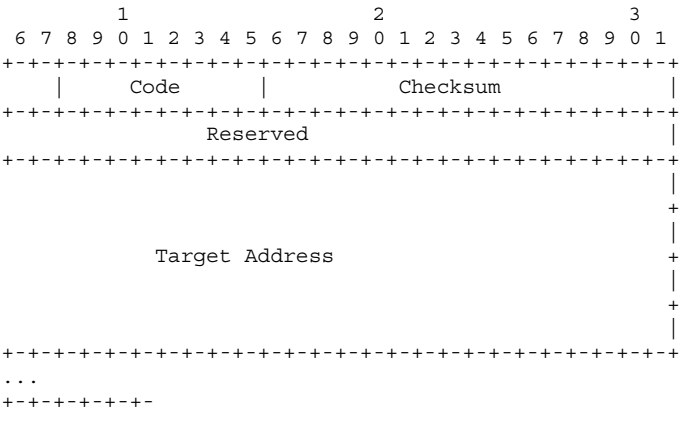
Requirement:

The IPv6 node SHOULD set the link-layer address associated with the IP address to be the contents of the Target Link-Layer Address field in the received Neighbor Advertisement.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	**Override flag. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address**. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8171 Process Neighbor Advertisement

RFC2461 4.4 MANDATORY

Applies to: Router, Host

Context:

An IPv6 node receives a Neighbor Advertisement message with the O-Flag (octet 5, bit 2) set to zero (0)

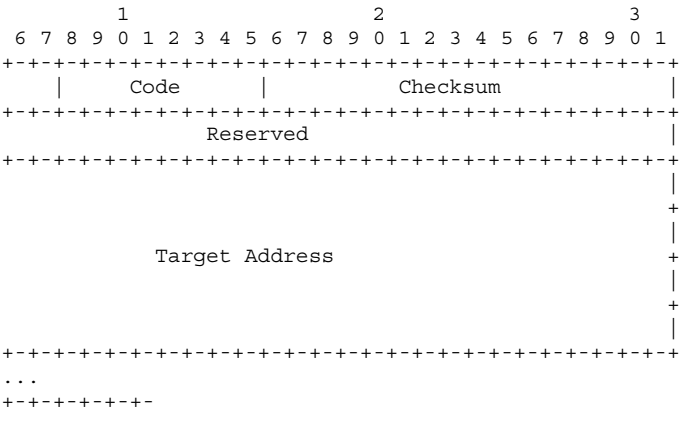
Requirement:

The IPv6 node MUST NOT change its existing association of a particular link-layer address with the IP address contained in the Target Address field.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	**Override flag**. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. **When it is not set the advertisement will not update a cached link-layer address** though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8172 Process Neighbor Advertisement

RFC2461 4.4 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a Neighbor Advertisement message with the O-Flag (octet 5, bit 2) set to zero (0)

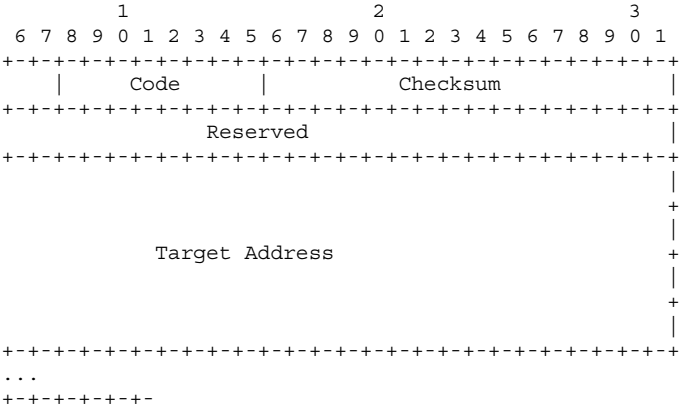
Requirement:

The IPv6 node MUST establish an association between the IP address contained in the Target Address field of the received Neighbor Advertisement and the link-layer address contained in the Target Link-layer Address option field if no association already exists for that IP address.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	**Override flag.** When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address **though it will update an existing Neighbor Cache entry for which no link-layer address is known.** It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8173 Form Neighbor Advertisement Header

RFC2461 4.4 RECOMMENDED

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Solicitation message with an anycast address in the Source Address field of the IPv6 packet Header.

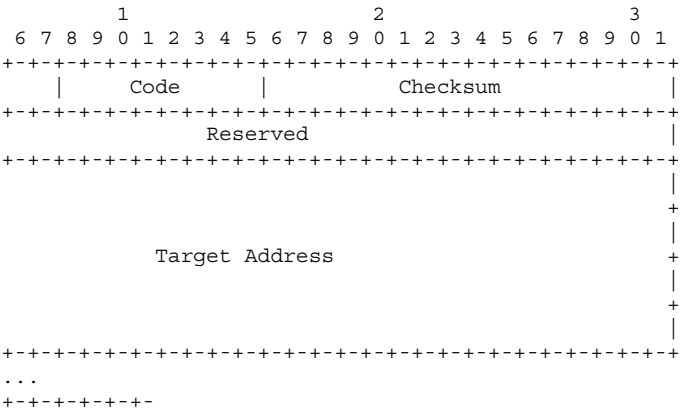
Requirement:

The IPv6 node SHOULD set the O-flag (octet 5, bit 2) to zero (0) in the Neighbor Advertisement sent in response to the solicitation.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	**Override flag.** When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known**. It SHOULD NOT be set in solicited advertisements for anycast addresses** and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8174 Process Proxy NS

RFC2461 4.4 RECOMMENDED

Applies to: Router

Context:

An IPv6 router receives a valid Neighbor Solicitation message with an IPv6 address for which the node is acting as a proxy set in the Source Address field of the IPv6 packet Header.

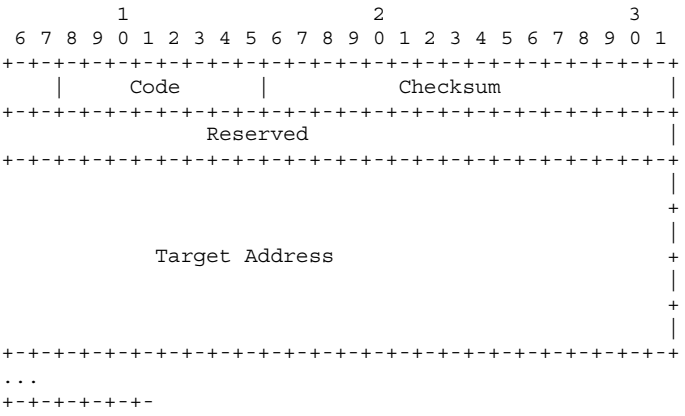
Requirement:

The IPv6 router SHOULD set the O-flag (octet 5, bit 2) to zero (0) in the Neighbor Advertisement sent in response to the solicitation.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	**Override flag**. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. **It SHOULD NOT be set** in solicited advertisements for anycast addresses and **in solicited proxy advertisements**. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8175 Form Neighbor Advertisement Header

RFC2461 4.4 RECOMMENDED

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Solicitation that does not have a unicast address in the Source Address field of the IPv6 packet header nor is the implementation acting as a proxy for the address in the Destination Address field of the header.

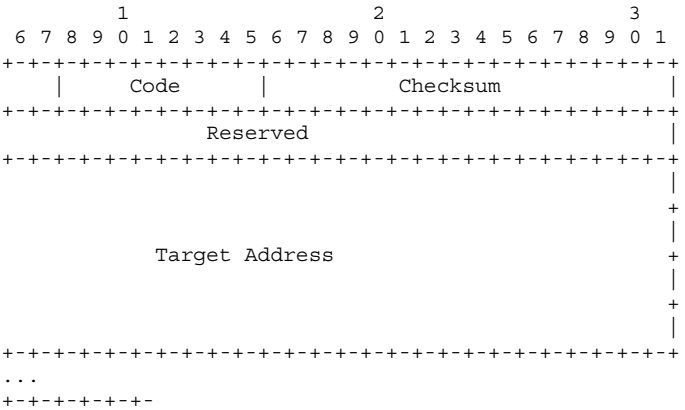
Requirement:

The IPv6 node SHOULD set the O-flag (octet 5, bit 2) to one (1) in the Neighbor Advertisement sent in response to the solicitation.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

```
ICMP Fields:

  Type           136
  Code           0
  Checksum       The ICMP checksum.  See RFC 2463.
  R              Router flag.  When set, the R-bit indicates that
                 the sender is a router.  The R-bit is used by
                 Neighbor Unreachability Detection to detect a
                 router that changes to a host.
  S              Solicited flag.  When set, the S-bit indicates that
                 the advertisement was sent in response to a
                 Neighbor Solicitation from the Destination address.
                 The S-bit is used as a reachability confirmation
                 for Neighbor Unreachability Detection.  It MUST NOT
                 be set in multicast advertisements or in
                 unsolicited unicast advertisements.
  O              Override flag.  When set, the O-bit indicates that
                 the advertisement should override an existing cache
                 entry and update the cached link-layer address.
                 When it is not set the advertisement will not
                 update a cached link-layer address though it will
                 update an existing Neighbor Cache entry for which
                 no link-layer address is known.  It SHOULD NOT be
                 set in solicited advertisements for anycast
                 addresses and in solicited proxy advertisements.
                 It SHOULD be set in other solicited advertisements
                 and in unsolicited advertisements.
  Reserved       29-bit unused field.  It MUST be initialized to
                 zero by the sender and MUST be ignored by the
                 receiver.
  Target Address
                 For solicited advertisements, the Target Address
                 field in the Neighbor Solicitation message that
                 prompted this advertisement.  For an unsolicited
                 advertisement, the address whose link-layer address
                 has changed.  The Target Address MUST NOT be a
                 multicast address.
```

RQ_000_8176 Form Unsolicited NA Header

RFC2461 4.4 RECOMMENDED

Applies to: Router, Host

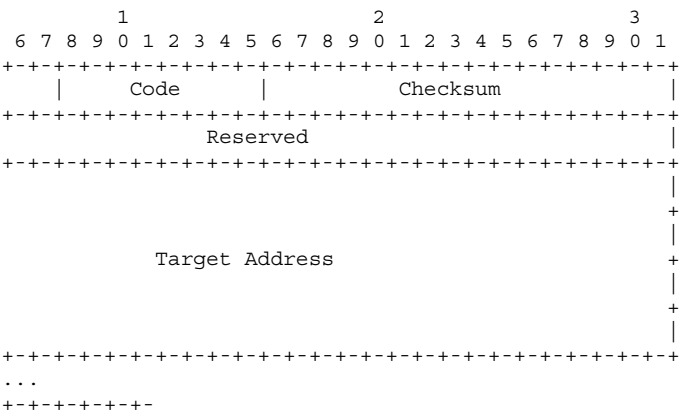
Context:

Requirement:

```
An IPv6 node SHOULD set the O-Flag (octet 5, bit 2) to one (1) in an unsolicited Neighbor
Advertisement message.
```

Specification Text:

```
Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends
unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.
```



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	**Override flag**. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. **It SHOULD be set** in other solicited advertisements and **in unsolicited advertisements**.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8177 Form Neighbor Advertisement Header

RFC2461 4.4 MANDATORY

Applies to: Router, Host

Context:

An IPv6 node receives a valid Neighbor Solicitation message.

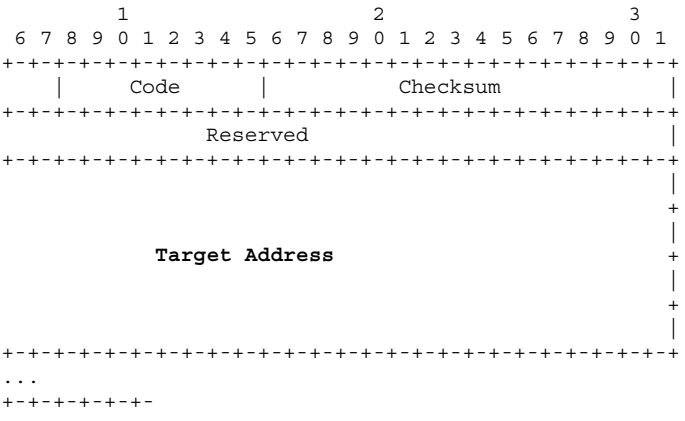
Requirement:

The IPv6 node MUST set the Target Address field in its corresponding neighbor Advertisement to the address value taken from the Target Address field in the received Neighbor Solicitation message.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	Override flag. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	**For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement.** For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8178 Form Unsolicited NA Header

RFC2461 4.4 MANDATORY

Applies to: Host, Router

Context:

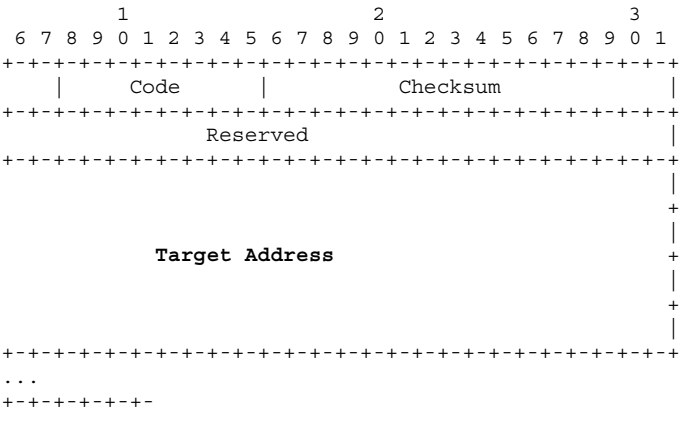
Requirement:

An IPv6 node MUST set the Target Address field in an unsolicited Neighbor Advertisement message to the IPv6 address associated link-layer address included in the Target Link-layer Address option field.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address. The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	Override flag. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. **For an unsolicited advertisement, the address whose link-layer address has changed.** The Target Address MUST NOT be a multicast address.

RQ_000_8179 Form Neighbor Advertisement Header

RFC2461 4.4 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Solicitation with a multicast IPv6 address set in the Destination Address field of the IPv6 packet header.

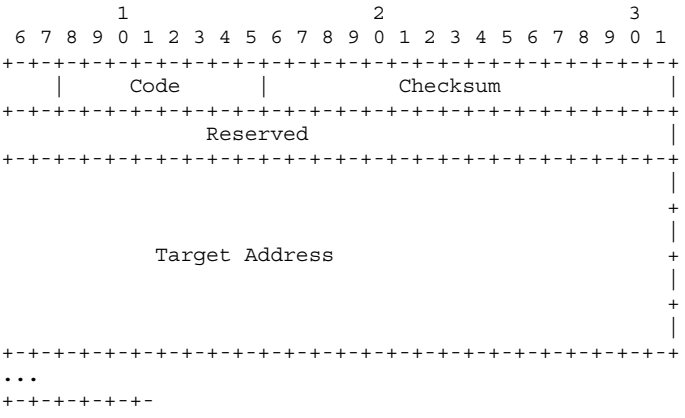
Requirement:

The IPv6 node MUST include the Target Link-layer Address Option field in the corresponding Neighbor Advertisement message if the advertisement is to be sent on a link-layer that has an address.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

Possible options:

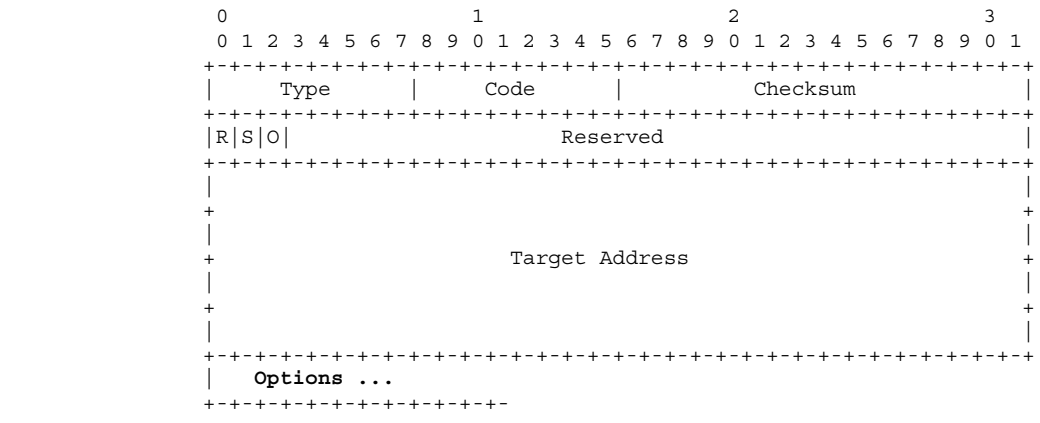
Target link-layer address
The link-layer address for the target, i.e., the sender of the advertisement. This option MUST be included on link layers that have addresses when responding to multicast solicitations. When responding to a unicast Neighbor Solicitation this option SHOULD be included.

The option MUST be included for multicast solicitations in order to avoid infinite Neighbor Solicitation "recursion" when the peer node does not have a cache entry to return a Neighbor Advertisements message. When responding to unicast solicitations, the option can be omitted since the sender of the solicitation has the correct link-layer address; otherwise it would not have be able to send the unicast solicitation in the first place. However, including the link-layer address in this case adds little overhead and eliminates a potential race condition where the sender deletes the cached link-layer address prior to receiving a response to a previous solicitation.

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.

RQ_000_8180 Form Neighbor Advertisement Header
RFC2461 4.4 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 node receives a valid Neighbor Solicitation with a multicast IPv6 address set in the Destination Address field of the IPv6 packet header.
Requirement:
The IPv6 node SHOULD include the Target Link-layer Address Option field in the corresponding Neighbor Advertisement message if the advertisement is to be sent on a link-layer that has an address.
Specification Text:
Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……
Possible options:

Target link-layer address
The link-layer address for the target, i.e., the sender of the advertisement. This option MUST be included on link layers that have addresses when responding to multicast solicitations. **When responding to a unicast Neighbor Solicitation this option SHOULD be included.**

The option MUST be included for multicast solicitations in order to avoid infinite Neighbor Solicitation "recursion" when the peer node does not have a cache entry to return a Neighbor Advertisements message. **When responding to unicast solicitations, the option can be omitted since the sender of the solicitation has the correct link-layer address; otherwise it would not have be able to send the unicast solicitation in the first place. However, including the link-layer address in this case adds little overhead and eliminates a potential race condition where the sender deletes the cached link-layer address prior to receiving a response to a previous solicitation.**

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.

RQ_000_8181 Process Option Anomalies in NA

RFC2461 4.4 MANDATORY

Applies to: Host, Router

Context:

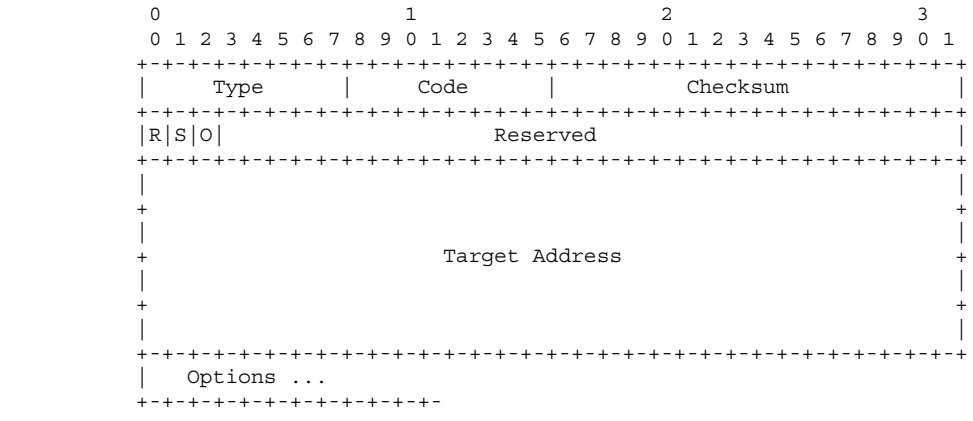
Requirement:

An IPv6 node MUST silently ignore any unrecognizable options included in a received Neighbor Advertisement message.

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

Possible options:

Target link-layer address

The link-layer address for the target, i.e., the sender of the advertisement. This option MUST be included on link layers that have addresses when responding to multicast solicitations. When responding to a unicast Neighbor Solicitation this option SHOULD be included.

The option MUST be included for multicast solicitations in order to avoid infinite Neighbor Solicitation "recursion" when the peer node does not have a cache entry to return a Neighbor Advertisements message. When responding to unicast solicitations, the option can be omitted since the sender of the solicitation has the correct link-layer address; otherwise it would not have be able to send the unicast solicitation in the first place. However, including the link-layer address in this case adds little overhead and eliminates a potential race condition where the sender deletes the cached link-layer address prior to receiving a response to a previous solicitation.

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.

RQ_000_8182 Generate Redirect Message
RFC2461 4.5 RECOMMENDED
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet from a local host. It is not the destination node and a better first hope node exists.
Requirement:
The IPv6 router SHOULD send a Redirect message in response to the received packet informing the local host of the better first hop node for the particular destination.
Specification Text:
Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.

RQ_000_8183 Generate Redirect Message
RFC2461 4.5 OPTIONAL
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet from a local host. The destination node is a neighbor of the source host.
Requirement:
The IPv6 router MAY send a Redirect packet with the Target Address field set to the same value as the Destination Address field.
Specification Text:
Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but **can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address**.

RQ_000_8184 Generate Redirect Message
RFC2461 4.5 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Redirect message, an IPv6 router MUST set fields in the IPv6 packet header as follows:

IPv6 Header Field	Value
Source Address	the link-local address assigned to the interface on which the message is to be sent
Destination Address	the Source Address of the packet triggering the Redirect
Hop Limit	255.

Specification Text:
Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.

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 the packet that triggered the redirect.

Hop Limit 255

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.

RQ_000_8185 Generate Redirect Message

RFC2461 4.5 RECOMMENDED

Applies to: Router

Context:

Requirement:

When constructing a Redirect message, an IPv6 router SHOULD include an Authentication Header in the IPv6 packet if an AH-based Security Association exists between the IPv6 node and the destination address.

Specification Text:

Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.

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 the packet that triggered the redirect.

Hop Limit 255

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.

RQ_000_8186 Generate Redirect Message

RFC2461 4.5 MANDATORY

Applies to: Router

Context:

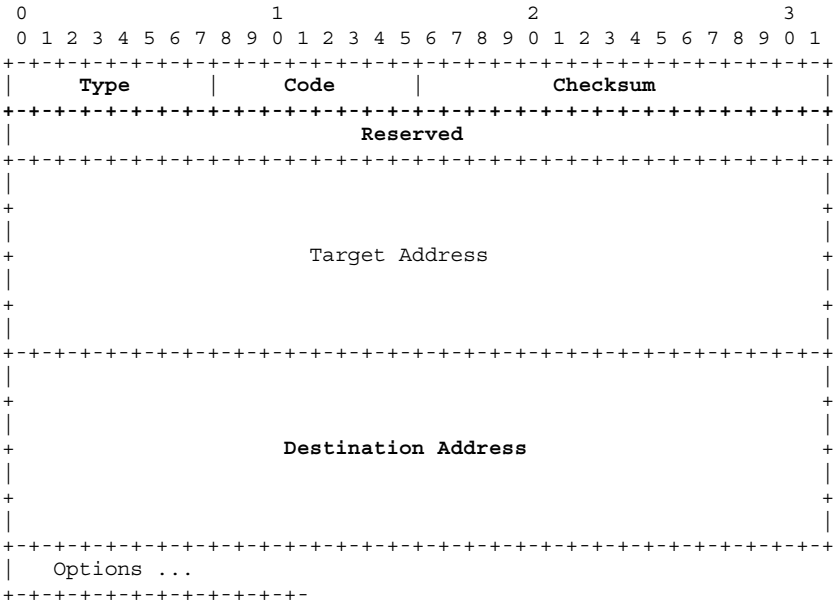
Requirement:

When constructing a Redirect message, an IPv6 router MUST set the fields in the ICMPv6 packet as follows:

ICMPv6 Field	Octets	Value
Type	1	137
Code	2	0
Checksum	3 & 4	ICMPv6 packet checksum
Reserved	5 to 8	0
Destination Address	25 to 40	The IP address of the destination node which is redirected to the target

Specification Text:

Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.



……

ICMP Fields:

Type	**137**
Code	**0**
Checksum	**The ICMP checksum. See RFC 2463**
Reserved	**This field is unused. It MUST be initialized to zero by the sender** and MUST be ignored by the receiver.
Target Address	An IP address that is a better first hop to use for the ICMP Destination Address. When the target is the actual endpoint of communication, i.e., the destination is a neighbor, the Target Address field MUST contain the same value as the ICMP Destination Address field. Otherwise the target is a better first-hop router and the Target Address MUST be the router's link-local address so that hosts can uniquely identify routers.
Destination Address	**The IP address of the destination which is redirected to the target**.

RQ_000_8187 Process Field Anomalies in Redirect Message

RFC2461 4.5 MANDATORY

Applies to: Host

Context:

Requirement:

An IPv6 host MUST ignore the contents of the Reserved field in a received Redirect message.

Specification Text:

Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.

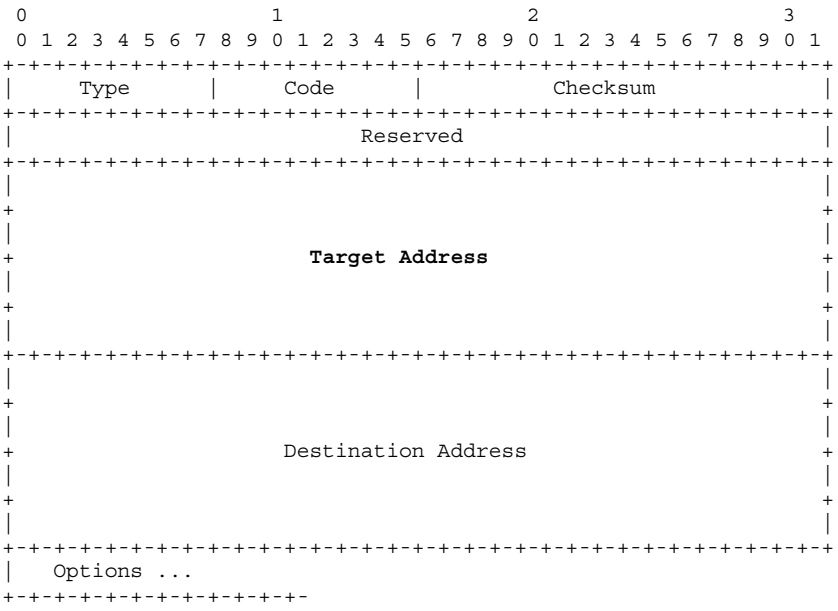
……

ICMP Fields:

Type	137
Code	0
Checksum	The ICMP checksum. See RFC 2463
Reserved	**This field is unused**. It MUST be initialized to zero by the sender and **MUST be ignored by the receiver**.
Target Address	An IP address that is a better first hop to use for the ICMP Destination Address. When the target is the actual endpoint of communication, i.e., the destination is a neighbor, the Target Address field MUST contain the same value as the ICMP Destination Address field. Otherwise the target is a better first-hop router and the Target Address MUST be the router's link-local address so that hosts can uniquely identify routers.
Destination Address	The IP address of the destination which is redirected to the target.

RQ_000_8188 Determine Redirect Target Address Field
RFC2461 4.5 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Redirect message, an IPv6 router MUST set the Target Address field to contain the IPv6 address of the router calculated to be a better first hop for future messages from the receiving node to the node whose address is contained in the Destination Address field.
Specification Text:
Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.



……

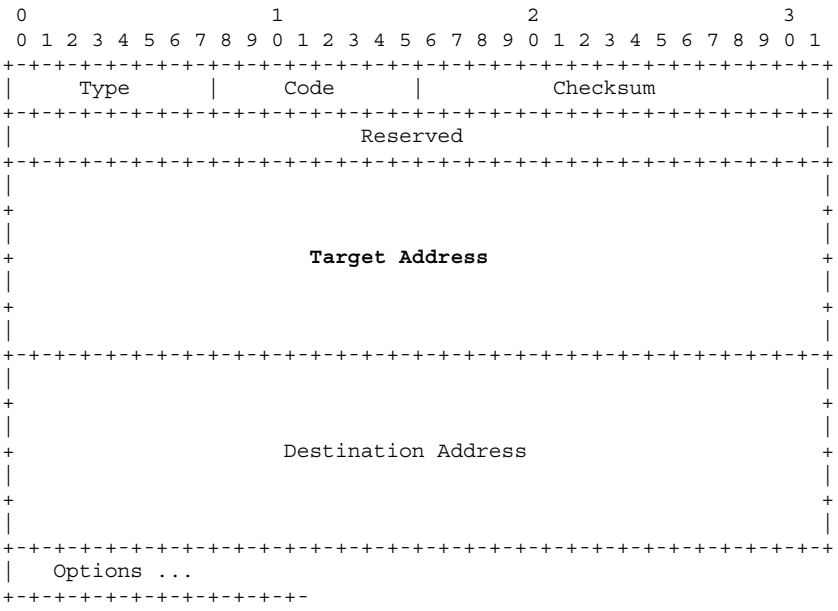
ICMP Fields:

Type	137
Code	0
Checksum	The ICMP checksum. See RFC 2463
Reserved	This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	**An IP address that is a better first hop to use for the ICMP Destination Address**. When the target is the actual endpoint of communication, i.e., the destination is a neighbor, the Target Address field MUST contain the same value as the ICMP Destination Address field. **Otherwise the target is a better first-hop router and the Target Address MUST be the router's link-local address so that hosts can uniquely identify routers**.
Destination Address	The IP address of the destination which is redirected to the target.

RQ_000_8189 Determine Redirect Target Address Field
RFC2461 4.5 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Redirect message related to a target node that is the endpoint of communication (i.e., a neighbor), an IPv6 router MUST set the Target Address field to contain the same value as the Destination Address field.

Specification Text:
Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.



……

ICMP Fields:

Type	137
Code	0
Checksum	The ICMP checksum. See RFC 2463
Reserved	This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	**An IP address that is a better first hop to use for the ICMP Destination Address. When the target is the actual endpoint of communication, i.e., the destination is a neighbor, the Target Address field MUST contain the same value as the ICMP Destination Address field**. Otherwise the target is a better first-hop router and the Target Address MUST be the router's link-local address so that hosts can uniquely identify routers.
Destination Address	The IP address of the destination which is redirected to the target.

RQ_000_8190 Generate Redirect Options
RFC2461 4.5 RECOMMENDED
Applies to: Router
Context:

Requirement:
When constructing a Redirect message to be sent to a host that is connected to a link that is not a non-broadcast multiple access (NBMA) link, an IPv6 router SHOULD include the redirection target node's link-layer address (if known) in the Target Link-layer Address option field in the Redirect.
Specification Text:
Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.

……

Possible options:

Target link-layer address
The link-layer address for the target. It SHOULD be included (if known). Note that on NBMA links, hosts may rely on the presence of the Target Link-Layer Address option in Redirect messages as the means for determining the link-layer addresses of neighbors. In such cases, the option MUST be included in Redirect messages.

Redirected Header
As much as possible of the IP packet that triggered the sending of the Redirect without making the redirect packet exceed 1280 octets.

RQ_000_8191 Generate Redirect Options

RFC2461 4.5 MANDATORY

Applies to: Router

Context:

The implementation is generating a Redirect message on an NBMA link with a known link-layer address for the target.

Requirement:

When constructing a Redirect message to be sent to a host that is connected to a non-broadcast multiple access (NBMA) link, an IPv6 router MUST include the redirection target node's link-layer address in the Target Link-layer Address option field in the Redirect.

Specification Text:

Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.

……

Possible options:

Target link-layer address
The link-layer address for the target. It SHOULD be included (if known). **Note that on NBMA links, hosts may rely on the presence of the Target Link-Layer Address option in Redirect messages as the means for determining the link-layer addresses of neighbors. In such cases, the option MUST be included in Redirect messages.**

Redirected Header
As much as possible of the IP packet that triggered the sending of the Redirect without making the redirect packet exceed 1280 octets.

RQ_000_8192 Generate Redirect Options
RFC2461 4.5 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Redirect message, an IPv6 router MUST insert as much as possible of the IP packet that triggered the sending of the Redirect without making the Redirect packet exceed 1280 octets.

Specification Text:
Routers send Redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP Target Address equal to the ICMP Destination Address.

……

Possible options:

Target link-layer address
The link-layer address for the target. It SHOULD be included (if known). Note that on NBMA links, hosts may rely on the presence of the Target Link-Layer Address option in Redirect messages as the means for determining the link-layer addresses of neighbors. In such cases, the option MUST be included in Redirect messages.

Redirected Header
As much as possible of the IP packet that triggered the sending of the Redirect without making the redirect packet exceed 1280 octets.

RQ_000_8193 Process Option Anomalies in NS

RFC2461 4.6 MANDATORY

Applies to: Host, Router

Context:

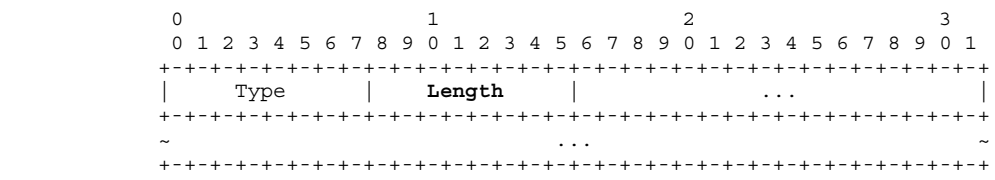
Requirement:

An IPv6 node MUST silently discard a received Neighbor solicitation message that contains an option in which the Length field is set to zero (0).

Specification Text:

Option Formats

Neighbor Discovery messages include zero or more options, some of which may appear multiple times in the same message. All options are of the form:



Fields:

Type — 8-bit identifier of the type of option. The options defined in this document are:

Option Name	Type
Source Link-Layer Address	1
Target Link-Layer Address	2
Prefix Information	3
Redirected Header	4
MTU	5

Length — **8-bit unsigned integer**. The length of the option (including the type and length fields) in units of 8 octets. **The value 0 is invalid. Nodes MUST silently discard an ND packet that contains an option with length zero**.

RQ_000_8194 Process Option Anomalies in NA

RFC2461 4.6 MANDATORY

Applies to: Host, Router

Context:

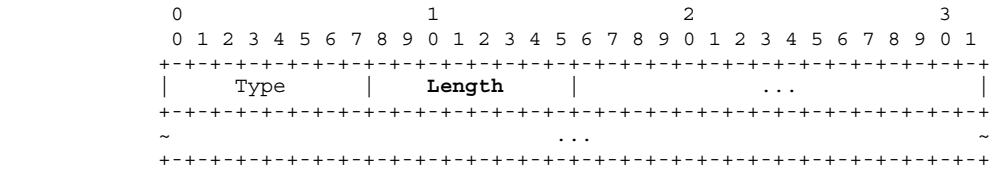
Requirement:

An IPv6 node MUST silently discard a received Neighbor Advertisement message that contains an option in which the Length field is set to zero (0).

Specification Text:

Option Formats

Neighbor Discovery messages include zero or more options, some of which may appear multiple times in the same message. All options are of the form:



Fields:

Type — 8-bit identifier of the type of option. The options defined in this document are:

Option Name	Type
Source Link-Layer Address	1
Target Link-Layer Address	2
Prefix Information	3
Redirected Header	4
MTU	5

Length — **8-bit unsigned integer**. The length of the option (including the type and length fields) in units of 8 octets. **The value 0 is invalid. Nodes MUST silently discard an ND packet that contains an option with length zero**.

RQ_000_8195 Process Option Anomalies in RS

RFC2461 4.6 MANDATORY

Applies to: Host, Router

Context:

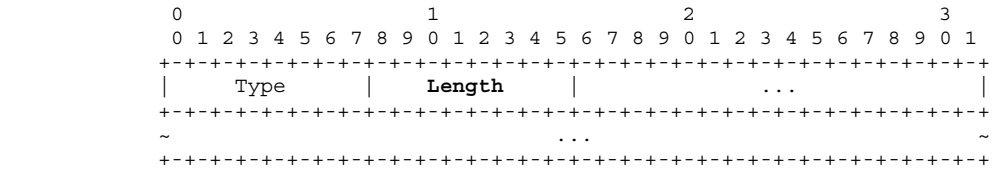
Requirement:

An IPv6 node MUST silently discard a received Router Solicitation message that contains an option in which the Length field is set to zero (0).

Specification Text:

Option Formats

Neighbor Discovery messages include zero or more options, some of which may appear multiple times in the same message. All options are of the form:



Fields:

Type — 8-bit identifier of the type of option. The options defined in this document are:

Option Name	Type
Source Link-Layer Address	1
Target Link-Layer Address	2
Prefix Information	3
Redirected Header	4
MTU	5

Length — **8-bit unsigned integer**. The length of the option (including the type and length fields) in units of 8 octets. **The value 0 is invalid. Nodes MUST silently discard an ND packet that contains an option with length zero**.

RQ_000_8196 Process Option Anomalies in RA

RFC2461 4.6 MANDATORY

Applies to: Router, Host

Context:

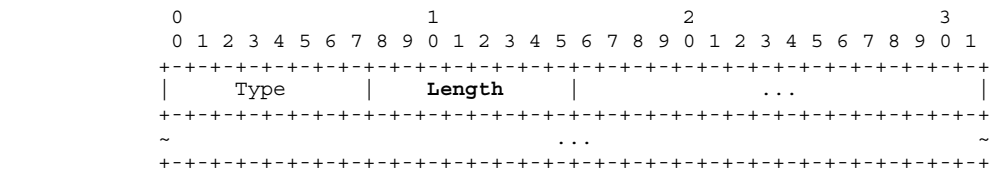
Requirement:

An IPv6 node MUST silently discard a received Router Solicitation message that contains an option in which the Length field is set to zero (0).

Specification Text:

Option Formats

Neighbor Discovery messages include zero or more options, some of which may appear multiple times in the same message. All options are of the form:



Fields:

Type — 8-bit identifier of the type of option. The options defined in this document are:

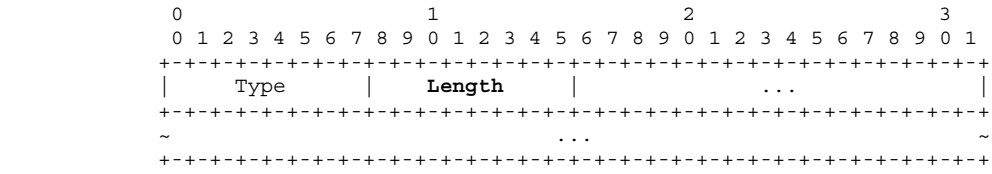
Option Name	Type
Source Link-Layer Address	1
Target Link-Layer Address	2
Prefix Information	3
Redirected Header	4
MTU	5

Length — **8-bit unsigned integer**. The length of the option (including the type and length fields) in units of 8 octets. **The value 0 is invalid. Nodes MUST silently discard an ND packet that contains an option with length zero**.

RQ_000_8197 Process Field Anomalies in Redirect Message
RFC2461 4.6 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Redirect message that contains an option in which the Length field is set to zero (0).
Specification Text:
Option Formats

Neighbor Discovery messages include zero or more options, some of which may appear multiple times in the same message. All options are of the form:



Fields:

Type 8-bit identifier of the type of option. The options defined in this document are:

Option Name	Type
Source Link-Layer Address	1
Target Link-Layer Address	2
Prefix Information	3
Redirected Header	4
MTU	5

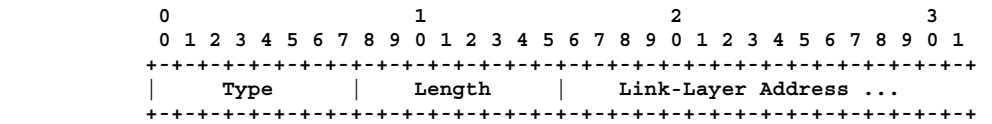
Length **8-bit unsigned integer**. The length of the option (including the type and length fields) in units of 8 octets. **The value 0 is invalid. Nodes MUST silently discard an ND packet that contains an option with length zero**.

RQ_000_8198 Generate Neighbor Solicitation Option
RFC2461 4.6.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Solicitation message containing a Source Link-Layer Address Option, an IPv6 node MUST set the option fields as follows:

Option Field	Octet	Value
Type	1	1
Length	2	Total option length in units of 8 octets
Link-Layer Address	3 to end	Source link layer address

Specification Text:
Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address
Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**

Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the **Neighbor Solicitation**, Router Solicitation, and Router Advertisement packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets.

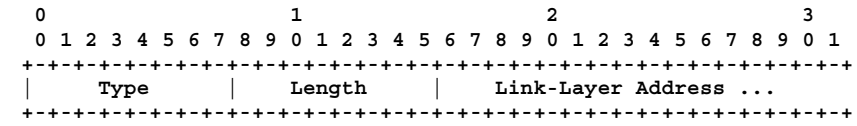
These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8199 Generate RS Source Link-Layer Address Option
RFC2461 4.6.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When constructing a Router Solicitation message containing a Source Link-Layer Address Option, an IPv6 node MUST set the option fields as follows:

Option Field	Octet	Value
Type	1	1
Length	2	Total option length in units of 8 octets
Link-Layer Address	3 to end	Source link layer address

Specification Text:
Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address
Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**
Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, **Router Solicitation,** and Router Advertisement packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets.

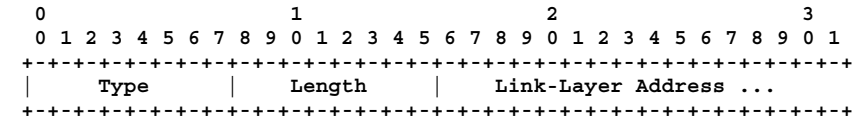
These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8200 Generate Router Advertisement
RFC2461 4.6.1 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Router Advertisement message containing a Source Link-Layer Address Option, an IPv6 node MUST set the option fields as follows:

Option Field	Octet	Value
Type	1	1
Length	2	Total option length in units of 8 octets
Link-Layer Address	3 to end	Source link layer address

Specification Text:
Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address
Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**
Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and **Router Advertisement** packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets.

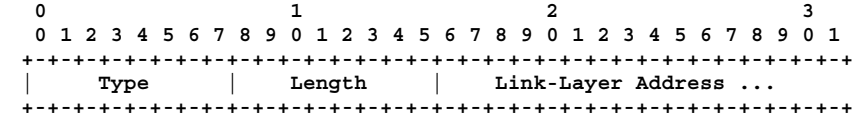
These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8201 Generate Neighbor Advertisement
RFC2461 4.6.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Advertisement message containing a Target Link-Layer Address Option, an IPv6 node MUST set the option fields as follows:

Option Field	Octet	Value
Type	1	1
Length	2	Total option length in units of 8 octets
Link-Layer Address	3 to end	Target link layer address

Specification Text:
Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address
Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**
Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and Router Advertisement packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets.

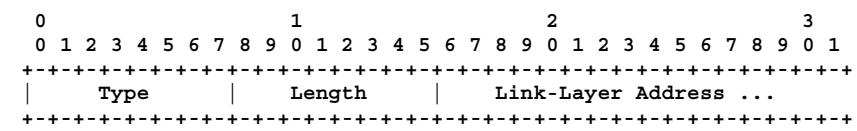
These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8202 Generate Redirect Options
RFC2461 4.6.1 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Redirect message containing a Target Link-Layer Address Option, an IPv6 node MUST set the option fields as follows:

Option Field	Octet	Value
Type	1	1
Length	2	Total option length in units of 8 octets
Link-Layer Address	3 to end	Target link layer address

Specification Text:
Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address
Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**
Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and Router Advertisement packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement **and Redirect packets**.

These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8203 Process Option Anomalies in NS

RFC2461 4.6.1 MANDATORY

Applies to: Host, Router

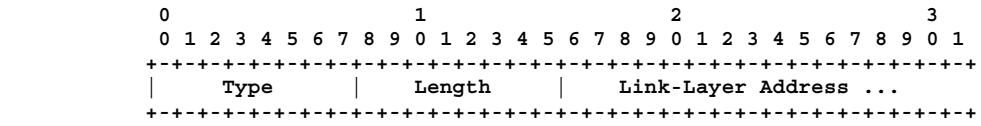
Context:

Requirement:

An IPv6 node MUST silently ignore any value set in the Target Link-Layer Address option of a received Neighbor Solicitation message

Specification Text:

Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address

Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**

Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and Router Advertisement packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets.

These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8204 Process Option Anomalies in RS

RFC2461 4.6.1 MANDATORY

Applies to: Router

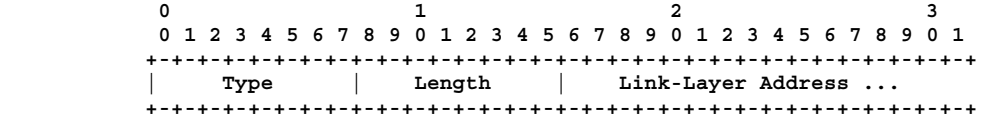
Context:

Requirement:

An IPv6 router MUST silently ignore any value set in the Target Link-Layer Address option of a received Router Solicitation message

Specification Text:

Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address
Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**
Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

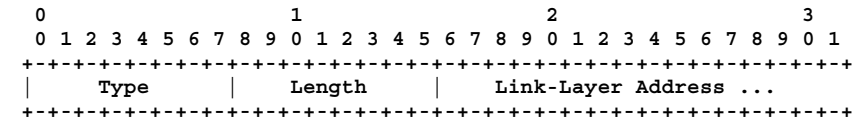
The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and Router Advertisement packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets.

These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8205 Process Option Anomalies in RA
RFC2461 4.6.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently ignore any value set in the Target Link-Layer Address option of a received Router Advertisement message
Specification Text:
Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address
Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**
Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and Router Advertisement packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets.

These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8206 Process Option Anomalies in NA

RFC2461 4.6.1 MANDATORY

Applies to: Router, Host

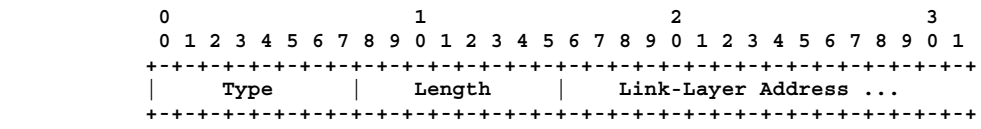
Context:

Requirement:

An IPv6 node MUST silently ignore any value set in the Source Link-Layer Address option of a received Neighbor Advertisement message

Specification Text:

Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address

Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**

Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and Router Advertisement packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets.

These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8207 Process Option Anomalies in Redirect Message

RFC2461 4.6.1 MANDATORY

Applies to: Host

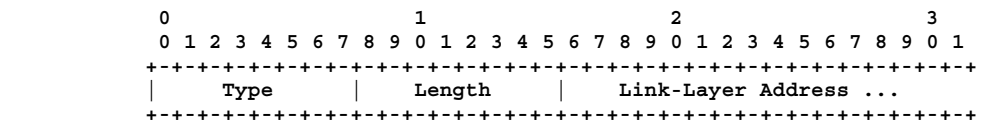
Context:

Requirement:

An IPv6 host MUST silently ignore any value set in the Source Link-Layer Address option of a received Redirect message

Specification Text:

Source/Target Link-layer Address



Fields:

Type
1 for Source Link-layer Address
2 for Target Link-layer Address

Length **The length of the option (including the type and length fields) in units of 8 octets. For example, the length for IEEE 802 addresses is 1 [RFC 2464].**

Link-Layer Address
The variable length link-layer address.
The content and format of this field (including byte and bit ordering) is expected to be specified in specific documents that describe how IPv6 operates over different link layers. For instance, RFC 2464.

Description

The Source Link-Layer Address option contains the link-layer address of the sender of the packet. It is used in the Neighbor Solicitation, Router Solicitation, and Router Advertisement packets.

The Target Link-Layer Address option contains the link-layer address of the target. It is used in Neighbor Advertisement and Redirect packets.

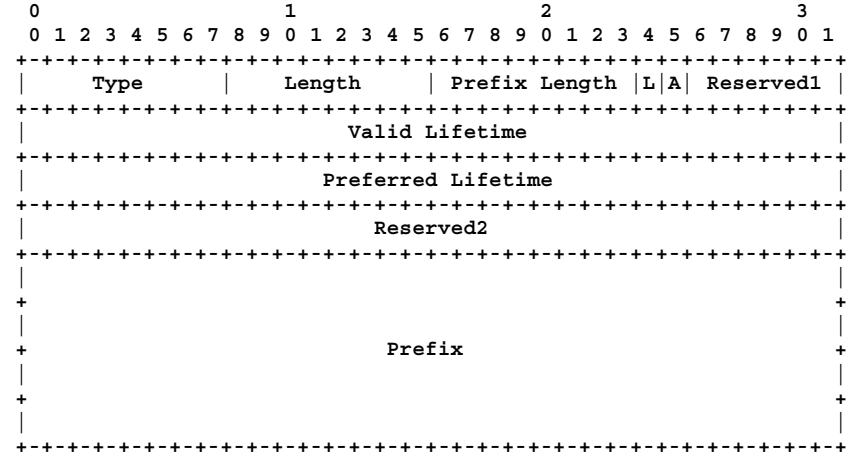
These options MUST be silently ignored for other Neighbor Discovery messages

RQ_000_8208 RA Prefix Option
RFC2461 4.6.2 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Prefix Information Option for inclusion in a Router Advertisement message, an IPv6 router MUST set the fields in the option as follows:

Field Name	Octets	Value
Type	1	3
Length	2	4
Prefix Length	3	Number of leading bits in the Prefix that are valid (0 to 128)
L-Flag	4 (bit 0)	1 if prefix can be used for on-link determination 0 otherwise
A-Flag	4 (bit 1)	1 if prefix can be used for autonomous address configuration as specified in RFC 2462
Reserved1	4 (bits 2-7)	0
Valid-Lifetime	5 to 8	The time in seconds relative to the time the Router Advertisement is sent that the prefix is valid for on-link determination
Preferred-Lifetime	9 to 12	the time in seconds relative to the time the advertisement is sent that addresses generated from the prefix by stateless autoconfiguration remain preferred
Reserved2	13 to 16	0
Prefix	17 to 32	High order bits defined by Prefix Length field: IP Address or Prefix Remaining low-order bits: 0

Specification Text:
Prefix Information



Fields:

Type	**3**
Length	**4**
Prefix Length	**8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.**
L	**1-bit on-link flag. When set, indicates that this prefix can be used for on-link determination. When not set the advertisement makes no statement about on-link or off-link properties of the prefix. For instance, the prefix might be used for address configuration with some of the addresses belonging to the prefix being on-link and others being off-link.**
A	**1-bit autonomous address-configuration flag. When set indicates that this prefix can be used for autonomous address configuration as specified in RFC 2462.**
Reserved1	**6-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.**
Valid Lifetime	**32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity. The Valid Lifetime is also used by RFC 2462.**
Preferred Lifetime	**32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred (RFC 2462). A value of all one bits (0xffffffff) represents infinity. See RFC 2462.**
Reserved2	**This field is unused. It MUST be initialized 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**. A router SHOULD NOT send a prefix option for the link-local prefix and a host SHOULD ignore such a prefix option.

RQ_000_8209 Process Option Anomalies in RA

RFC2461 4.6.2 MANDATORY

Applies to: Router, Host

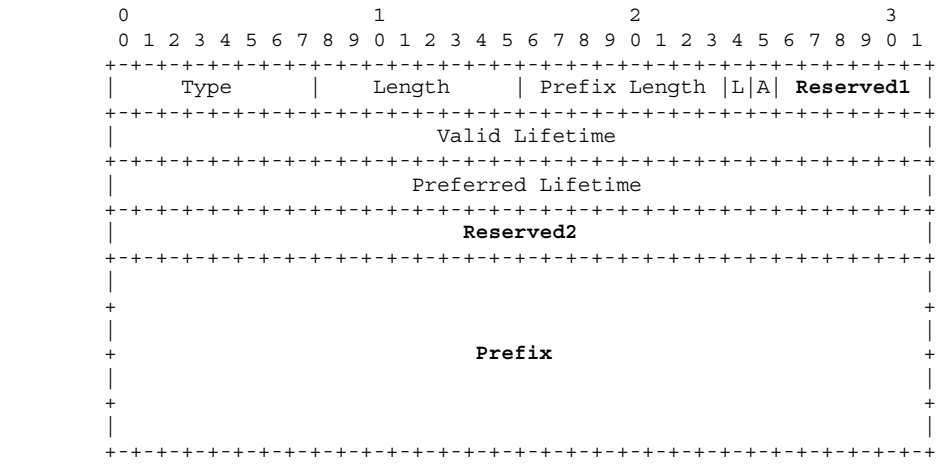
Context:

Requirement:

An IPv6 node MUST ignore any value in the Reserved1 and Reserved2 fields and the bits after the prefix length in the Prefix field in the Prefix Information Option of a received Router Advertisement message.

Specification Text:

Prefix Information



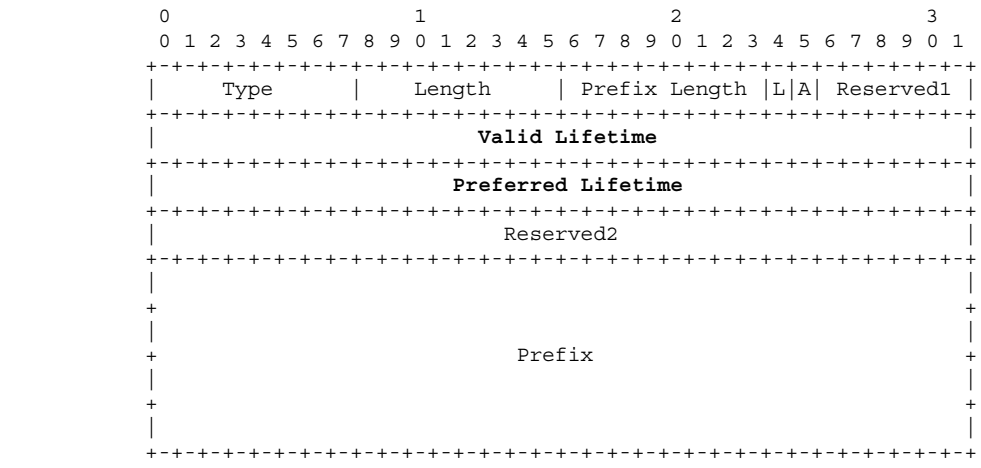
Fields:

Type	3
Length	4
Prefix Length	8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.
L	1-bit on-link flag. When set, indicates that this prefix can be used for on-link determination. When not set the advertisement makes no statement about on-link or off-link properties of the prefix. For instance, the prefix might be used for address configuration with some of the addresses belonging to the prefix being on-link and others being off-link.
A	1-bit autonomous address-configuration flag. When set indicates that this prefix can be used for autonomous address configuration as specified in RFC 2462.
Reserved1	**6-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.**
Valid Lifetime	32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity. The Valid Lifetime is also used by RFC 2462.
Preferred Lifetime	32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred (RFC 2462). A value of all one bits (0xffffffff) represents infinity. See RFC 2462.
Reserved2	**This field is unused. It MUST be initialized 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**. A router SHOULD NOT send a prefix option for the link-local prefix and a host SHOULD ignore such a prefix option.

RQ_000_8210 Router Processing of RA
RFC2461 4.6.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST interpret the hexadecimal value FFFFFFFF as infinity if it is set in either (or both) the Valid Lifetime or Preferred Lifetime fields in the Prefix Information option of a received Router Advertisement message.

Specification Text:
Prefix Information



Fields:

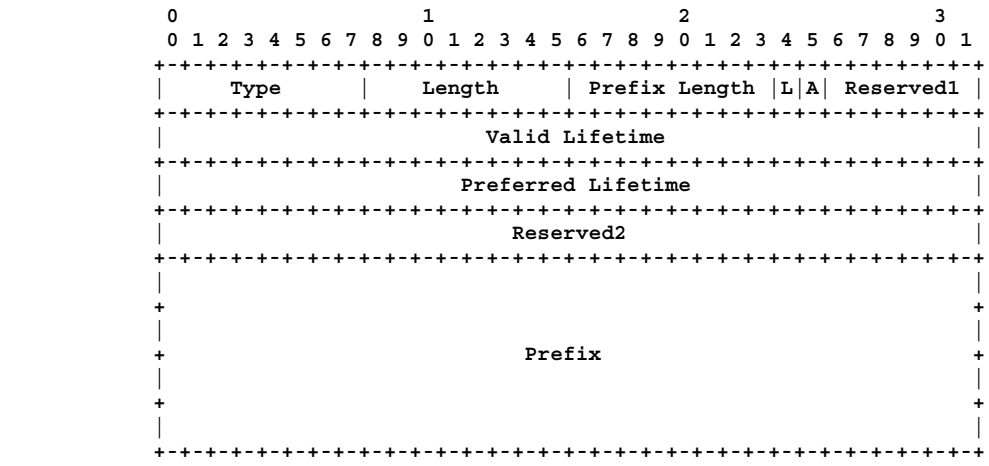
Type	3
Length	4
Prefix Length	8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.
L	1-bit on-link flag. When set, indicates that this prefix can be used for on-link determination. When not set the advertisement makes no statement about on-link or off-link properties of the prefix. For instance, the prefix might be used for address configuration with some of the addresses belonging to the prefix being on-link and others being off-link.
A	1-bit autonomous address-configuration flag. When set indicates that this prefix can be used for autonomous address configuration as specified in RFC 2462.
Reserved1	6-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Valid Lifetime	32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. **A value of all one bits (0xffffffff) represents infinity.** The Valid Lifetime is also used by RFC 2462.
Preferred Lifetime	32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred (RFC 2462). **A value of all one bits (0xffffffff) represents infinity.** See RFC 2462.
Reserved2	This field is unused. It MUST be initialized 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.  A router SHOULD NOT send a prefix
                option for the link-local prefix and a host SHOULD
                ignore such a prefix option.
```

RQ_000_8211 Form Router Advertisement Options
RFC2461 4.6.2 RECOMMENDED
Applies to: Router
Context:

Requirement:
An IPv6 router SHOULD NOT send a Router Advertisement containing a Prefix Information option for the link-local prefix (FF02:x).

Specification Text:
Prefix Information




```
Fields:

 Type           3
 Length         4
 Prefix Length  8-bit unsigned integer.  The number of leading bits
                in the Prefix that are valid.  The value ranges
                from 0 to 128.
 L              1-bit on-link flag.  When set, indicates that this
                prefix can be used for on-link determination.  When
                not set the advertisement makes no statement about
                on-link or off-link properties of the prefix.  For
                instance, the prefix might be used for address
                configuration with some of the addresses belonging
                to the prefix being on-link and others being off-
                link.
 A              1-bit autonomous address-configuration flag.  When
                set indicates that this prefix can be used for
                autonomous address configuration as specified in
                RFC 2462.
 Reserved1      6-bit unused field.  It MUST be initialized to zero
                by the sender and MUST be ignored by the receiver.
 Valid Lifetime
                32-bit unsigned integer.  The length of time in
                seconds (relative to the time the packet is sent)
                that the prefix is valid for the purpose of on-link
                determination.  A value of all one bits
                (0xffffffff) represents infinity.  The Valid
                Lifetime is also used by RFC 2462.
 Preferred Lifetime
                32-bit unsigned integer.  The length of time in
                seconds (relative to the time the packet is sent)
                that addresses generated from the prefix via
                stateless address autoconfiguration remain
                preferred (RFC 2462).  A value of all one bits
                (0xffffffff) represents infinity.  See RFC 2462.
```

```
Reserved2       This field is unused.  It MUST be initialized 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.  A router SHOULD NOT send a prefix
                option for the link-local prefix and a host SHOULD
                ignore such a prefix option.
```

RQ_000_8212 Process Router Advertisement

RFC2461 4.6.2 RECOMMENDED

Applies to: Host

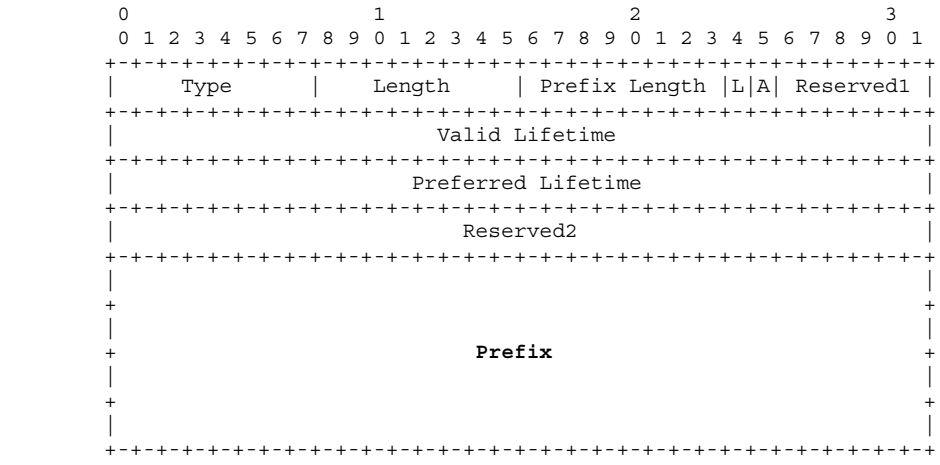
Context:

Requirement:

An IPv6 node SHOULD ignore the contents of the Prefix field in the Prefix Information Option of a received Router Advertisement message if it is set to the link-local prefix (FF02:x).

Specification Text:

Prefix Information



Fields:

```
Type            3
Length          4
Prefix Length   8-bit unsigned integer.  The number of leading bits
                in the Prefix that are valid.  The value ranges
                from 0 to 128.
L               1-bit on-link flag.  When set, indicates that this
                prefix can be used for on-link determination.  When
                not set the advertisement makes no statement about
                on-link or off-link properties of the prefix.  For
                instance, the prefix might be used for address
                configuration with some of the addresses belonging
                to the prefix being on-link and others being off-
                link.
A               1-bit autonomous address-configuration flag.  When
                set indicates that this prefix can be used for
                autonomous address configuration as specified in
                RFC 2462.
Reserved1       6-bit unused field.  It MUST be initialized to zero
                by the sender and MUST be ignored by the receiver.
Valid Lifetime
                32-bit unsigned integer.  The length of time in
                seconds (relative to the time the packet is sent)
                that the prefix is valid for the purpose of on-link
                determination.  A value of all one bits
                (0xffffffff) represents infinity.  The Valid
                Lifetime is also used by RFC 2462.
```

Preferred Lifetime
32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred (RFC 2462). A value of all one bits (0xffffffff) represents infinity. See RFC 2462.

Reserved2 This field is unused. It MUST be initialized 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. A router SHOULD NOT send a prefix option for the link-local prefix and **a host SHOULD ignore such a prefix option**.

RQ_000_8213 Process Option Anomalies in NS

RFC2461 4.6.2 MANDATORY

Applies to: Host, Router

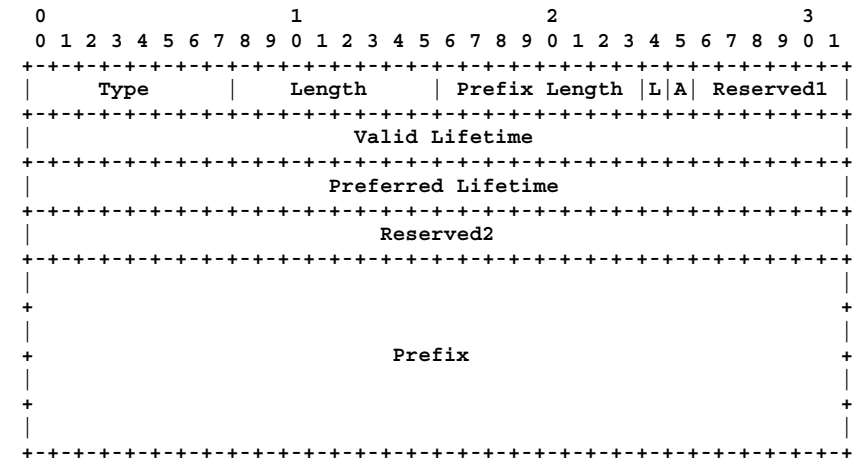
Context:

Requirement:

An IPv6 node MUST silently ignore a Prefix Information option received in a Neighbor Solicitation message.

Specification Text:

Prefix Information



……

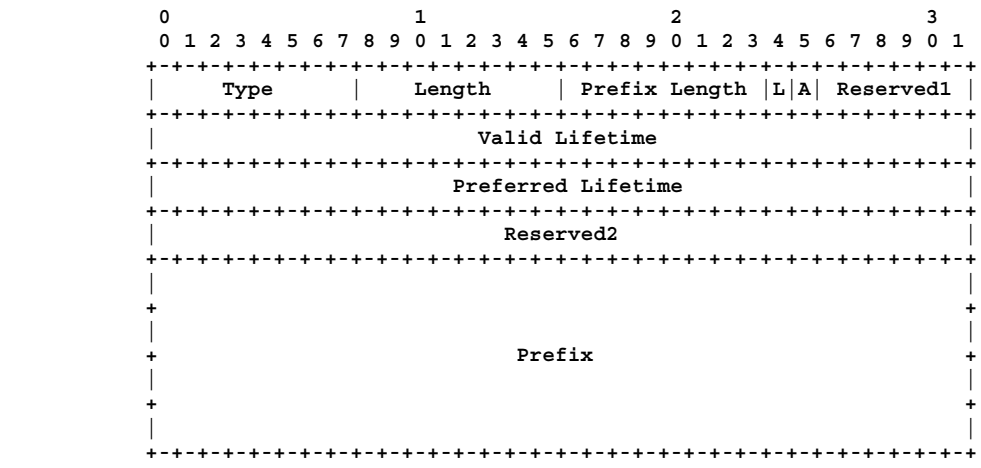
Description

The Prefix Information option provide hosts with on-link prefixes and prefixes for Address Autoconfiguration.

The Prefix Information option appears in Router Advertisement packets and MUST be silently ignored for other messages.

RQ_000_8214 Process Option Anomalies in NA
RFC2461 4.6.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently ignore a Prefix Information option received in a Neighbor Advertisement message.
Specification Text:
Prefix Information

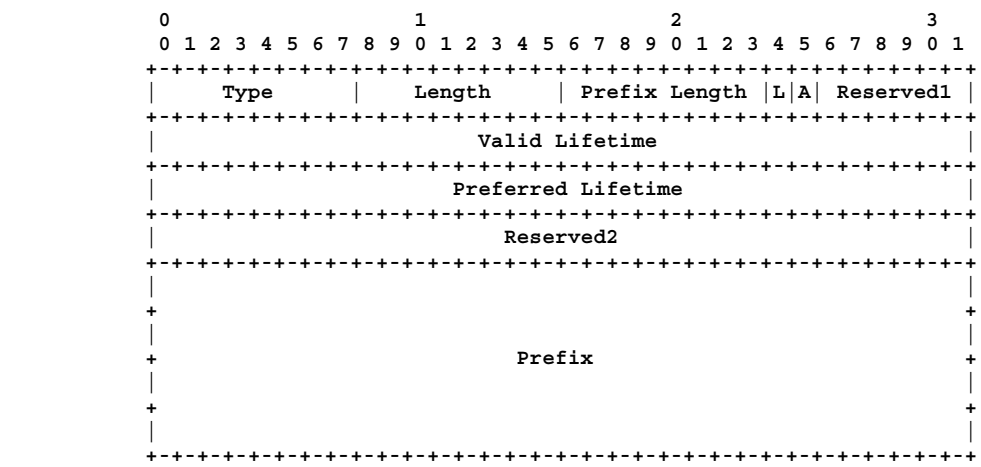


……
Description
The Prefix Information option provide hosts with on-link prefixes and prefixes for Address Autoconfiguration.

The Prefix Information option appears in Router Advertisement packets and MUST be silently ignored for other messages.

RQ_000_8215 Process Option Anomalies in RS
RFC2461 4.6.2 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently ignore a Prefix Information option received in a Router Solicitation message.
Specification Text:
Prefix Information



……
Description
The Prefix Information option provide hosts with on-link prefixes and prefixes for Address Autoconfiguration.

The Prefix Information option appears in Router Advertisement packets and MUST be silently ignored for other messages.

RQ_000_8216 Process Option Anomalies in Redirect Message

RFC2461 4.6.2 MANDATORY

Applies to: Host

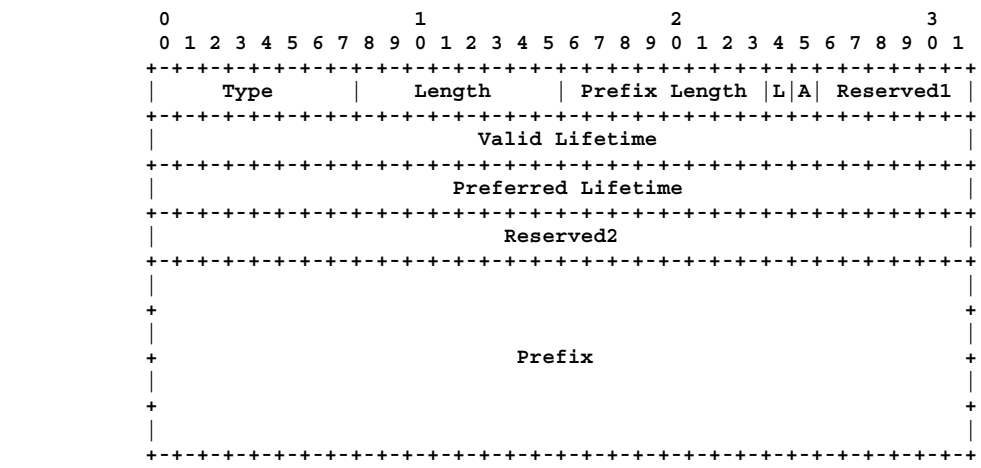
Context:

Requirement:

An IPv6 host MUST silently ignore a Prefix Information option received in a Redirect message.

Specification Text:

Prefix Information



……

Description

The Prefix Information option provide hosts with on-link prefixes and prefixes for Address Autoconfiguration.

The Prefix Information option appears in Router Advertisement packets and MUST be silently ignored for other messages.

RQ_000_8217 Generate Redirect Options

RFC2461 4.6.3 MANDATORY

Applies to: Router

Context:

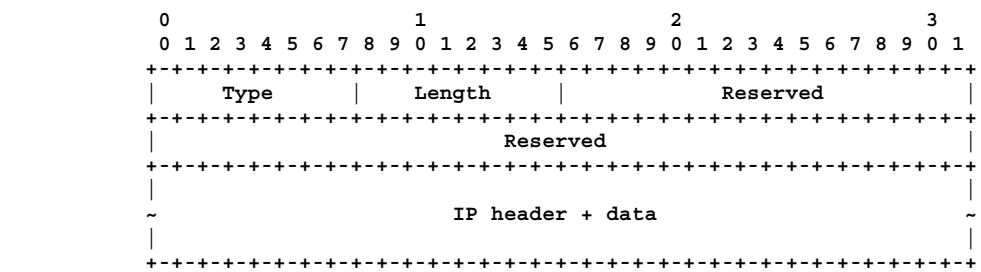
Requirement:

When constructing a Redirect Header option for inclusion in a Redirect message, an IPv6 router MUST set the fields in the Redirect Header option as follows:

Field Name	Octets	Value
Type	1	4
Length	2	Length of the option in units of 8 octets
Reserved	3 to 8	0
IP Header & Data	9 to end	Original packet truncated, if necessary, to fit within 1280 octets

Specification Text:

Redirected Header



Fields:

Type	**4**
Length	**The length of the option in units of 8 octets.**
Reserved	**These fields are unused. They MUST be initialized to zero by the sender** and MUST be ignored by the receiver.
IP header + data	**The original packet truncated to ensure that the size of the redirect message does not exceed 1280 octets.**

RQ_000_8218 Process Option Anomalies in Redirect Message

RFC2461 4.6.3 MANDATORY

Applies to: Host

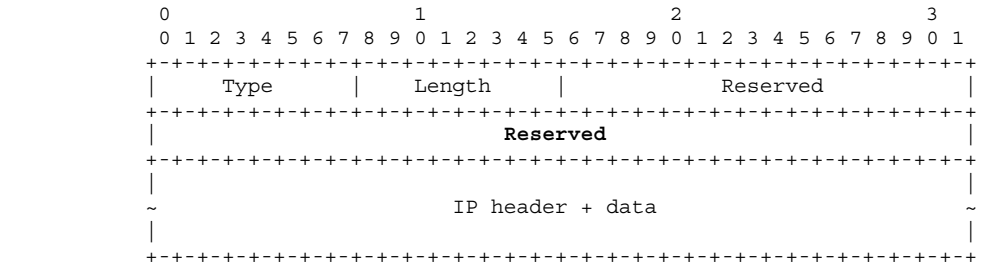
Context:

Requirement:

An IPv6 host MUST ignore any value set in the Reserved field in the Redirected Header option of a received Redirect message.

Specification Text:

Redirected Header



Fields:

Type	4
Length	The length of the option in units of 8 octets.
Reserved	**These fields are unused.** They MUST be initialized to zero by the sender and **MUST be ignored by the receiver.**
IP header + data	The original packet truncated to ensure that the size of the redirect message does not exceed 1280 octets.

RQ_000_8219 Process Option Anomalies in NS

RFC2461 4.6.3 MANDATORY

Applies to: Router, Host

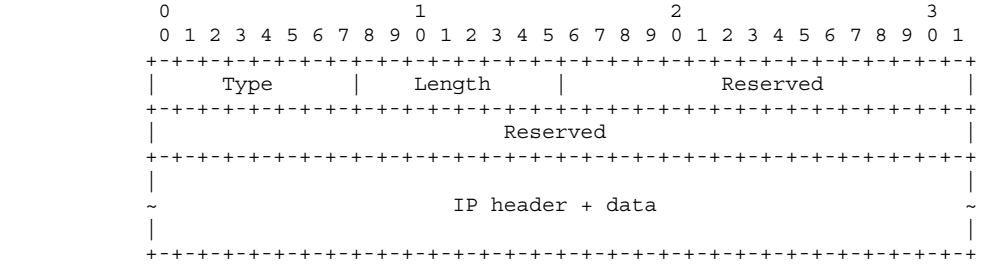
Context:

Requirement:

An IPv6 node MUST silently ignore a Redirected Header option received in a Neighbor Solicitation message.

Specification Text:

Redirected Header



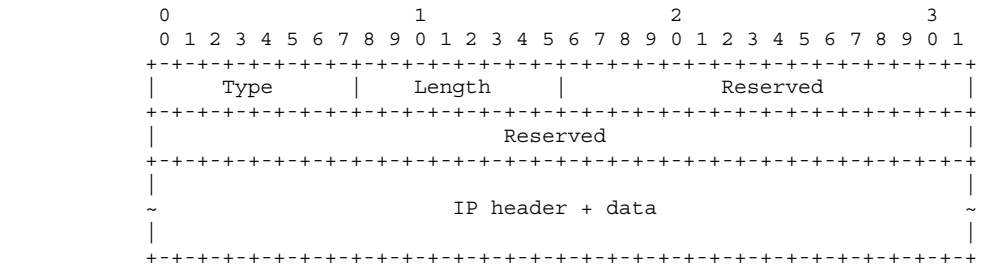
……

Description
The Redirected Header option is used in Redirect messages and contains all or part of the packet that is being redirected.

This option MUST be silently ignored for other Neighbor Discovery messages.

RQ_000_8220 Process Option Anomalies in NA
RFC2461 4.6.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently ignore a Redirected Header option received in a Neighbor Advertisement message.
Specification Text:
Redirected Header



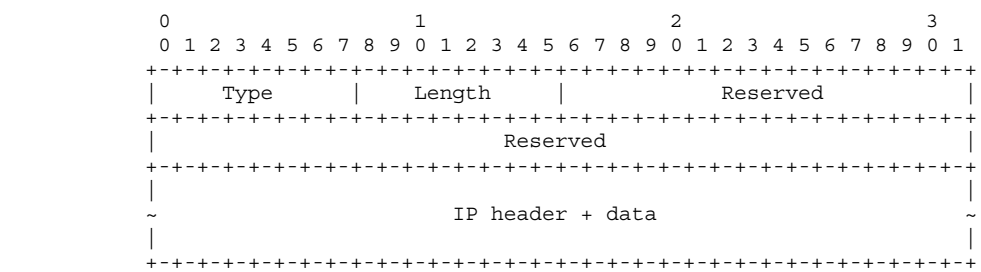
……

Description
The Redirected Header option is used in Redirect messages and contains all or part of the packet that is being redirected.

This option MUST be silently ignored for other Neighbor Discovery messages.

RQ_000_8221 Process Option Anomalies in RA
RFC2461 4.6.3 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently ignore a Redirected Header option received in a Router Advertisement message.
Specification Text:
Redirected Header



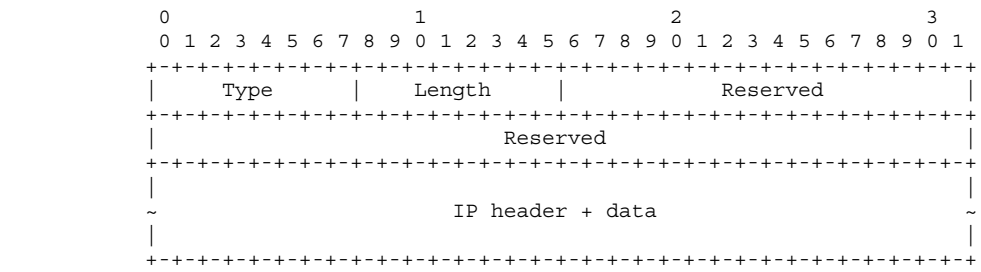
……

Description
The Redirected Header option is used in Redirect messages and contains all or part of the packet that is being redirected.

This option MUST be silently ignored for other Neighbor Discovery messages.

RQ_000_8222 Process Option Anomalies in RS
RFC2461 4.6.3 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently ignore a Redirected Header option received in a Router Solicitation message.
Specification Text:
Redirected Header



……

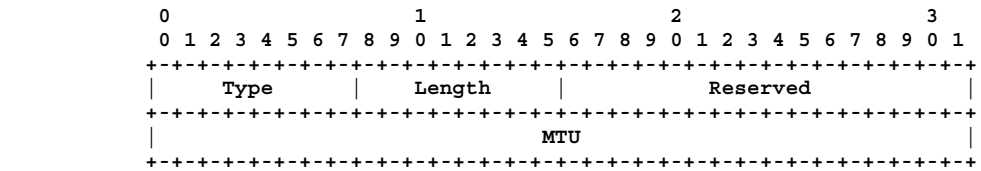
Description
The Redirected Header option is used in Redirect messages and contains all or part of the packet that is being redirected.

This option MUST be silently ignored for other Neighbor Discovery messages.

RQ_000_8223 RA MTU Option
RFC2461 4.6.4 MANDATORY
Applies to: Router
Context:
The implementation is generating a Router Advertisement containing an MTU option.
Requirement:
When constructing an MTU option for inclusion in a Router advertisement message, an IPv6 router MUST set the fields in the MTU option as follows:

Field Name	Octets	Value
Type	1	5
Length	2	1
Reserved	3 to 4	0
MTU	5 to 8	The recommended MTU for the link

Specification Text:
MTU

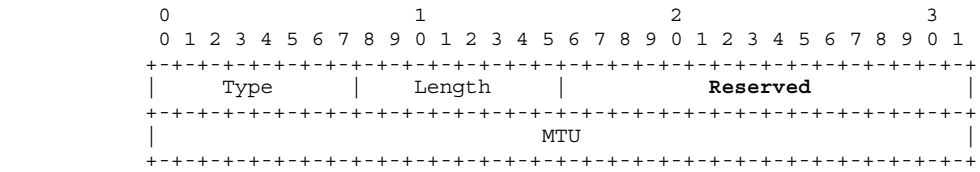


Fields:

Type	**5**
Length	**1**
Reserved	**This field is unused. It MUST be initialized to zero by the sender** and MUST be ignored by the receiver.
MTU	**32-bit unsigned integer. The recommended MTU for the link.**

RQ_000_8224 Process Option Anomalies in RA
RFC2461 4.6.3 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST ignore the contents of the Reserved field in the MTU option of a received Router Advertisement message.
Specification Text:
MTU

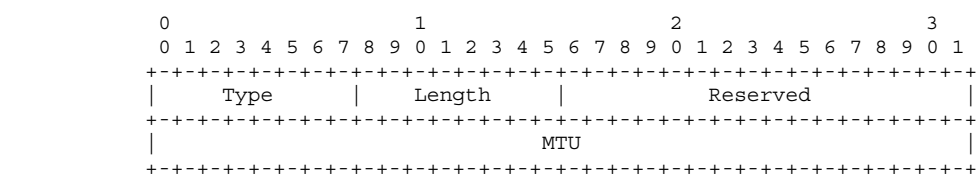


Fields:

Type	5
Length	1
Reserved	**This field is unused.** It MUST be initialized to zero by the sender **and MUST be ignored by the receiver.**
MTU	32-bit unsigned integer. The recommended MTU for the link.

RQ_000_8225 Process Option Anomalies in NA
RFC2461 4.6.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently ignore an MTU option received in a neighbor Advertisement message.
Specification Text:
MTU



……

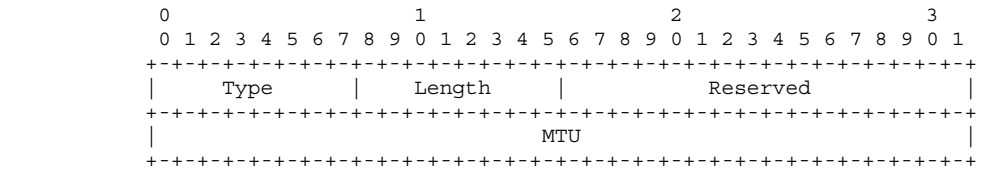
Description
The MTU option is used in Router Advertisement messages to insure that all nodes on a link use the same MTU value in those cases where the link MTU is not well known.

This option MUST be silently ignored for other Neighbor Discovery messages.

In configurations in which heterogeneous technologies are bridged together, the maximum supported MTU may differ from one segment to another. If the bridges do not generate ICMP Packet Too Big messages, communicating nodes will be unable to use Path MTU to dynamically determine the appropriate MTU on a per-neighbor basis. In such cases, routers use the MTU option to specify the maximum MTU value that is supported by all segments.

RQ_000_8226 Process Option Anomalies in NS
RFC2461 4.6.4 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently ignore an MTU option received in a neighbor Solicitation message.
Specification Text:
MTU



……

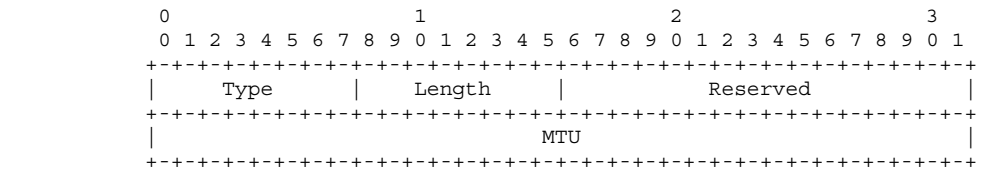
Description
The MTU option is used in Router Advertisement messages to insure that all nodes on a link use the same MTU value in those cases where the link MTU is not well known.

This option MUST be silently ignored for other Neighbor Discovery messages.

In configurations in which heterogeneous technologies are bridged together, the maximum supported MTU may differ from one segment to another. If the bridges do not generate ICMP Packet Too Big messages, communicating nodes will be unable to use Path MTU to dynamically determine the appropriate MTU on a per-neighbor basis. In such cases, routers use the MTU option to specify the maximum MTU value that is supported by all segments.

RQ_000_8227 Process Option Anomalies in RS
RFC2461 4.6.4 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently ignore an MTU option received in a Router Solicitation message.
Specification Text:
MTU



……

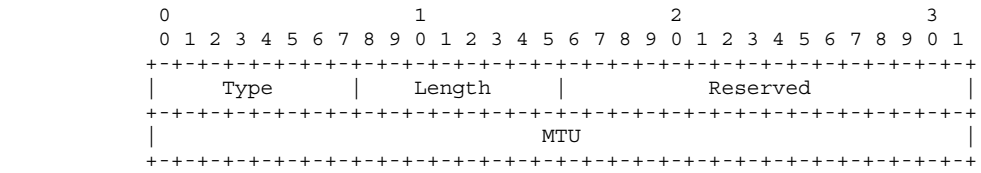
Description
The MTU option is used in Router Advertisement messages to insure that all nodes on a link use the same MTU value in those cases where the link MTU is not well known.

This option MUST be silently ignored for other Neighbor Discovery messages.

In configurations in which heterogeneous technologies are bridged together, the maximum supported MTU may differ from one segment to another. If the bridges do not generate ICMP Packet Too Big messages, communicating nodes will be unable to use Path MTU to dynamically determine the appropriate MTU on a per-neighbor basis. In such cases, routers use the MTU option to specify the maximum MTU value that is supported by all segments.

RQ_000_8228 Process Option Anomalies in Redirect Message
RFC2461 4.6.4 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently ignore an MTU option received in a Redirect message.
Specification Text:
MTU



……

Description
The MTU option is used in Router Advertisement messages to insure that all nodes on a link use the same MTU value in those cases where the link MTU is not well known.

This option MUST be silently ignored for other Neighbor Discovery messages.

In configurations in which heterogeneous technologies are bridged together, the maximum supported MTU may differ from one segment to another. If the bridges do not generate ICMP Packet Too Big messages, communicating nodes will be unable to use Path MTU to dynamically determine the appropriate MTU on a per-neighbor basis. In such cases, routers use the MTU option to specify the maximum MTU value that is supported by all segments.

RQ_000_8231 Host Processing of RA
RFC2461 5.4 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
An IPv6 node SHOULD retain at least two entries in its Default Router List and Prefix List until after their lifetimes expire.
Specification Text:
A node should retain entries in the Default Router List and the Prefix List until their lifetimes expire. However, a node may garbage collect entries prematurely if it is low on memory. If not all routers are kept on the Default Router list, **a node should retain at least two entries in the Default Router List (and preferably more) in order to maintain robust connectivity for off-link destinations**.

RQ_000_8232 Next Hop Determination
RFC2461 5.4 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
When a router is removed from the Default Router List, an IPv6 node MAY perform next-hop determination for any entries in the Destination Cache that use the removed router.
Specification Text:
When removing an entry from the Prefix List there is no need to purge any entries from the Destination or Neighbor Caches. Neighbor Unreachability Detection will efficiently purge any entries in these caches that have become invalid. **When removing an entry from the Default Router List, however, any entries in the Destination Cache that go through that router must perform next-hop determination again to select a new default router.**

RQ_000_8233 Host Processing of RS
RFC2461 6.1.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard any received Router Solicitation messages.
Specification Text:
Hosts MUST silently discard any received Router Solicitation Messages.

RQ_000_8234 Process Field Anomalies in RS
RFC2461 6.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently discard a received Router Solicitation message if the Hop Limit field in the IPv6 packet header is not set to the decimal value 255.
Specification Text:
A router MUST silently discard any received Router Solicitation messages that do not satisfy all of the following validity checks:

- **The IP Hop Limit field has a value of 255**, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 8 or more octets.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8235 Process Field Anomalies in RS
RFC2461 6.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently discard a received Router Solicitation message containing an Authentication Header if the packet fails authentication.
Specification Text:
A router MUST silently discard any received Router Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- **If the message includes an IP Authentication Header, the message authenticates correctly.**
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 8 or more octets.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8236 Process Field Anomalies in RS
RFC2461 6.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently discard a received Router Solicitation message containing an invalid ICMPv6 checksum.

Specification Text:
A router MUST silently discard any received Router Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- **ICMP Checksum is valid.**
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 8 or more octets.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8237 Process Field Anomalies in RS
RFC2461 6.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently discard a received Router Solicitation message in which the ICMPv6 Code field is set to zero (0)
Specification Text:
A router MUST silently discard any received Router Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- **ICMP Code is 0.**
- ICMP length (derived from the IP length) is 8 or more octets.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8238 Process Field Anomalies in RS
RFC2461 6.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently discard a received Router Solicitation message in which the length of the ICMPv6 packet is less than 8 octets
Specification Text:
A router MUST silently discard any received Router Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- **ICMP length (derived from the IP length) is 8 or more octets.**
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8239 Process Option Anomalies in RS
RFC2461 6.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently discard a received Router Solicitation message in which the length of any included option is zero (0)

Specification Text:
A router MUST silently discard any received Router Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 8 or more octets.
- **All included options have a length that is greater than zero.**
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8240 Process Option Anomalies in RS
RFC2461 6.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST silently discard a received Router Solicitation in which the IPv6 Source Address field is set to the Unspecified Address (0:0:0:0:0:0:0:0) but no Source Link-layer Address option is included in the solicitation.
Specification Text:
A router MUST silently discard any received Router Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 8 or more octets.
- All included options have a length that is greater than zero.
- **If the IP source address is the unspecified address, there is no source link-layer address option in the message.**

RQ_000_8241 Process Option Anomalies in RS
RFC2461 6.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST ignore the contents of an unrecognized option contained in a received Router Solicitation message.
Specification Text:
The contents of the Reserved field, and **of any unrecognized options, MUST be ignored**. Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values.

RQ_000_8242 Process Option Anomalies in RS
RFC2461 6.1.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST ignore any option contained in a received Router Solicitation message but which is not valid in a Router Solicitation.
Specification Text:
The contents of any defined options that are not specified to be used with Router Solicitation messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Source Link-Layer Address option.

RQ_000_8244 Process Field Anomalies in RA
RFC2461 6.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Router Advertisement message if the Source Address field of the containing IPv6 packet header is not set to a link-local address.
Specification Text:
A node MUST silently discard any received Router Advertisement messages that do not satisfy all of the following validity checks:

- **IP Source Address is a link-local address.** Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers.

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.

- If the message includes an IP Authentication Header, the message authenticates correctly.

- ICMP Checksum is valid.

- ICMP Code is 0.

- ICMP length (derived from the IP length) is 16 or more octets.

- All included options have a length that is greater than zero.

RQ_000_8245 Process Field Anomalies in RA
RFC2461 6.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently discard a received Router Advertisement message if the Hop Limit field in the containing IPv6 packet header is not set to the decimal value 255.
Specification Text:
A node MUST silently discard any received Router Advertisement messages that do not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers.
- **The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.**
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 16 or more octets.
- All included options have a length that is greater than zero.

RQ_000_8246 Process Field Anomalies in RA
RFC2461 6.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Router Advertisement message containing an Authentication Header if the packet fails authentication.

Specification Text:
A node MUST silently discard any received Router Advertisement messages that do not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers.
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- **If the message includes an IP Authentication Header, the message authenticates correctly.**
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 16 or more octets.
- All included options have a length that is greater than zero.

RQ_000_8247 Process Field Anomalies in RA
RFC2461 6.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently discard a received Router Advertisement message containing an invalid ICMPv6 checksum.
Specification Text:
A node MUST silently discard any received Router Advertisement messages that do not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers.
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- **ICMP Checksum is valid.**
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 16 or more octets.
- All included options have a length that is greater than zero.

RQ_000_8248 Process Field Anomalies in RA
RFC2461 6.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently discard a received Router Advertisement message in which the ICMPv6 Code field is set to zero (0)
Specification Text:
A node MUST silently discard any received Router Advertisement messages that do not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers.
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- **ICMP Code is 0.**
- ICMP length (derived from the IP length) is 16 or more octets.
- All included options have a length that is greater than zero.

RQ_000_8249 Process Field Anomalies in RA
RFC2461 6.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently discard a received Router Advertisement message in which the length of the ICMPv6 packet is less than 16 octets
Specification Text:
A node MUST silently discard any received Router Advertisement messages that do not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers.
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- **ICMP length (derived from the IP length) is 16 or more octets.**
- All included options have a length that is greater than zero.

RQ_000_8250 Process Option Anomalies in RA
RFC2461 6.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Router Advertisement message in which the length of any included option is zero (0)
Specification Text:
A node MUST silently discard any received Router Advertisement messages that do not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers.
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 16 or more octets.
- **All included options have a length that is greater than zero.**

RQ_000_8251 Process Option Anomalies in RA
RFC2461 6.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST ignore the contents of an unrecognized option contained in a received Router Advertisement message.
Specification Text:
The contents of the Reserved field, and **of any unrecognized options, MUST be ignored**. Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values.

RQ_000_8252 Process Option Anomalies in RA
RFC2461 6.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ignore any option contained in a received Router Advertisement message but which is not valid in a Router Advertisement.
Specification Text:
The contents of any defined options that are not specified to be used with Router Advertisement messages MUST be ignored and the packet processed as normal. The only defined options that may appear are the Source Link-Layer Address, Prefix Information and MTU options.

RQ_000_8253 Form Router Advertisement Options
RFC2461 6.1.2 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Router Advertisement message, an IPv6 router MUST NOT include any options other than Source Link-Layer Address, Prefix Information or MTU in the advertisement.
Specification Text:
The contents of any defined options that are not specified to be used with Router Advertisement messages MUST be ignored and the packet processed as normal. **The only defined options that may appear are the Source Link-Layer Address, Prefix Information and MTU options**.

RQ_000_8255 Startup Router Advertisement Behavior
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST make it possible for the sending of Router advertisements to be enabled and disabled by system management procedures.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
For each multicast interface:

AdvSendAdvertisements
A flag indicating whether or not the router sends periodic Router Advertisements and responds to Router Solicitations.

Default: FALSE

Note that AdvSendAdvertisements MUST be FALSE by default so that a node will not accidentally start acting as a router unless it is explicitly configured by system management to send Router Advertisements.

RQ_000_8256 Startup Router Advertisement Behavior
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST NOT enable the sending of Router Advertisement messages unless explicitly configured to do so by system management procedures.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……

For each multicast interface:

AdvSendAdvertisements
A flag indicating whether or not the router sends periodic Router Advertisements and responds to Router Solicitations.

Default: FALSE

Note that AdvSendAdvertisements MUST be FALSE by default so that a node will not accidentally start acting as a router unless it is explicitly configured by system management to send Router Advertisements.

RQ_000_8258 MaxRtrAdvInterval
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST make it possible for the maximum permitted interval between sending unsolicited multicast Router Advertisement messages from an interface to be set by system management procedures to integer values between 4 seconds and 1800 seconds.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
For each multicast interface:

MaxRtrAdvInterval
The maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be no less than 4 seconds and no greater than 1800 seconds.

Default: 600 seconds

RQ_000_8259 MaxRtrAdvInterval
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST set the maximum permitted interval between sending unsolicited multicast Router Advertisement messages from an interface to 600 seconds unless set to a different legitimate value by systems management procedures.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
For each multicast interface:

MaxRtrAdvInterval
The maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be no less than 4 seconds and no greater than 1800 seconds.

Default: 600 seconds

RQ_000_8260 MaxRtrAdvInterval
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
Having sent an unsolicited multicast Router advertisement from an interface, an IPv6 router MUST send another Router Advertisement message from the same interface within the maximum permitted interval configured either by default or by systems management procedures.

Specification Text:

A router MUST allow for the following conceptual variables to be configured by system management.

……

For each multicast interface:

MaxRtrAdvInterval
The maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be no less than 4 seconds and no greater than 1800 seconds.

Default: 600 seconds

RQ_000_8261 MinRtrAdvInterval

RFC2461 6.2.1 MANDATORY

Applies to: Router

Context:

Requirement:

An IPv6 router MUST make it possible for the minimum permitted interval between sending unsolicited multicast Router Advertisement messages from an interface to be set by system management procedures to integer values between 3 seconds and 0.75 times the configured maximum time permitted for sending the same message.

Specification Text:

A router MUST allow for the following conceptual variables to be configured by system management.

……

For each multicast interface:

MinRtrAdvInterval
The minimum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be no less than 3 seconds and no greater than .75 * MaxRtrAdvInterval.

Default: 0.33 * MaxRtrAdvInterval

RQ_000_8262 MinRtrAdvInterval

RFC2461 6.2.1 MANDATORY

Applies to: Router

Context:

Requirement:

An IPv6 router MUST set the minimum permitted interval between sending unsolicited multicast Router Advertisement messages from an interface to one third (0.33) of the configured maximum permitted interval unless set to a different legitimate value by systems management procedures.

Specification Text:

A router MUST allow for the following conceptual variables to be configured by system management.

……

For each multicast interface:

MinRtrAdvInterval
The minimum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be no less than 3 seconds and no greater than .75 * MaxRtrAdvInterval.

Default: 0.33 * MaxRtrAdvInterval

RQ_000_8263 MinRtrAdvInterval

RFC2461 6.2.1 MANDATORY

Applies to: Router

Context:

Requirement:

Having sent an unsolicited multicast Router advertisement from an interface, an IPv6 router MUST NOT send another Router Advertisement message from the same interface within the minimum permitted interval configured either by default or by systems management procedures.

Specification Text:

A router MUST allow for the following conceptual variables to be configured by system management.

……

For each multicast interface:

MinRtrAdvInterval
The minimum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be no less than 3 seconds and no greater than .75 * MaxRtrAdvInterval.

Default: 0.33 * MaxRtrAdvInterval

RQ_000_8264 AdvManagedFlag

RFC2461 6.2.1 MANDATORY

Applies to: Router

Context:

Requirement:

An IPv6 router MUST make it possible for the value (1 or 0) of the M-Flag in outgoing Router Advertisement messages to be established by systems management procedures for each multicast interface.

Specification Text:

A router MUST allow for the following conceptual variables to be configured by system management.

……

For each multicast interface:

AdvManagedFlag
The TRUE/FALSE value to be placed in the "Managed address configuration" flag field in the Router Advertisement. See RFC 2462.

Default: FALSE

RQ_000_8265 AdvManagedFlag

RFC2461 6.2.1 MANDATORY

Applies to: Router

Context:

Requirement:

An IPv6 router MUST set the value of the M-Flag to 0 (FALSE) in each Router Advertisement message sent from an interface unless configured by system management procedures to be a different value (TRUE).

Specification Text:

A router MUST allow for the following conceptual variables to be configured by system management.

……

For each multicast interface:

AdvManagedFlag
The TRUE/FALSE value to be placed in the "Managed address configuration" flag field in the Router Advertisement. See RFC 2462.

Default: FALSE

RQ_000_8267 AdvOtherConfigFlag

RFC2461 6.2.1 MANDATORY

Applies to: Router

Context:

Requirement:

An IPv6 router MUST make it possible for the value (1 or 0) of the O-Flag in outgoing Router Advertisement messages to be established by systems management procedures for each multicast interface.

Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
For each multicast interface:

AdvOtherConfigFlag
The TRUE/FALSE value to be placed in the "Other stateful configuration" flag field in the Router Advertisement. See RFC 2462.

Default: FALSE

RQ_000_8268 AdvOtherConfigFlag
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST set the value of the O-Flag to 0 (FALSE) in each Router Advertisement message sent from an interface unless configured by system management procedures to be a different value (TRUE).
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
For each multicast interface:

AdvOtherConfigFlag
The TRUE/FALSE value to be placed in the "Other stateful configuration" flag field in the Router Advertisement. See RFC 2462.

Default: FALSE

RQ_000_8270 RA MTU Option
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST make it possible for the value of the MTU options in outgoing Router Advertisement messages to be established by systems management procedures for each multicast interface.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
For each multicast interface:

AdvLinkMTU **The value to be placed in MTU options sent by the router**. A value of zero indicates that no MTU options are sent.

Default: 0

RQ_000_8271 RA MTU Option
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Router Advertisement message an IPv6 router MUST NOT include MTU options in the message if the value established for MTU options by system management procedures or by default is zero (0)
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……

For each multicast interface:

AdvLinkMTU The value to be placed in MTU options sent by the router. A value of zero indicates that no MTU options are sent.

Default: 0

RQ_000_8272 RA MTU Option
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Router Advertisement message an IPv6 node MUST set the MTU options to the value established by system management procedures if this value is not zero (0).
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
For each multicast interface:

AdvLinkMTU The value to be placed in MTU options sent by the router. A value of zero indicates that no MTU options are sent.

Default: 0

RQ_000_8273 AdvReachableTime
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST make it possible for the value of the Reachable Time field in outgoing Router Advertisement messages to be established by systems management procedures at between "unspecified" (0) and 3,600,000 milliseconds for each multicast interface.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
AdvReachableTime
The value to be placed in the Reachable Time field in the Router Advertisement messages sent by the router. The value zero means unspecified (by this router). MUST be no greater than 3,600,000 milliseconds (1 hour).

Default: 0

RQ_000_8274 AdvReachableTime
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST set the value of the Reachable Time field to unspecified (0) in each Router Advertisement message sent from an interface unless configured by system management procedures to be a different value.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……

AdvReachableTime
The value to be placed in the Reachable Time field in the Router Advertisement messages sent by the router. The value zero means unspecified (by this router). MUST be no greater than 3,600,000 milliseconds (1 hour).

Default: 0

RQ_000_8276 AdvRetransTimer
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST make it possible for the value of the Retrans Timer field in outgoing Router Advertisement messages to be established by systems management procedures at between "unspecified" (0) and 4,294,967,295 milliseconds (32 bits unsigned) for each multicast interface.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
AdvRetransTimer
The value to be placed in the Retrans Timer field in the Router Advertisement messages sent by the router. The value zero means unspecified (by this router).

Default: 0

RQ_000_8277 AdvRetransTimer
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST set the value of the Retrans Timer field to unspecified (0) in each Router Advertisement message sent from an interface unless configured by system management procedures to be a different value.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
AdvRetransTimer
The value to be placed in the Retrans Timer field in the Router Advertisement messages sent by the router. The value zero means unspecified (by this router).

Default: 0

RQ_000_8279 AdvCurHopLimit
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST make it possible for the value of the Cur Hop Limit field in outgoing Router Advertisement messages to be established by systems management procedures at between "unspecified" (0) and 255 for each multicast interface.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……

AdvCurHopLimit
The default value to be placed in the Cur Hop Limit field in the Router Advertisement messages sent by the router. The value should be set to that current diameter of the Internet. **The value zero means unspecified (by this router).**

Default: The value specified in the "Assigned Numbers" RFC 1700 that was in effect at the time of implementation.

RQ_000_8282 AdvCurHopLimit
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST set the value of the Cur Hop Limit field in each Router Advertisement message sent from an interface to the value specified in RFC 1700 at the time of implementation unless configured by system management procedures to be a different value.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
AdvCurHopLimit
The default value to be placed in the Cur Hop Limit field in the Router Advertisement messages sent by the router. The value should be set to that current diameter of the Internet. The value zero means unspecified (by this router).

Default: The value specified in the "Assigned Numbers" RFC 1700 that was in effect at the time of implementation.

RQ_000_8283 AdvDefaultLifetime
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST make it possible for the value of the Router Lifetime field in outgoing Router Advertisement messages to be established by systems management procedures at zero (not a default router) or between the value configured as the Maximum Router Advertisement Interval and 9000 seconds for each multicast interface.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
AdvDefaultLifetime
The value to be placed in the Router Lifetime field of Router Advertisements sent from the interface, in seconds. MUST be either zero or between MaxRtrAdvInterval and 9000 seconds. A value of zero indicates that the router is not to be used as a default router.

Default: 3 * MaxRtrAdvInterval

RQ_000_8284 AdvDefaultLifetime
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST set the value of the Router Lifetime field to a value of 3 times the configured Maximum Router Advertisement Interval in each Router Advertisement message sent from an interface unless configured by system management procedures to be a valid different value.

Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
AdvDefaultLifetime
The value to be placed in the Router Lifetime field of Router Advertisements sent from the interface, in seconds. MUST be either zero or between MaxRtrAdvInterval and 9000 seconds. A value of zero indicates that the router is not to be used as a default router.

Default: 3 * MaxRtrAdvInterval

RQ_000_8287 AdvDefaultLifetime
RFC2461 6.2.1 RECOMMENDED
Applies to: Host
Context:
An IPv6 host receives a Router Advertisement message with the Router Lifetime field set to 0 in the ICMPv6 packet.
Requirement:
The IPv6 host SHOULD NOT use the advertising router as one of its default routers.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
AdvDefaultLifetime
The value to be placed in the Router Lifetime field of Router Advertisements sent from the interface, in seconds. MUST be either zero or between MaxRtrAdvInterval and 9000 seconds. **A value of zero indicates that the router is not to be used as a default router.**

Default: 3 * MaxRtrAdvInterval

RQ_000_8288 RA Prefix Option
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:
The implementation is being configured for operation.
Requirement:
An IPv6 router MUST make it possible for the contents of the Prefix Information option in outgoing Router Advertisement messages to be established by systems management procedures as follows:

Prefix Information	Value Range
Valid Lifetime	0 to FFFFFFFFhex seconds
On-Link flag (L-Flag)	TRUE or FALSE
Preferred Lifetime	0 to FFFFFFFFhex seconds
Autonomous Flag (A-Flag)	TRUE or FALSE
Prefix	IPv6 Address or IPv6 Address prefix

System management provides for each implementation's multicast interface a list of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from the interface. For each prefix in the list, system management can configure the value in seconds to be placed in the Valid Lifetime field and the value to be placed in the on-link flag ("L-bit") field in the Prefix Information option. For Address Autoconfiguration of each prefix in the list, system management can configure the value in seconds to be placed in the Preferred Lifetime and the value to be placed in the Autonomous Flag field in the Prefix Information option.
Specification Text:
A router MUST allow for the following conceptual variables to be configured by system management.
……
AdvPrefixList
A list of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from the interface.

Default: all prefixes that the router advertises via routing
protocols as being on-link for the interface from
which the advertisement is sent. The link-local
prefix SHOULD NOT be included in the list of
advertised prefixes.

Each prefix has an associated:

AdvValidLifetime

The value to be placed in the Valid Lifetime in the Prefix Information option, in seconds. The designated value of all 1's (0xffffffff) represents infinity. Implementations MUST allow AdvValidLifetime to be specified in two ways:
- a time that decrements in real time, that is, one that will result in a Lifetime of zero at the specified time in the future, or
- a fixed time that stays the same in consecutive advertisements.

Default: 2592000 seconds (30 days), fixed (i.e., stays the same in consecutive advertisements).

AdvOnLinkFlag

The value to be placed in the on-link flag ("L-bit") field in the Prefix Information option.
Default: TRUE

Automatic address configuration [RFC 2462] defines additional information associated with each the prefixes:

AdvPreferredLifetime

The value to be placed in the Preferred Lifetime in the Prefix Information option, in seconds. The designated value of all 1's (0xffffffff) represents infinity. See RFC 2462 for details on how this value is used. Implementations MUST allow AdvPreferredLifetime to be specified in two ways:
- a time that decrements in real time, that is, one that will result in a Lifetime of zero at a specified time in the future, or
- a fixed time that stays the same in consecutive advertisements.

Default: 604800 seconds (7 days), fixed (i.e., stays the same in consecutive advertisements).

AdvAutonomousFlag

The value to be placed in the Autonomous Flag field in the Prefix Information option. See RFC 2462.
Default: TRUE

RQ_000_8289 RA Prefix Option

RFC2461 6.2.1 MANDATORY

Applies to: Router

Context:

Requirement:

An IPv6 router MUST set the contents of the Prefix Information option in each Router Advertisement message sent from an interface as follows unless configured by system management procedures to be different valid values.

Prefix Information	Default Value
Valid Lifetime	2,592,000 seconds (30 days)
On-Link flag (L-Flag)	TRUE
Preferred Lifetime	604,800 seconds (7 days) seconds
Autonomous Flag (A-Flag)	TRUE
Prefix	all prefixes that the router advertises via routing protocols as being on-link for the interface from which the advertisement is sent.

Specification Text:

A router MUST allow for the following conceptual variables to be configured by system management.

……

AdvPrefixList

A list of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from the interface.

Default: all prefixes that the router advertises via routing protocols as being on-link for the interface from which the advertisement is sent. The link-local prefix SHOULD NOT be included in the list of advertised prefixes.

Each prefix has an associated:

AdvValidLifetime

The value to be placed in the Valid Lifetime in the Prefix Information option, in seconds. The designated value of all 1's (0xffffffff) represents infinity. Implementations MUST allow AdvValidLifetime to be specified in two ways:

- a time that decrements in real time, that is, one that will result in a Lifetime of zero at the specified time in the future, or
- a fixed time that stays the same in consecutive advertisements.

Default: 2592000 seconds (30 days), fixed (i.e., stays the same in consecutive advertisements).

AdvOnLinkFlag

The value to be placed in the on-link flag ("L-bit") field in the Prefix Information option.
Default: TRUE

Automatic address configuration [RFC 2462] defines additional information associated with each the prefixes:

AdvPreferredLifetime

The value to be placed in the Preferred Lifetime in the Prefix Information option, in seconds. The designated value of all 1's (0xffffffff) represents infinity. See RFC 2462 for details on how this value is used. Implementations MUST allow AdvPreferredLifetime to be specified in two ways:

- a time that decrements in real time, that is, one that will result in a Lifetime of zero at a specified time in the future, or
- a fixed time that stays the same in consecutive advertisements.

Default: 604800 seconds (7 days), fixed (i.e., stays the same in consecutive advertisements).

AdvAutonomousFlag

The value to be placed in the Autonomous Flag field in the Prefix Information option. See RFC 2462.
Default: TRUE

RQ_000_8290 RA Prefix Option

RFC2461 6.2.1 RECOMMENDED

Applies to: Router

Context:

Requirement:

An IPv6 router SHOULD NOT send a Router Advertisement containing a Prefix Information option for the link-local prefix (FF02:x).

Specification Text:

A router MUST allow for the following conceptual variables to be configured by system management.

……

AdvPrefixList

A list of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from the interface.

Default: all prefixes that the router advertises via routing protocols as being on-link for the interface from which the advertisement is sent. **The link-local prefix SHOULD NOT be included in the list of advertised prefixes.**

```
      Each prefix has an associated:
         AdvValidLifetime
                 The value to be placed in the Valid Lifetime in
                 the Prefix Information option, in seconds.  The
                 designated value of all 1's (0xffffffff) represents
                 infinity.  Implementations MUST allow
                 AdvValidLifetime to be specified in two ways:
                 - a time that decrements in real time, that is, one
                   that will result in a Lifetime of zero at the
                   specified time in the future, or
                - a fixed time that stays the same in consecutive
                  advertisements.
                Default: 2592000 seconds (30 days), fixed (i.e., stays
                         the same in consecutive advertisements).
         AdvOnLinkFlag
                The value to be placed in the on-link flag ("L-bit")
                field in the Prefix Information option.
                Default: TRUE

Automatic address configuration [RFC 2462] defines additional information associated with each
the prefixes:

         AdvPreferredLifetime
                The value to be placed in the Preferred Lifetime in
                the Prefix Information option, in seconds.  The
                designated value of all 1's (0xffffffff) represents
                infinity.  See RFC 2462 for details on how this value
                is used.  Implementations MUST allow AdvPreferredLifetime
                to be specified in two ways:
                - a time that decrements in real time, that is, one that
                  will result in a Lifetime of zero at a specified time
                  in the future, or
                - a fixed time that stays the same in consecutive
                  advertisements.
             Default: 604800 seconds (7 days), fixed (i.e., stays the
                      same in consecutive advertisements).
         AdvAutonomousFlag
                The value to be placed in the Autonomous Flag field in
                the Prefix Information option.  See RFC 2462.
                Default: TRUE
```

RQ_000_8291 RA Prefix Option

RFC2461 6.2.1 MANDATORY

Applies to: Router

Context:

Requirement:

```
An IPv6 router MUST allow the Prefix Preferred Lifetime established by system management
procedures or by default for inclusion in the Prefix options of outgoing Router Advertisement
messages to decrease in real time from the point of establishment to zero such that each
successive Router Advertisement message contains a lower value of this parameter than previous
RA messages.
```

Specification Text:

```
A router MUST allow for the following conceptual variables to be configured by system
management.
……
 AdvPrefixList
      A list of prefixes to be placed in Prefix Information
      options in Router Advertisement messages sent from the
      interface.
      Default: all prefixes that the router advertises via routing
               protocols as being on-link for the interface from
               which the advertisement is sent.  The link-local
               prefix SHOULD NOT be included in the list of
               advertised prefixes.
      Each prefix has an associated:
         AdvValidLifetime
                 The value to be placed in the Valid Lifetime in
                 the Prefix Information option, in seconds.  The
                 designated value of all 1's (0xffffffff) represents
                 infinity.  Implementations MUST allow
                 AdvValidLifetime to be specified in two ways:
                 - a time that decrements in real time, that is, one
                   that will result in a Lifetime of zero at the
                   specified time in the future, or
```

```
              - a fixed time that stays the same in consecutive
                advertisements.
              Default: 2592000 seconds (30 days), fixed (i.e., stays
                       the same in consecutive advertisements).
         AdvOnLinkFlag
              The value to be placed in the on-link flag ("L-bit")
              field in the Prefix Information option.
              Default: TRUE

Automatic address configuration [RFC 2462] defines additional information associated with each
the prefixes:

         AdvPreferredLifetime
              The value to be placed in the Preferred Lifetime in
              the Prefix Information option, in seconds.  The
              designated value of all 1's (0xffffffff) represents
              infinity.  See RFC 2462 for details on how this value
              is used.  Implementations MUST allow AdvPreferredLifetime
              to be specified in two ways:
              - a time that decrements in real time, that is, one that
                will result in a Lifetime of zero at a specified time
                in the future, or
              - a fixed time that stays the same in consecutive
                advertisements.
            Default: 604800 seconds (7 days), fixed (i.e., stays the
                     same in consecutive advertisements).
         AdvAutonomousFlag
              The value to be placed in the Autonomous Flag field in
              the Prefix Information option.  See RFC 2462.
              Default: TRUE
```

RQ_000_8292 RA Prefix Option

RFC2461 6.2.1 MANDATORY

Applies to: Router

Context:

Requirement:

```
An IPv6 router MUST allow the Prefix Preferred Lifetime established by system management
procedures or by default for inclusion in the Prefix options of outgoing Router Advertisement
messages to be a fixed value that stays the same in consecutive Router advertisement messages.
```

Specification Text:

```
A router MUST allow for the following conceptual variables to be configured by system
management.
……
 AdvPrefixList
      A list of prefixes to be placed in Prefix Information
      options in Router Advertisement messages sent from the
      interface.
      Default: all prefixes that the router advertises via routing
               protocols as being on-link for the interface from
               which the advertisement is sent.  The link-local
               prefix SHOULD NOT be included in the list of
               advertised prefixes.
      Each prefix has an associated:
         AdvValidLifetime
                The value to be placed in the Valid Lifetime in
                the Prefix Information option, in seconds.  The
                designated value of all 1's (0xffffffff) represents
                infinity.  Implementations MUST allow
                AdvValidLifetime to be specified in two ways:
                - a time that decrements in real time, that is, one
                  that will result in a Lifetime of zero at the
                  specified time in the future, or
              - a fixed time that stays the same in consecutive
                advertisements.
              Default: 2592000 seconds (30 days), fixed (i.e., stays
                       the same in consecutive advertisements).
         AdvOnLinkFlag
              The value to be placed in the on-link flag ("L-bit")
              field in the Prefix Information option.
              Default: TRUE
```

Automatic address configuration [RFC 2462] defines additional information associated with each the prefixes:

AdvPreferredLifetime
The value to be placed in the Preferred Lifetime in the Prefix Information option, in seconds. The designated value of all 1's (0xffffffff) represents infinity. See RFC 2462 for details on how this value is used. **Implementations MUST allow AdvPreferredLifetime to be specified in two ways:**
- a time that decrements in real time, that is, one that will result in a Lifetime of zero at a specified time in the future, or
- **a fixed time that stays the same in consecutive advertisements.**

Default: 604800 seconds (7 days), fixed (i.e., stays the same in consecutive advertisements).

AdvAutonomousFlag
The value to be placed in the Autonomous Flag field in the Prefix Information option. See RFC 2462.
Default: TRUE

RQ_000_8293 Router Advertisement Behavior
RFC2461 6.2.1 MANDATORY
Applies to: Router
Context:

Requirement:
Although an IPv6 router is not required to modify its configured values of Current Hop Limit, Reachability Time and Retransmission timer on the basis of a received Router Advertisement message, it MUST comply with the requirement specified in RFC2461 for IPv6 hosts in respect to the use of these parameters.
Specification Text:
The above variables contain information that is placed in outgoing Router Advertisement messages. Hosts use the received information to initialize a set of analogous variables that control their external behavior (see Section 6.3.2{of RFC 2461}). Some of these host variables (e.g., CurHopLimit, RetransTimer, and ReachableTime) apply to all nodes including routers. In practice, these variables may not actually be present on routers, since their contents can be derived from the variables described above. However, external router behavior MUST be the same as host behavior with respect to these variables. In particular, this includes the occasional randomization of the ReachableTime value as described in Section 6.3.2 {of RFC 2461}.

RQ_000_8294 Generate Router Advertisement
RFC2461 6.2.2 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST NOT send Router advertisement messages on any interface that has not been configured by system management procedures to be able to send Router advertisements.
Specification Text:
The term "advertising interface" refers to any functioning and enabled multicast interface that has at least one unicast IP address assigned to it and whose corresponding AdvSendAdvertisements flag is TRUE. A router MUST NOT send Router Advertisements out any interface that is not an advertising interface.

RQ_000_8295 Generate Router Advertisement
RFC2461 6.2.2 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST NOT send Router advertisement messages on any interface that does not have at least one unicast address assigned to it.
Specification Text:
The term "advertising interface" refers to any functioning and enabled multicast interface that has at least one unicast IP address assigned to it and whose corresponding AdvSendAdvertisements flag is TRUE. A router MUST NOT send Router Advertisements out any interface that is not an advertising interface.

RQ_000_8299 Router Advertisement Behavior on Reconfiguration
RFC2461 6.2.2 MANDATORY
Applies to: Router
Context:
An IPv6 router receives a valid Router Solicitation on an advertising interface with the link-local all-routers multicast address (FF02:0:0:0:0:0:0:2) set in Destination Address field of the containing IPv6 packet.
Requirement:
The IPv6 router MUST send a Router advertisement as a response to the Router Solicitation.
Specification Text:
A router MUST join the all-routers multicast address on an advertising interface. Routers respond to Router Solicitations sent to the all-routers address and verify the consistency of Router Advertisements sent by neighboring routers.

RQ_000_8301 RA Source Link-Layer Address Option
RFC2461 6.2.3 OPTIONAL
Applies to: Router
Context:

Requirement:
An IPv6 router MAY omit the Source link-layer address option in a Router Advertisement message.
Specification Text:
Router Advertisement Message Content

A router sends periodic as well as solicited Router Advertisements out its advertising interfaces. Outgoing Router Advertisements are filled with the following values consistent with the message format given in Section 4.2:

- In the Router Lifetime field: the interface's configured AdvDefaultLifetime.
- In the M and O flags: the interface's configured AdvManagedFlag and AdvOtherConfigFlag, respectively. See [ADDRCONF].
- In the Cur Hop Limit field: the interface's configured CurHopLimit.
- In the Reachable Time field: the interface's configured AdvReachableTime.
- In the Retrans Timer field: the interface's configured AdvRetransTimer.
- **In the options:**
  - **Source Link-Layer Address option: link-layer address of the sending interface. This option MAY be omitted to facilitate in-bound load balancing over replicated interfaces.**
  - MTU option: the interface's configured AdvLinkMTU value if the value is non-zero. If AdvLinkMTU is zero the MTU option is not sent.
  - Prefix Information options: one Prefix Information option for each prefix listed in AdvPrefixList with the option fields set from the information in the AdvPrefixList entry as follows:
    - In the "on-link" flag: the entry's AdvOnLinkFlag.
    - In the Valid Lifetime field: the entry's AdvValidLifetime.
    - In the "Autonomous address configuration" flag: the entry's AdvAutonomousFlag.
    - In the Preferred Lifetime field: the entry's AdvPreferredLifetime

RQ_000_8302 RA Prefix Option
RFC2461 6.2.3 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Router Advertisement message to be sent from a particular interface, an IPv6 router MUST include one Prefix Information option for each prefix established for that interface by default or by system management procedures.

Specification Text:

Router Advertisement Message Content

A router sends periodic as well as solicited Router Advertisements out its advertising interfaces. Outgoing Router Advertisements are filled with the following values consistent with the message format given in Section 4.2:

- In the Router Lifetime field: the interface's configured AdvDefaultLifetime.
- In the M and O flags: the interface's configured AdvManagedFlag and AdvOtherConfigFlag, respectively. See [ADDRCONF].
- In the Cur Hop Limit field: the interface's configured CurHopLimit.
- In the Reachable Time field: the interface's configured AdvReachableTime.
- In the Retrans Timer field: the interface's configured AdvRetransTimer.
- **In the options:**
  - o Source Link-Layer Address option: link-layer address of the sending interface. This option MAY be omitted to facilitate in-bound load balancing over replicated interfaces.
  - o MTU option: the interface's configured AdvLinkMTU value if the value is non-zero. If AdvLinkMTU is zero the MTU option is not sent.
  - **o Prefix Information options: one Prefix Information option for each prefix listed in AdvPrefixList** with the option fields set from the information in the AdvPrefixList entry as follows:
    - In the "on-link" flag: the entry's AdvOnLinkFlag.
    - In the Valid Lifetime field: the entry's AdvValidLifetime.
    - In the "Autonomous address configuration" flag: the entry's AdvAutonomousFlag.
    - In the Preferred Lifetime field: the entry's AdvPreferredLifetime

RQ_000_8303 Startup Router Advertisement Behavior

RFC2461 6.2.3 MANDATORY

Applies to: Router

Context:

Requirement:

When constructing a Router advertisement message, an IPv6 router MUST set the Router Lifetime field to zero (0) if the router is not to be considered as a default router by receiving nodes.

Specification Text:

A router might want to send Router Advertisements without advertising itself as a default router. For instance, a router might advertise prefixes for address autoconfiguration while not wishing to forward packets. **Such a router sets the Router Lifetime field in outgoing advertisements to zero.**

RQ_000_8304 Form Router Advertisement Options

RFC2461 6.2.3 OPTIONAL

Applies to: Router

Context:

Requirement:

When constructing a Router advertisement which is to be sent as an unsolicited advertisement, an IPv6 router MAY include in the message all, some or none of the options specified for Router advertisements.

Specification Text:

A router MAY choose not to include some or all options when sending unsolicited Router Advertisements. For example, if prefix lifetimes are much longer than AdvDefaultLifetime, including them every few advertisements may be sufficient. However, when responding to a Router Solicitation or while sending the first few initial unsolicited advertisements, a router SHOULD include all options so that all information (e.g., prefixes) is propagated quickly during system initialization.

RQ_000_8305 Form Router Advertisement Options
RFC2461 6.2.3 RECOMMENDED
Applies to: Router
Context:

Requirement:
When constructing a Router advertisement which is to be one of the first few unsolicited advertisements sent after system initialization, an IPv6 node SHOULD include in the message all of the options specified for Router advertisements.
Specification Text:
A router MAY choose not to include some or all options when sending unsolicited Router Advertisements. For example, if prefix lifetimes are much longer than AdvDefaultLifetime, including them every few advertisements may be sufficient. However, when responding to a Router Solicitation or **while sending the first few initial unsolicited advertisements, a router SHOULD include all options so that all information (e.g., prefixes) is propagated quickly during system initialization**.

RQ_000_8306 Form Router Advertisement Options
RFC2461 6.2.3 RECOMMENDED
Applies to: Router
Context:

Requirement:
When constructing a Router advertisement to be sent in response to a received Router Solicitation message, an IPv6 router SHOULD include in the advertisement all options specified for Router advertisements.
Specification Text:
A router MAY choose not to include some or all options when sending unsolicited Router Advertisements. For example, if prefix lifetimes are much longer than AdvDefaultLifetime, including them every few advertisements may be sufficient. However, **when responding to a Router Solicitation** or while sending the first few initial unsolicited advertisements, **a router SHOULD include all options so that all information (e.g., prefixes) is propagated quickly during system initialization**.

RQ_000_8307 Form Router Advertisement Options
RFC2461 6.2.3 OPTIONAL
Applies to: Router
Context:

Requirement:
An IPv6 router MAY send multiple Router advertisements, each containing a subset of the required options, if the size of a single advertisement containing all of the options would exceed the link MTU.
Specification Text:
A router MAY choose not to include some or all options when sending unsolicited Router Advertisements. For example, if prefix lifetimes are much longer than AdvDefaultLifetime, including them every few advertisements may be sufficient. However, when responding to a Router Solicitation or while sending the first few initial unsolicited advertisements, a router SHOULD include all options so that all information (e.g., prefixes) is propagated quickly during system initialization.

If including all options causes the size of an advertisement to exceed the link MTU, multiple advertisements can be sent, each containing a subset of the options.

RQ_000_8308 Generate Router Advertisement
RFC2461 6.2.4 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST NOT send Router advertisement messages at any time.
Specification Text:
A host MUST NOT send Router Advertisement messages at any time.

RQ_000_8309 Router Advertisement Behavior
RFC2461 6.2.4 MANDATORY
Applies to: Router
Context:
An IPv6 router has sent 3 unsolicited multicast Router Advertisements from a particular interface since system initialization.
Requirement:
The IPv6 router MUST ensure that the intervals between successive unsolicited multicast Router Advertisement messages sent from the interface are uniformly-distributed random time values between the Minimum Router Advertisement Interval and the Maximum Router Advertisement Interval configured by default or by system management procedures.
Specification Text:
Unsolicited Router Advertisements are not strictly periodic: the interval between subsequent transmissions is randomized to reduce the probability of synchronization with the advertisements from other routers on the same link. Each advertising interface has its own timer. **Whenever a multicast advertisement is sent from an interface, the timer is reset to a uniformly-distributed random value between the interface's configured MinRtrAdvInterval and MaxRtrAdvInterval; expiration of the timer causes the next advertisement to be sent and a new random value to be chosen**.

For the first few advertisements (up to MAX_INITIAL_RTR_ADVERTISEMENTS) sent from an interface when it becomes an advertising interface, if the randomly chosen interval is greater than MAX_INITIAL_RTR_ADVERT_INTERVAL, the timer SHOULD be set to MAX_INITIAL_RTR_ADVERT_INTERVAL instead. Using a smaller interval for the initial advertisements increases the likelihood of a router being discovered quickly when it first becomes available, in the presence of possible packet loss.

RQ_000_8310 Startup Router Advertisement Behavior
RFC2461 6.2.4 RECOMMENDED
Applies to: Router
Context:

Requirement:
An IPv6 router SHOULD ensure that the interval between each of the first 3 unsolicited Router advertisements sent from a particular interface after the router becomes an advertising router does not exceed 16 seconds.
Specification Text:
Unsolicited Router Advertisements are not strictly periodic: the interval between subsequent transmissions is randomized to reduce the probability of synchronization with the advertisements from other routers on the same link. Each advertising interface has its own timer. Whenever a multicast advertisement is sent from an interface, the timer is reset to a uniformly-distributed random value between the interface's configured MinRtrAdvInterval and MaxRtrAdvInterval; expiration of the timer causes the next advertisement to be sent and a new random value to be chosen.

For the first few advertisements (up to MAX_INITIAL_RTR_ADVERTISEMENTS) sent from an interface when it becomes an advertising interface, if the randomly chosen interval is greater than MAX_INITIAL_RTR_ADVERT_INTERVAL, the timer SHOULD be set to MAX_INITIAL_RTR_ADVERT_INTERVAL instead. Using a smaller interval for the initial advertisements increases the likelihood of a router being discovered quickly when it first becomes available, in the presence of possible packet loss.

RQ_000_8312 Router Advertisement Behavior on Reconfiguration
RFC2461 6.2.5 RECOMMENDED
Applies to: Router
Context:
An interface on an IPv6 router is configured to cease being an advertising interface.
Requirement:
The IPv6 router SHOULD send at least one but not more than 3 multicast Router Advertisement messages in which the Router Lifetime field is set to zero (0)
Specification Text:
An interface may cease to be an advertising interface, through actions of system management such as:

- **changing the AdvSendAdvertisements flag of an enabled interface from TRUE to FALSE, or**
- **administratively disabling the interface, or**
- **shutting down the system.**

In such cases the router SHOULD transmit one or more (but not more than MAX_FINAL_RTR_ADVERTISEMENTS) final multicast Router Advertisements on the interface with a Router Lifetime field of zero. In the case of a router becoming a host, the system SHOULD also depart from the all-routers IP multicast group on all interfaces on which the router supports IP multicast (whether or not they had been advertising interfaces). In addition, the host MUST insure that subsequent Neighbor Advertisement messages sent from the interface have the Router flag set to zero.

Note that system management may disable a router's IP forwarding capability (i.e., changing the system from being a router to being a host), a step that does not necessarily imply that the router's interfaces stop being advertising interfaces. In such cases, subsequent Router Advertisements MUST set the Router Lifetime field to zero.

RQ_000_8313 Configure Address
RFC2461 6.2.5 RECOMMENDED
Applies to: Router
Context:

Requirement:
When reconfigured to cease operation as a router and to become a host, an IPv6 node SHOULD NOT respond to subsequent received IPv6 packets in which the Destination Address field is set to the link-local all-routers multicast address (FF02:0:0:0:0:0:0:2).
Specification Text:
An interface may cease to be an advertising interface, through actions of system management such as:

- changing the AdvSendAdvertisements flag of an enabled interface from TRUE to FALSE, or
- administratively disabling the interface, or
- shutting down the system.

In such cases the router SHOULD transmit one or more (but not more than MAX_FINAL_RTR_ADVERTISEMENTS) final multicast Router Advertisements on the interface with a Router Lifetime field of zero. **In the case of a router becoming a host, the system SHOULD also depart from the all-routers IP multicast group on all interfaces on which the router supports IP multicast (whether or not they had been advertising interfaces)**. In addition, the host MUST insure that subsequent Neighbor Advertisement messages sent from the interface have the Router flag set to zero.

Note that system management may disable a router's IP forwarding capability (i.e., changing the system from being a router to being a host), a step that does not necessarily imply that the router's interfaces stop being advertising interfaces. In such cases, subsequent Router Advertisements MUST set the Router Lifetime field to zero.

RQ_000_8314 Generate Unsolicited Neighbor Advertisement
RFC2461 6.2.5 MANDATORY
Applies to: Router
Context:

Requirement:
When reconfigured to cease operation as a router and to become a host, an IPv6 node MUST NOT set the R-Flag to zero (0) in any subsequent Neighbor Advertisement messages that it sends.
Specification Text:
An interface may cease to be an advertising interface, through actions of system management such as:

- changing the AdvSendAdvertisements flag of an enabled interface from TRUE to FALSE, or
- administratively disabling the interface, or
- shutting down the system.

In such cases the router SHOULD transmit one or more (but not more than MAX_FINAL_RTR_ADVERTISEMENTS) final multicast Router Advertisements on the interface with a Router Lifetime field of zero. In the case of a router becoming a host, the system SHOULD also depart from the all-routers IP multicast group on all interfaces on which the router supports IP multicast (whether or not they had been advertising interfaces). **In addition, the host MUST insure that subsequent Neighbor Advertisement messages sent from the interface have the Router flag set to zero.**

Note that system management may disable a router's IP forwarding capability (i.e., changing the system from being a router to being a host), a step that does not necessarily imply that the router's interfaces stop being advertising interfaces. In such cases, subsequent Router Advertisements MUST set the Router Lifetime field to zero.

RQ_000_8315 Router Advertisement Behavior on Reconfiguration
RFC2461 6.2.5 MANDATORY
Applies to: Router
Context:

Requirement:
When an IPv6 router is reconfigured to cease being a router and to become a host but its interfaces remain as advertising interfaces, it MUST set the Router Lifetime field in any subsequent outgoing Router Advertisement messages to zero (0).
Specification Text:
An interface may cease to be an advertising interface, through actions of system management such as:

- changing the AdvSendAdvertisements flag of an enabled interface from TRUE to FALSE, or
- administratively disabling the interface, or
- shutting down the system.

In such cases the router SHOULD transmit one or more (but not more than MAX_FINAL_RTR_ADVERTISEMENTS) final multicast Router Advertisements on the interface with a Router Lifetime field of zero. In the case of a router becoming a host, the system SHOULD also depart from the all-routers IP multicast group on all interfaces on which the router supports IP multicast (whether or not they had been advertising interfaces). In addition, the host MUST insure that subsequent Neighbor Advertisement messages sent from the interface have the Router flag set to zero.

Note that system management may disable a router's IP forwarding capability (i.e., changing the system from being a router to being a host), a step that does not necessarily imply that the router's interfaces stop being advertising interfaces. In such cases, subsequent Router Advertisements MUST set the Router Lifetime field to zero.

RQ_000_8316 Host Processing of RS
RFC2461 6.2.6 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard any received Router Solicitation messages.
Specification Text:
A host MUST silently discard any received Router Solicitation messages.

RQ_000_8317 Router Processing of RS
RFC2461 6.2.6 OPTIONAL
Applies to: Router
Context:
An IPv6 router receives a valid Router Solicitation message in which the Source Address field of the containing IPv6 packet header is not set to the IPv6 Unspecified Address (0:0:0:0:0:0:0:0)
Requirement:
The IPv6 router MAY set the Destination address in the IPv6 packet header containing the Router Advertisement response to the soliciting host's address.
Specification Text:
In addition to sending periodic, unsolicited advertisements, **a router sends advertisements in response to valid solicitations received on an advertising interface. A router MAY choose to unicast the response directly to the soliciting host's address (if the solicitation's source address is not the unspecified address)**, but the usual case is to multicast the response to the all-nodes group. In the latter case, the interface's interval timer is reset to a new random value, as if an unsolicited advertisement had just been sent (see Section 6.2.4).

RQ_000_8318 Router Processing of RS
RFC2461 6.2.6 RECOMMENDED
Applies to: Router
Context:
An IPv6 router receives a valid Router Solicitation message sent to an advertising interface
Requirement:
The IPv6 router SHOULD send a Router advertisement message with the Destination Address in the containing IPv6 packet header set to the link-local all-nodes multicast address (FF02:0:0:0:0:0:0:1).

Specification Text:
In addition to sending periodic, unsolicited advertisements, **a router sends advertisements in response to valid solicitations received on an advertising interface**. A router MAY choose to unicast the response directly to the soliciting host's address (if the solicitation's source address is not the unspecified address), but **the usual case is to multicast the response to the all-nodes group**. In the latter case, the interface's interval timer is reset to a new random value, as if an unsolicited advertisement had just been sent (see Section 6.2.4).

RQ_000_8319 Router Processing of RS
RFC2461 6.2.6 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST delay a random time of between 0 and 0.5 seconds after receiving a valid Router Solicitation message before sending the Router advertisement in response.
Specification Text:
In all cases, Router Advertisements sent in response to a Router Solicitation MUST be delayed by a random time between 0 and MAX_RA_DELAY_TIME seconds. (If a single advertisement is sent in response to multiple solicitations, the delay is relative to the first solicitation.) In addition, consecutive Router Advertisements sent to the all-nodes multicast address MUST be rate limited to no more than one advertisement every MIN_DELAY_BETWEEN_RAS seconds.

RQ_000_8320 Router Processing of RS
RFC2461 6.2.6 MANDATORY
Applies to: Router
Context:

Requirement:
When sending a single Router Advertisement message in response to multiple valid Router solicitations, an IPv6 router MUST wait for between 0 and 0.5 seconds after the receipt of the first solicitation before sending the advertisement.
Specification Text:
In all cases, Router Advertisements sent in response to a Router Solicitation MUST be delayed by a random time between 0 and MAX_RA_DELAY_TIME seconds. (If a single advertisement is sent in response to multiple solicitations, the delay is relative to the first solicitation.) In addition, consecutive Router Advertisements sent to the all-nodes multicast address MUST be rate limited to no more than one advertisement every MIN_DELAY_BETWEEN_RAS seconds.

RQ_000_8321 Router Processing of RS
RFC2461 6.2.6 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST ensure that it waits for at least 3 seconds between sending consecutive Router Advertisements to the link-local all-node multicast address (FF02:0:0:0:0:0:0:1)
Specification Text:
In all cases, Router Advertisements sent in response to a Router Solicitation MUST be delayed by a random time between 0 and MAX_RA_DELAY_TIME seconds. (If a single advertisement is sent in response to multiple solicitations, the delay is relative to the first solicitation.) **In addition, consecutive Router Advertisements sent to the all-nodes multicast address MUST be rate limited to no more than one advertisement every MIN_DELAY_BETWEEN_RAS seconds**.

RQ_000_8325 Router Processing of RS
RFC2461 6.2.6 OPTIONAL
Applies to: Router
Context:

Requirement:
An IPv6 router MAY send a solicited Router advertisement message before the configured Minimum Router advertisement Interval has passed since the previous Router Advertisement message was sent.

Specification Text:
Note that a router is permitted to send multicast Router Advertisements more frequently than indicated by the MinRtrAdvInterval configuration variable so long as the more frequent advertisements are responses to Router Solicitations. In all cases, however, unsolicited multicast advertisements MUST NOT be sent more frequently than indicated by MinRtrAdvInterval.

RQ_000_8326 Startup Router Advertisement Behavior
RFC2461 6.2.6 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST NOT send an unsolicited Router advertisement message before the configured Minimum Router advertisement Interval has passed since the previous Router Advertisement message was sent.
Specification Text:
Note that a router is permitted to send multicast Router Advertisements more frequently than indicated by the MinRtrAdvInterval configuration variable so long as the more frequent advertisements are responses to Router Solicitations. **In all cases, however, unsolicited multicast advertisements MUST NOT be sent more frequently than indicated by MinRtrAdvInterval**.

RQ_000_8327 Discover Neighbor by RS
RFC2461 6.2.6 MANDATORY
Applies to: Router
Context:
An IPv6 router receives a Router Solicitation with the Source Address field in the containing IPv6 packet header set to the Unspecified Address.
Requirement:
The IPv6 node MUST NOT categorize the source node as being on-link (a neighbor).
Specification Text:
Router Solicitations in which the Source Address is the unspecified address MUST NOT update the router's Neighbor Cache; solicitations with a proper source address update the Neighbor Cache as follows. If the router already has a Neighbor Cache entry for the solicitation's sender, the solicitation contains a Source Link-Layer Address option, and the received link-layer address differs from that already in the cache, the link-layer address SHOULD be updated in the appropriate Neighbor Cache entry, and its reachability state MUST also be set to STALE. If there is no existing Neighbor Cache entry for the solicitation's sender, the router creates one, installs the link- layer address and sets its reachability state to STALE as specified in Section 7.3.3. Whether or not a Source Link-Layer Address option is provided, if a Neighbor Cache entry for the solicitation's sender exists (or is created) the entry's IsRouter flag MUST be set to FALSE.

RQ_000_8328 Router Processing of RS
RFC2461 6.2.6 RECOMMENDED
Applies to: Router
Context:
An IPv6 router receives a Router Solicitation from a known neighbor but with Source Link-Layer option set to a value that is different from the link-layer address currently associated with the neighbor's source IP address.
Requirement:
The IPv6 node SHOULD use the received Source Link-Layer Address in all subsequent communications with the source node, SHOULD NOT attempt to verify the reachability of the source node until traffic is sent to it and SHOULD NOT categorize the source node as a router.
Specification Text:
Router Solicitations in which the Source Address is the unspecified address MUST NOT update the router's Neighbor Cache; solicitations with a proper source address update the Neighbor Cache as follows. **If the router already has a Neighbor Cache entry for the solicitation's sender, the solicitation contains a Source Link-Layer Address option, and the received link-layer address differs from that already in the cache, the link-layer address SHOULD be updated in the appropriate Neighbor Cache entry, and its reachability state MUST also be set to STALE**. If there is no existing Neighbor Cache entry for the solicitation's sender, the router creates one, installs the link- layer address and sets its reachability state to STALE as specified in Section 7.3.3. **Whether or not a Source Link-Layer Address option is provided, if a Neighbor Cache entry for the solicitation's sender exists (or is created) the entry's IsRouter flag MUST be set to FALSE**.

RQ_000_8329 Router Processing of RS
RFC2461 6.2.6 MANDATORY
Applies to: Router
Context:
An IPv6 router receives a Router Solicitation from a known neighbor but with Source Link-Layer option set to a valid address when there is no link-layer address currently associated with the neighbor's source IP address.
Requirement:
The IPv6 node MUST use the received Source Link-Layer Address in all subsequent communications with the source node, MUST NOT attempt to verify the reachability of
Specification Text:
Router Solicitations in which the Source Address is the unspecified address MUST NOT update the router's Neighbor Cache; solicitations with a proper source address update the Neighbor Cache as follows. If the router already has a Neighbor Cache entry for the solicitation's sender, the solicitation contains a Source Link-Layer Address option, and the received link-layer address differs from that already in the cache, the link-layer address SHOULD be updated in the appropriate Neighbor Cache entry, and its reachability state MUST also be set to STALE. **If there is no existing Neighbor Cache entry for the solicitation's sender, the router creates one, installs the link- layer address and sets its reachability state to STALE as specified in Section 7.3.3.** Whether or not a Source Link-Layer Address option is provided, if a Neighbor Cache entry for the solicitation's sender exists (or is created) the entry's IsRouter flag MUST be set to FALSE.

RQ_000_8330 Router Processing of RS
RFC2461 6.2.6 MANDATORY
Applies to: Router
Context:
An IPv6 router receives a valid Router Solicitation in which there is no Source Link-layer Address option specified.
Requirement:
The IPv6 router MUST NOT categorize the Router Solicitation source node as a router.
Specification Text:
Router Solicitations in which the Source Address is the unspecified address MUST NOT update the router's Neighbor Cache; solicitations with a proper source address update the Neighbor Cache as follows. If the router already has a Neighbor Cache entry for the solicitation's sender, the solicitation contains a Source Link-Layer Address option, and the received link-layer address differs from that already in the cache, the link-layer address SHOULD be updated in the appropriate Neighbor Cache entry, and its reachability state MUST also be set to STALE. If there is no existing Neighbor Cache entry for the solicitation's sender, the router creates one, installs the link- layer address and sets its reachability state to STALE as specified in Section 7.3.3. **Whether or not a Source Link-Layer Address option is provided, if a Neighbor Cache entry for the solicitation's sender exists (or is created) the entry's IsRouter flag MUST be set to FALSE**.

RQ_000_8332 Router Processing of RA
RFC2461 6.2.7 RECOMMENDED
Applies to: Router
Context:

Requirement:
An IPv6 router SHOULD record in its system error log any inconsistencies detected between the information received in Router advertisements on a particular link and advertised information sent from that link based on at least the following properties:

- Current Hop Limit if not zero (unspecified)
- State of the M-Flag
- State of the O-Flag
- Reachable Time if not zero (unspecified)
- Retransmission Timer if not zero (unspecified)
- MTU options
- Preferred Lifetime of each advertised prefix
- Valid Lifetime of each advertised prefix

Specification Text:
Router Advertisement Consistency

Routers SHOULD inspect valid Router Advertisements sent by other routers and verify that the routers are advertising consistent information on a link. Detected inconsistencies indicate that one or more routers might be misconfigured and SHOULD be logged to system or network management. The minimum set of information to check includes:

- Cur Hop Limit values (except for the unspecified value of zero).

- **Values of the M or O flags.**
- **Reachable Time values (except for the unspecified value of zero).**
- **Retrans Timer values (except for the unspecified value of zero).**
- **Values in the MTU options.**
- **Preferred and Valid Lifetimes for the same prefix.** If AdvPreferredLifetime and/or AdvValidLifetime decrement in real time as specified in section 6.2.7 then the comparison of the lifetimes can not compare the content of the fields in the Router Advertisement but must instead compare the time at which the prefix will become deprecated and invalidated, respectively. Due to link propagation delays and potentially poorly synchronized clocks between the routers such comparison SHOULD allow some time skew.

Note that it is not an error for different routers to advertise different sets of prefixes. Also, some routers might leave some fields as unspecified, i.e., with the value zero, while other routers specify values. The logging of errors SHOULD be restricted to conflicting information that causes hosts to switch from one value to another with each received advertisement.

Any other action on reception of Router Advertisement messages by a router is beyond the scope of this document.

RQ_000_8333 Router Processing of RA

RFC2461 6.2.7 RECOMMENDED

Applies to: Router

Context:

Requirement:

When verifying the consistency of a received Router advertisement message, an IPv6 router SHOULD allow for link propagation delays and poorly synchronized clocks when validating prefix Preferred Lifetimes and prefix Valid Lifetimes.

Specification Text:

Router Advertisement Consistency

Routers SHOULD inspect valid Router Advertisements sent by other routers and verify that the routers are advertising consistent information on a link. Detected inconsistencies indicate that one or more routers might be misconfigured and SHOULD be logged to system or network management. The minimum set of information to check includes:

- Cur Hop Limit values (except for the unspecified value of zero).
- Values of the M or O flags.
- Reachable Time values (except for the unspecified value of zero).
- Retrans Timer values (except for the unspecified value of zero).
- Values in the MTU options.
- Preferred and Valid Lifetimes for the same prefix. **If AdvPreferredLifetime and/or AdvValidLifetime decrement in real time as specified in section 6.2.7 then the comparison of the lifetimes can not compare the content of the fields in the Router Advertisement but must instead compare the time at which the prefix will become deprecated and invalidated, respectively. Due to link propagation delays and potentially poorly synchronized clocks between the routers such comparison SHOULD allow some time skew.**

Note that it is not an error for different routers to advertise different sets of prefixes. Also, some routers might leave some fields as unspecified, i.e., with the value zero, while other routers specify values. The logging of errors SHOULD be restricted to conflicting information that causes hosts to switch from one value to another with each received advertisement.

Any other action on reception of Router Advertisement messages by a router is beyond the scope of this document.

RQ_000_8337 Router Advertisement Behavior on Reconfiguration
RFC2461 6.2.8 RECOMMENDED
Applies to: Router
Context:

Requirement:
Whenever the link-local address for one of its interfaces is changed (by systems management procedures), an IPv6 router SHOULD send up to 3 unsolicited Router advertisement messages from the old link local address with the Router Lifetime field set to zero(0) and up to 3 Router Advertisement messages from the revised link-local address with the Router Lifetime field set to a non-zero value.

Specification Text:
If a router changes the link-local address for one of its interfaces, it SHOULD inform hosts of this change. **The router SHOULD multicast a few Router Advertisements from the old link-local address with the Router Lifetime field set to zero and also multicast a few Router Advertisements from the new link-local address.** The overall effect should be the same as if one interface ceases being an advertising interface, and a different one starts being an advertising interface.

RQ_000_8338 Initialize
RFC2461 6.3.2 MANDATORY
Applies to: Host
Context:

Requirement:
When constructing and processing Neighbor Discovery messages, an IPv6 host MUST use each of the following parameter values unless a different value has been specified in a valid received Router advertisement message:

ND Parameter	Default setting
Link MTU	The value specified in the document that describes how IPv6 operates over the particular link-layer
Current Hop Limit	The value specified in RFC 1700
Base Reachable Time	30,000 milliseconds
Reachable Time	Between 0.5 * Base Reachable Time and 1.5 * Base Reachable Time
Retransmission Timer	1,000 milliseconds

For each of its interfaces, the implementation assigns the following default values: Link MTU - the value defined in the specific document that describes how IPv6 operates over the particular link layer (e.g., [IPv6-ETHER]); Current Hop Limit - For sending unicast packets, the value specified in the "Assigned Numbers" RFC [ASSIGNED] that is in effect at the time of implementation; Reachable Time - a uniformly distributed random value between the protocol constants MIN_RANDOM_FACTOR and MAX_RANDOM_FACTOR times the Base Reachable Time in ms; and Retrans Timer - the protocol constant RETRANS_TIMER in milliseconds.

Specification Text:
Host Variables

A host maintains certain Neighbor Discovery related variables in addition to the data structures defined in Section 5.1. The specific variable names are used for demonstration purposes only, and an implementation is not required to have them, so long as its external behavior is consistent with that described in this document.

These variables have default values that are overridden by information received in Router Advertisement messages. The default values are used when there is no router on the link or when all received Router Advertisements have left a particular value unspecified.

The default values in this specification may be overridden by specific documents that describe how IP operates over different link layers. This rule allows Neighbor Discovery to operate over links with widely varying performance characteristics.

For each interface:

LinkMTU **The MTU of the link. Default: The valued defined in the specific document that describes how IPv6 operates over the particular link layer (e.g., RFC 2464).**

CurHopLimit **The default hop limit to be used when sending (unicast) IP packets.**

Default: The value specified in the "Assigned Numbers" RFC 1700 that was in effect at the time of implementation.

BaseReachableTime
A base value used for computing the random ReachableTime value.
Default: REACHABLE_TIME milliseconds.

ReachableTime **The time a neighbor is considered reachable after receiving a reachability confirmation. This value should be a uniformly-distributed random value between MIN_RANDOM_FACTOR and MAX_RANDOM_FACTOR times BaseReachableTime milliseconds. A new random value should be calculated when BaseReachableTime changes (due to Router Advertisements) or at least every few hours even if no Router Advertisements are received.**

RetransTimer **The time between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.**
Default: RETRANS_TIMER milliseconds

RQ_000_8339 Initialize
RFC2461 6.3.2 and "ReachableTime" RECOMMENDED
Applies to: Host
Context:

Requirement:
An IPv6 host SHOULD calculate a new value of Reachable Time whenever the value of the Base Reachable Time is modified or every few hours.

Specification Text:
Host Variables

A host maintains certain Neighbor Discovery related variables in addition to the data structures defined in Section 5.1. The specific variable names are used for demonstration purposes only, and an implementation is not required to have them, so long as its external behavior is consistent with that described in this document.

These variables have default values that are overridden by information received in Router Advertisement messages. The default values are used when there is no router on the link or when all received Router Advertisements have left a particular value unspecified.

The default values in this specification may be overridden by specific documents that describe how IP operates over different link layers. This rule allows Neighbor Discovery to operate over links with widely varying performance characteristics.

For each interface:

LinkMTU The MTU of the link.
Default: The valued defined in the specific document that describes how IPv6 operates over the particular link layer (e.g., [IPv6-ETHER]).

CurHopLimit The default hop limit to be used when sending (unicast) IP packets.
Default: The value specified in the "Assigned Numbers" RFC [ASSIGNED] that was in effect at the time of implementation.

BaseReachableTime
A base value used for computing the random ReachableTime value.
Default: REACHABLE_TIME milliseconds.

ReachableTime The time a neighbor is considered reachable after receiving a reachability confirmation. This value should be a uniformly-distributed random value between MIN_RANDOM_FACTOR and MAX_RANDOM_FACTOR times BaseReachableTime milliseconds. **A new random value should be calculated when BaseReachableTime changes (due to Router Advertisements) or at least every few hours even if no Router Advertisements are received.**

```
RetransTimer   The time between retransmissions of Neighbor
               Solicitation messages to a neighbor when
               resolving the address or when probing the
               reachability of a neighbor.
               Default: RETRANS_TIMER milliseconds
```

RQ_000_8340 Initialize
RFC2461 6.3.3 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST respond to any valid message received on a multicast-capable interface and sent to the link-local all-users multicast address (FF:02:0:0:0:0:0:2)

For each of its multicast-capable interfaces, the implementation joins the all-nodes multicast address.

Specification Text:
The host joins the all-nodes multicast address on all multicast-capable interfaces.

RQ_000_8342 Host Processing of RA
RFC2461 6.3.4 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST NOT invalidate any information received in previous Router Advertisement messages on the basis of the contents of a received Router Advertisement.

Specification Text:
When multiple routers are present, the information advertised collectively by all routers may be a superset of the information contained in a single Router Advertisement. Moreover, information may also be obtained through other dynamic means, such as stateful autoconfiguration. Hosts accept the union of all received information; **the receipt of a Router Advertisement MUST NOT invalidate all information received in a previous advertisement or from another source**. However, when received information for a specific parameter (e.g., Link MTU) or option (e.g., Lifetime on a specific Prefix) differs from information received earlier, and the parameter/option can only have one value, the most recently-received information is considered authoritative.

RQ_000_8343 Host Processing of RA
RFC2461 6.3.4 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST use the specific parameters and options most recently received in valid Router Advertisement messages when processing or constructing Neighbor Discovery messages.

Specification Text:
When multiple routers are present, the information advertised collectively by all routers may be a superset of the information contained in a single Router Advertisement. Moreover, information may also be obtained through other dynamic means, such as stateful autoconfiguration. Hosts accept the union of all received information; the receipt of a Router Advertisement MUST NOT invalidate all information received in a previous advertisement or from another source. However, **when received information for a specific parameter (e.g., Link MTU) or option (e.g., Lifetime on a specific Prefix) differs from information received earlier, and the parameter/option can only have one value, the most recently-received information is considered authoritative**.

RQ_000_8344 Host Processing of RA
RFC2461 6.3.4 RECOMMENDED
Applies to: Host
Context:

Requirement:
An IPv6 host SHOULD ignore any fields set to a value of "unspecified" in a received Router advertisement message.
Specification Text:
Some Router Advertisement fields (e.g., Cur Hop Limit, Reachable Time and Retrans Timer) may contain a value denoting unspecified. In such cases, the parameter should be ignored and the host should continue using whatever value it is already using. In particular, a host MUST NOT interpret the unspecified value as meaning change back to the default value that was in use before the first Router Advertisement was received. This rule prevents hosts from continually changing an internal variable when one router advertises a specific value, but other routers advertise the unspecified value.

RQ_000_8345 Host Processing of RA
RFC2461 6.3.4 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST NOT revert to using the default value of a Neighbor Discovery parameter on receipt of a valid Router Advertisement message containing the corresponding field set to the value "unspecified".
Specification Text:
Some Router Advertisement fields (e.g., Cur Hop Limit, Reachable Time and Retrans Timer) may contain a value denoting unspecified. In such cases, the parameter should be ignored and the host should continue using whatever value it is already using. **In particular, a host MUST NOT interpret the unspecified value as meaning change back to the default value that was in use before the first Router Advertisement was received**. This rule prevents hosts from continually changing an internal variable when one router advertises a specific value, but other routers advertise the unspecified value.

RQ_000_8346 Host Processing of RA
RFC2461 6.3.4 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a valid Router advertisement message:
- on an interface for which it has not categorized two routers as default routers;
- from a router that it was previously unaware of; and
- containing Router Lifetime field set to a non-zero value.

Requirement:
The IPv6 host MUST categorize the advertising router as a valid default router for the purposes of processing any outgoing IPv6 packets during the period specified in the Router Lifetime field.
Specification Text:
On receipt of a valid Router Advertisement, a host extracts the source address of the packet and does the following:

- **If the address is not already present in the host's Default Router List, and the advertisement's Router Lifetime is non-zero, create a new entry in the list, and initialize its invalidation timer value from the advertisement's Router Lifetime field.**
- If the address is already present in the host's Default Router List as a result of a previously-received advertisement, reset its invalidation timer to the Router Lifetime value in the newly-received advertisement.
- If the address is already present in the host's Default Router List and the received Router Lifetime value is zero, immediately time-out the entry as specified in Section 6.3.5.

To limit the storage needed for the Default Router List, a host MAY choose not to store all of the router addresses discovered via advertisements. **However, a host MUST retain at least two router addresses** and SHOULD retain more. Default router selections are made whenever communication to a destination appears to be failing. Thus, the more routers on the list, the more likely an alternative working router can be found quickly (e.g., without having to wait for the next advertisement to arrive).

RQ_000_8347 Host Processing of RA

RFC2461 6.3.4 RECOMMENDED

Applies to: Host

Context:

An IPv6 host receives a valid Router advertisement message:
- on an interface for which it has already categorized at least two routers as default routers;
- from a router that it was previously unaware of; and
- containing Router Lifetime field set to a non-zero value.

Requirement:

The IPv6 host SHOULD categorize the advertising router as a valid default router for the purposes of processing any outgoing IPv6 packets during the period specified in the Router Lifetime field.

Specification Text:

On receipt of a valid Router Advertisement, a host extracts the source address of the packet and does the following:

- **If the address is not already present in the host's Default Router List, and the advertisement's Router Lifetime is non-zero, create a new entry in the list, and initialize its invalidation timer value from the advertisement's Router Lifetime field.**
- If the address is already present in the host's Default Router List as a result of a previously-received advertisement, reset its invalidation timer to the Router Lifetime value in the newly-received advertisement.
- If the address is already present in the host's Default Router List and the received Router Lifetime value is zero, immediately time-out the entry as specified in Section 6.3.5.

To limit the storage needed for the Default Router List, a host MAY choose not to store all of the router addresses discovered via advertisements. **However, a host MUST retain at least two router addresses and SHOULD retain more.** Default router selections are made whenever communication to a destination appears to be failing. Thus, the more routers on the list, the more likely an alternative working router can be found quickly (e.g., without having to wait for the next advertisement to arrive).

RQ_000_8348 Host Processing of RA

RFC2461 6.3.4 MANDATORY

Applies to: Host

Context:

An IPv6 host receives a valid Router advertisement message:
- from a router that it has currently categorized as a default router; and
- containing Router Lifetime field set to a non-zero value.

Requirement:

The IPv6 host MUST continue to categorize the advertising router as a valid default router for the purposes of processing any outgoing IPv6 packets during the period specified in the Router Lifetime field of the newly-received Router Advertisement.

Specification Text:

On receipt of a valid Router Advertisement, a host extracts the source address of the packet and does the following:

- If the address is not already present in the host's Default Router List, and the advertisement's Router Lifetime is non-zero, create a new entry in the list, and initialize its invalidation timer value from the advertisement's Router Lifetime field.
- **If the address is already present in the host's Default Router List as a result of a previously-received advertisement, reset its invalidation timer to the Router Lifetime value in the newly-received advertisement.**
- If the address is already present in the host's Default Router List and the received Router Lifetime value is zero, immediately time-out the entry as specified in Section 6.3.5.

To limit the storage needed for the Default Router List, a host MAY choose not to store all of the router addresses discovered via advertisements. However, a host MUST retain at least two router addresses and SHOULD retain more. Default router selections are made whenever communication to a destination appears to be failing. Thus, the more routers on the list, the more likely an alternative working router can be found quickly (e.g., without having to wait for the next advertisement to arrive).

RQ_000_8349 Host Processing of RA

RFC2461 6.3.4 RECOMMENDED

Applies to: Host

Context:

An IPv6 host receives a valid Router advertisement message:
- from a router that it has currently categorized as a default router; and
- containing Router Lifetime field set to zero (0).

Requirement:

The IPv6 host SHOULD no longer categorize the advertising router as a default router.

Specification Text:

On receipt of a valid Router Advertisement, a host extracts the source address of the packet and does the following:

- If the address is not already present in the host's Default Router List, and the advertisement's Router Lifetime is non-zero, create a new entry in the list, and initialize its invalidation timer value from the advertisement's Router Lifetime field.
- If the address is already present in the host's Default Router List as a result of a previously-received advertisement, reset its invalidation timer to the Router Lifetime value in the newly-received advertisement.
- **If the address is already present in the host's Default Router List and the received Router Lifetime value is zero, immediately time-out the entry as specified in Section 6.3.5.**

To limit the storage needed for the Default Router List, a host MAY choose not to store all of the router addresses discovered via advertisements. However, a host MUST retain at least two router addresses and SHOULD retain more. Default router selections are made whenever communication to a destination appears to be failing. Thus, the more routers on the list, the more likely an alternative working router can be found quickly (e.g., without having to wait for the next advertisement to arrive).

RQ_000_8351 Host Processing of RA

RFC2461 6.3.4 RECOMMENDED

Applies to: Host

Context:

An IPv6 host receives a valid Router advertisement message:
- from a router that it has currently categorized as a default router; and
- containing a Cur Hop Limit field set to a non-zero value.

Requirement:

The IPv6 host SHOULD use the new Cur Hop Limit value in all IP communication through the default router.

Specification Text:

If the received Cur Hop Limit value is non-zero the host SHOULD set its CurHopLimit variable to the received value.

RQ_000_8352 Host Processing of RA

RFC2461 6.3.4 RECOMMENDED

Applies to: Host

Context:

An IPv6 host receives a valid Router advertisement message:
- from a router that it has currently categorized as a default router; and
- containing a Reachable Time field set to a non-zero value which is different from the Reachable Time value contained in previous Router Advertisements

Requirement:

When determining the reachability of a neighboring node, the IPv6 host SHOULD use a reachability time value calculated as a uniformly distributed random number between 0.5 times the contents of the received Reachability Time field and 1.5 times the Reachability Time field value.

Specification Text:

If the received Reachable Time value is non-zero the host SHOULD set its BaseReachableTime variable to the received value. **If the new value differs from the previous value, the host SHOULD recompute a new random ReachableTime value. ReachableTime is computed as a uniformly-distributed random value between MIN_RANDOM_FACTOR and MAX_RANDOM_FACTOR times the BaseReachableTime**. Using a random component eliminates the possibility Neighbor Unreachability Detection messages synchronize with each other.

RQ_000_8353 Host Processing of RA
RFC2461 6.3.4 RECOMMENDED
Applies to: Host
Context:

Requirement:
In the absence of any new values in the Reachability Time field of received Router Advertisement messages, an IPv6 host SHOULD recompute the reachability time to be used in Neighbor Unreachability determination as a uniformly distributed random number between 0.5 times the contents of the received Reachability Time field and 1.5 times the Reachability Time field value taken from the most recently received Router Advertisement message.
Specification Text:
In most cases, the advertised Reachable Time value will be the same in consecutive Router Advertisements and a host's BaseReachableTime rarely changes. In such cases, an implementation SHOULD insure that a new random value gets recomputed at least once every few hours.

RQ_000_8354 Host Processing of RA
RFC2461 6.3.4 RECOMMENDED
Applies to: Host
Context:
An IPv6 host receives a valid Router advertisement message:
- from a router that it has currently categorized as a default router; and
- containing a Retrans Timer field set to a non-zero value.

Requirement:
The IPv6 host SHOULD use the new Retrans Timer value in all IP communication through the default router.
Specification Text:
The RetransTimer variable SHOULD be copied from the Retrans Timer field, if the received value is non-zero.

RQ_000_8355 Discover Neighbor by RA
RFC2461 6.3.4 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a valid Router advertisement message:
- from a router that it has currently categorized as a default router;
- containing a Router Lifetime field set to a non-zero value; and
- containing a Prefix Information option in which the L-Flag is set to zero (0)

Requirement:
The IPv6 host MUST NOT categorize the prefix specified in the Prefix Information option of the received Router Advertisement message as off-link.
Specification Text:
Prefix Information options that have the "on-link" (L) flag set indicate a prefix identifying a range of addresses that should be considered on-link. **Note, however, that a Prefix Information option with the on-link flag set to zero conveys no information concerning on-link determination and MUST NOT be interpreted to mean that addresses covered by the prefix are off-link.** The only way to cancel a previous on-link indication is to advertise that prefix with the L-bit set and the Lifetime set to zero. The default behavior (see Section 5.2) when sending a packet to an address for which no information is known about the on-link status of the address is to forward the packet to a default router; the reception of a Prefix Information option with the "on-link " (L) flag set to zero does not change this behavior. The reasons for an address being treated as on-link is specified in the definition of "on-link" in Section 2.1. Prefixes with the on-link flag set to zero would normally have the autonomous flag set and be used by RFC 2462.

RQ_000_8356 Discover Neighbor by RA
RFC2461 6.3.4 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a valid Router advertisement message:
- from a router that it has currently categorized as a default router;
- containing a Router Lifetime field set to zero (0); and
- containing a Prefix Information option in which the L-Flag is set to zero (0)

Requirement:
The IPv6 host MUST categorize the prefix specified in the Prefix Information option of the received Router Advertisement message as off-link.

Specification Text:

Prefix Information options that have the "on-link" (L) flag set indicate a prefix identifying a range of addresses that should be considered on-link. **Note, however, that a Prefix Information option with the on-link flag set to zero conveys no information concerning on-link determination and MUST NOT be interpreted to mean that addresses covered by the prefix are off-link. The only way to cancel a previous on-link indication is to advertise that prefix with the L-bit set and the Lifetime set to zero.** The default behavior (see Section 5.2) when sending a packet to an address for which no information is known about the on-link status of the address is to forward the packet to a default router; the reception of a Prefix Information option with the "on-link " (L) flag set to zero does not change this behavior. The reasons for an address being treated as on-link is specified in the definition of "on-link" in Section 2.1. Prefixes with the on-link flag set to zero would normally have the autonomous flag set and be used by RFC 2462

RQ_000_8358 Host Processing of RA

RFC2461 6.3.4 MANDATORY

Applies to: Host

Context:

An IPv6 host receives a valid Router Advertisement message from a default router with the L-Flag in a Prefix Information option set to 1 (on-link) and the Prefix field in the option is set to the link-local prefix (FE80::).

Requirement:

The IPv6 host MUST silently ignore the option.

Specification Text:

For each Prefix Information option with the on-link flag set, a host does the following:

- **If the prefix is the link-local prefix, silently ignore the Prefix Information option.**
- If the prefix is not already present in the Prefix List, and the Prefix Information option's Valid Lifetime field is non-zero, create a new entry for the prefix and initialize its invalidation timer to the Valid Lifetime value in the Prefix Information option.
- If the prefix is already present in the host's Prefix List as the result of a previously-received advertisement, reset its invalidation timer to the Valid Lifetime value in the Prefix Information option. If the new Lifetime value is zero, time-out the prefix immediately (see Section 6.3.5).
- If the Prefix Information option's Valid Lifetime field is zero, and the prefix is not present in the host's Prefix List, silently ignore the option.

RQ_000_8359 Discover Neighbor by RA

RFC2461 6.3.4 MANDATORY

Applies to: Host

Context:

An IPv6 host receives a valid Router Advertisement message:
- from a known default router;
- containing an L-Flag in the Prefix Information options set to 1;
- containing a Prefix in the Prefix Information options set to a value not previously included in a Router advertisement; and
- containing a Valid Lifetime field in the Prefix Information options set to a non-zero value.

Requirement:

The IPv6 host MUST categorize the new prefix as "on-link" and set the prefix's invalidation timer to the value received in the Valid Lifetime field of the Prefix Information option in the Router Advertisement.

Specification Text:

For each Prefix Information option with the on-link flag set, a host does the following:

- If the prefix is the link-local prefix, silently ignore the Prefix Information option.
- **If the prefix is not already present in the Prefix List, and the Prefix Information option's Valid Lifetime field is non-zero, create a new entry for the prefix and initialize its invalidation timer to the Valid Lifetime value in the Prefix Information option.**
- If the prefix is already present in the host's Prefix List as the result of a previously-received advertisement, reset its invalidation timer to the Valid Lifetime value in the Prefix Information option. If the new Lifetime value is zero, time-out the prefix immediately (see Section 6.3.5).

```
   - If the Prefix Information option's Valid Lifetime field is zero,
     and the prefix is not present in the host's Prefix List,
     silently ignore the option.
```

RQ_000_8360 Host Processing of RA

RFC2461 6.3.4 MANDATORY

Applies to: Host

Context:

```
An IPv6 host receives a valid Router Advertisement message:
 - from a known default router;
 - containing an L-Flag in the Prefix Information options set to 1;
 - containing a Prefix in the Prefix Information options set to a value
   previously included in a Router advertisement; and
 - containing a Valid Lifetime field in the Prefix Information options set to
   a non-zero value.
```

Requirement:

```
The IPv6 host MUST set the prefix's invalidation timer to the value received in the Valid
Lifetime field of the Prefix Information option in the Router Advertisement.
```

Specification Text:

```
For each Prefix Information option with the on-link flag set, a host does the following:

   - If the prefix is the link-local prefix, silently ignore the
     Prefix Information option.
   - If the prefix is not already present in the Prefix List, and the
     Prefix Information option's Valid Lifetime field is non-zero,
     create a new entry for the prefix and initialize its
     invalidation timer to the Valid Lifetime value in the Prefix
     Information option.
   - If the prefix is already present in the host's Prefix List as
     the result of a previously-received advertisement, reset its
     invalidation timer to the Valid Lifetime value in the Prefix
     Information option.  If the new Lifetime value is zero, time-out
     the prefix immediately (see Section 6.3.5).
   - If the Prefix Information option's Valid Lifetime field is zero,
     and the prefix is not present in the host's Prefix List,
     silently ignore the option.
```

RQ_000_8361 Discover Neighbor by RA

RFC2461 6.3.4 MANDATORY

Applies to: Host

Context:

```
An IPv6 host receives a valid Router Advertisement message:
 - from a known default router;
 - containing an L-Flag in the Prefix Information options set to 1;
 - containing a Prefix in the Prefix Information options set to a value
   previously included in a Router advertisement; and
 - containing a Valid Lifetime field in the Prefix Information options set to
   zero (0).
```

Requirement:

```
The IPv6 host MUST categorize the prefix as "off-link".
```

Specification Text:

```
For each Prefix Information option with the on-link flag set, a host does the following:

   - If the prefix is the link-local prefix, silently ignore the
     Prefix Information option.
   - If the prefix is not already present in the Prefix List, and the
     Prefix Information option's Valid Lifetime field is non-zero,
     create a new entry for the prefix and initialize its
     invalidation timer to the Valid Lifetime value in the Prefix
     Information option.
   - If the prefix is already present in the host's Prefix List as
     the result of a previously-received advertisement, reset its
     invalidation timer to the Valid Lifetime value in the Prefix
     Information option.  If the new Lifetime value is zero, time-out
     the prefix immediately (see Section 6.3.5).
   - If the Prefix Information option's Valid Lifetime field is zero,
     and the prefix is not present in the host's Prefix List,
     silently ignore the option.
```

RQ_000_8362 Host Processing of RA
RFC2461 6.3.4 MANDATORY
Applies to: Host
Context:

An IPv6 host receives a valid Router Advertisement message:
- from a known default router;
- containing an L-Flag in the Prefix Information options set to 1;
- containing a Prefix in the Prefix Information options set to a value not previously included in a Router advertisement; and
- containing a Valid Lifetime field in the Prefix Information options set to zero (0).

Requirement:

The IPv6 host MUST silently ignore the Prefix Information option in the received Router Advertisement.

Specification Text:

For each Prefix Information option with the on-link flag set, a host does the following:

- If the prefix is the link-local prefix, silently ignore the Prefix Information option.
- If the prefix is not already present in the Prefix List, and the Prefix Information option's Valid Lifetime field is non-zero, create a new entry for the prefix and initialize its invalidation timer to the Valid Lifetime value in the Prefix Information option.
- If the prefix is already present in the host's Prefix List as the result of a previously-received advertisement, reset its invalidation timer to the Valid Lifetime value in the Prefix Information option. If the new Lifetime value is zero, time-out the prefix immediately (see Section 6.3.5).
- **If the Prefix Information option's Valid Lifetime field is zero, and the prefix is not present in the host's Prefix List, silently ignore the option.**

RQ_000_8363 Neighbor Unreachability Detection
RFC2461 6.3.5 MANDATORY
Applies to: Host
Context:

Requirement:

An IPv6 host MUST treat an advertised prefix as "off-link" after the period specified in the Valid Lifetime field in the Prefix Information option of the most recent Router Advertisement message advertising that prefix.

Specification Text:

Whenever the invalidation timer expires for a Prefix List entry, that entry is discarded. No existing Destination Cache entries need be updated, however. Should a reachability problem arise with an existing Neighbor Cache entry, Neighbor Unreachability Detection will perform any needed recovery.

RQ_000_8364 Next Hop Determination
RFC2461 6.3.5 MANDATORY
Applies to: Router, Host
Context:

Requirement:

An IPv6 node MUST ensure that no IP traffic is sent to a neighboring router that it no longer classifies as a default router.

Specification Text:

Whenever the Lifetime of an entry in the Default Router List expires, that entry is discarded. When removing a router from the Default Router list, the node MUST update the Destination Cache in such a way that **all entries using the router perform next-hop determination again rather than continue sending traffic to the (deleted) router.**

RQ_000_8365 Next Hop Determination
RFC2461 6.3.6 MANDATORY
Applies to: Host
Context:

Requirement:
If an IPv6 host has no default router identified for the destination of an outgoing packet , it MUST invoke a procedure for locating and selecting an appropriate default router to which the packet can be forwarded.
Specification Text:
The algorithm for selecting a router depends in part on whether or not a router is known to be reachable. The exact details of how a node keeps track of a neighbor's reachability state are covered in Section 7.3. **The algorithm for selecting a default router is invoked during next-hop determination when no Destination Cache entry exists for an off-link destination** or when communication through an existing router appears to be failing. Under normal conditions, a router would be selected the first time traffic is sent to a destination, with subsequent traffic for that destination using the same router as indicated in the Destination Cache modulo any changes to the Destination Cache caused by Redirect messages.

RQ_000_8366 Next Hop Determination
RFC2461 6.3.6 MANDATORY
Applies to: Host
Context:

Requirement:
If ongoing communication between an IPv6 host and the destination of an outgoing packet appears to be failing, the IPv6 host MUST invoke a procedure for locating and selecting a different default router to which the packet can be forwarded.
Specification Text:
The algorithm for selecting a router depends in part on whether or not a router is known to be reachable. The exact details of how a node keeps track of a neighbor's reachability state are covered in Section 7.3. **The algorithm for selecting a default router is invoked** during next-hop determination when no Destination Cache entry exists for an off-link destination or **when communication through an existing router appears to be failing.** Under normal conditions, a router would be selected the first time traffic is sent to a destination, with subsequent traffic for that destination using the same router as indicated in the Destination Cache modulo any changes to the Destination Cache caused by Redirect messages.

RQ_000_8367 Next Hop Determination
RFC2461 6.3.6 RECOMMENDED
Applies to: Host
Context:

Requirement:
Having located and selected an appropriate default router for a packet destination that is initially off-link, an IPv6 host SHOULD direct all subsequent packets for that destination through the selected router unless instructed by a Redirect message to use a different router.
Specification Text:
The algorithm for selecting a router depends in part on whether or not a router is known to be reachable. The exact details of how a node keeps track of a neighbor's reachability state are covered in Section 7.3. The algorithm for selecting a default router is invoked during next-hop determination when no Destination Cache entry exists for an off-link destination or when communication through an existing router appears to be failing. **Under normal conditions, a router would be selected the first time traffic is sent to a destination, with subsequent traffic for that destination using the same router as indicated in the Destination Cache modulo any changes to the Destination Cache caused by Redirect messages.**

RQ_000_8371 Router Solicitation Behavior
RFC2461 6.3.7 OPTIONAL
Applies to: Host
Context:

Requirement:
When one of its interfaces is initialized (at system startup or by system management procedures), an IPv6 host MAY transmit up to 3 Router Solicitation messages from the interface with each separated by at least 4 seconds.

Specification Text:
When an interface becomes enabled, a host may be unwilling to wait for the next unsolicited Router Advertisement to locate default routers or learn prefixes. To obtain Router Advertisements quickly, a host SHOULD transmit up to MAX_RTR_SOLICITATIONS Router Solicitation messages each separated by at least RTR_SOLICITATION_INTERVAL seconds. Router Solicitations may be sent after any of the following events:

RQ_000_8378 Generate Router Solicitation
RFC2461 6.3.7 MANDATORY
Applies to: Host
Context:

Requirement:
When constructing a Router Solicitation message from one of its interfaces, an IPv6 host MUST set the Destination Address field in the containing IPv6 packet to the link-local All-Routers multicast address (FF02:0:0:0:0:0:0:2) and the Source Address field to either one of the interface's unicast addresses or the IPv6 Unspecified Address (0:0:0:0:0:0:0:0).
Specification Text:
A host sends Router Solicitations to the All-Routers multicast address. The IP source address is set to either one of the interface's unicast addresses or the unspecified address. The Source Link-Layer Address option SHOULD be set to the host's link-layer address, if the IP source address is not the unspecified address

Before a host sends an initial solicitation, it SHOULD delay the transmission for a random amount of time between 0 and MAX_RTR_SOLICITATION_DELAY. This serves to alleviate congestion when many hosts start up on a link at the same time, such as might happen after recovery from a power failure. If a host has already performed a random delay since the interface became (re)enabled (e.g., as part of Duplicate Address Detection [ADDRCONF]) there is no need to delay again before sending the first Router Solicitation message.

RQ_000_8379 Generate RS Source Link-Layer Address Option
RFC2461 6.3.7 RECOMMENDED
Applies to: Host
Context:

Requirement:
When constructing a Router Solicitation message to send from one of its interfaces, an IPv6 host MUST set the Source Link-Layer Address field to its own link-layer address if it has set the IPv6 packet header Source Address field to contain one of the interface's unicast addresses.
Specification Text:
A host sends Router Solicitations to the All-Routers multicast address. The IP source address is set to either one of the interface's unicast addresses or the unspecified address. **The Source Link-Layer Address option SHOULD be set to the host's link-layer address, if the IP source address is not the unspecified address.**

Before a host sends an initial solicitation, it SHOULD delay the transmission for a random amount of time between 0 and MAX_RTR_SOLICITATION_DELAY. This serves to alleviate congestion when many hosts start up on a link at the same time, such as might happen after recovery from a power failure. If a host has already performed a random delay since the interface became (re)enabled (e.g., as part of Duplicate Address Detection [ADDRCONF]) there is no need to delay again before sending the first Router Solicitation message.

RQ_000_8380 Router Solicitation Behavior
RFC2461 6.3.7 RECOMMENDED
Applies to: Host
Context:

Requirement:
An IPv6 host SHOULD delay the transmission of the first Router Solicitation message to be sent from one of its interfaces for a random period of between 0 and 1 second.
Specification Text:
A host sends Router Solicitations to the All-Routers multicast address. The IP source address is set to either one of the interface's unicast addresses or the unspecified address. The Source Link-Layer Address option SHOULD be set to the host's link-layer address, if the IP source address is not the unspecified address.

Before a host sends an initial solicitation, it SHOULD delay the transmission for a random amount of time between 0 and MAX_RTR_SOLICITATION_DELAY. This serves to alleviate congestion when many hosts start up on a link at the same time, such as might happen after recovery from a power failure. If a host has already performed a random delay since the interface became (re)enabled (e.g., as part of Duplicate Address Detection [ADDRCONF]) there is no need to delay again before sending the first Router Solicitation message.

RQ_000_8381 Router Solicitation Behavior
RFC2461 6.3.7 OPTIONAL
Applies to: Host
Context:

Requirement:
An IPv6 host MAY omit delaying the transmission of the first Router Solicitation message to be sent from one of its interfaces for a random period of between 0 and 1 second if it has already performed a random message delay since the interface became (re)enabled.
Specification Text:
A host sends Router Solicitations to the All-Routers multicast address. The IP source address is set to either one of the interface's unicast addresses or the unspecified address. The Source Link-Layer Address option SHOULD be set to the host's link-layer address, if the IP source address is not the unspecified address.

Before a host sends an initial solicitation, it SHOULD delay the transmission for a random amount of time between 0 and MAX_RTR_SOLICITATION_DELAY.}} This serves to alleviate congestion when many hosts start up on a link at the same time, such as might happen after recovery from a power failure. **If a host has already performed a random delay since the interface became (re)enabled (e.g., as part of Duplicate Address Detection RFC 2462) there is no need to delay again before sending the first Router Solicitation message.**

RQ_000_8382 Router Solicitation Behavior
RFC2461 6.3.7 MANDATORY
Applies to: Host
Context:
An IPv6 host has received a valid Router Advertisement message containing a Router Lifetime field set to a non-zero value in response to its transmitted Router Solicitation message.
Requirement:
The IPv6 host MUST NOT send further Router Solicitations from that interface until the next time the interface is re-enabled.
Specification Text:
Once the host sends a Router Solicitation, and receives a valid Router Advertisement with a non-zero Router Lifetime, the host MUST desist from sending additional solicitations on that interface, until the next time one of the above events occurs. Moreover, a host SHOULD send at least one solicitation in the case where an advertisement is received prior to having sent a solicitation. Unsolicited Router Advertisements may be incomplete (see Section 6.2.3); solicited advertisements are expected to contain complete information.

RQ_000_8383 Router Solicitation Behavior
RFC2461 6.3.7 RECOMMENDED
Applies to: Host
Context:
An IPv6 host receives a valid Router Advertisement message containing a non-zero value in the Router Lifetime field on one of its recently (re)enabled interfaces before it has sent an initial Router Solicitation message from that interface.
Requirement:
The IPv6 host SHOULD send at least one Router Solicitation from the interface.
Specification Text:
Once the host sends a Router Solicitation, and receives a valid Router Advertisement with a non-zero Router Lifetime, the host MUST desist from sending additional solicitations on that interface, until the next time one of the above events occurs. **Moreover, a host SHOULD send at least one solicitation in the case where an advertisement is received prior to having sent a solicitation. Unsolicited Router Advertisements may be incomplete (see Section 6.2.3); solicited advertisements are expected to contain complete information.**

RQ_000_8385 Host Processing of RA
RFC2461 6.3.7 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST continue to receive and process Router Advertisement messages on a newly enabled interface after having sent 3 Router Solicitation from that interface and waiting a further 1 second without receiving a Router advertisement in response.
Specification Text:
If a host sends MAX_RTR_SOLICITATIONS solicitations, and receives no Router Advertisements after having waited MAX_RTR_SOLICITATION_DELAY seconds after sending the last solicitation, the host concludes that there are no routers on the link for the purpose of RFC 2462. **However, the host continues to receive and process Router Advertisements messages in the event that routers appear on the link.**

RQ_000_8386 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Solicitation message that does not have the decimal value 255 set in the Hop Limit field of the containing IPv6 packet header.
Specification Text:
A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks:

- **The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.**
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8387 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Solicitation message containing an Authentication Header if the packet fails authentication.
Specification Text:
A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- **If the message includes an IP Authentication Header, the message authenticates correctly.**
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8388 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Solicitation message in which the contents of the ICMPv6 Checksum field does not match the calculated checksum value.
Specification Text:
A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- **ICMP Checksum is valid.**
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8389 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Solicitation message in which the ICMPv6 Code field is not set to zero (0)
Specification Text:
A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- **ICMP Code is 0.**
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8390 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Solicitation message in which the ICMPv6 packet length (derived from the Payload Length field in the IPv6 Packet Header) is less than 24 octets.
Specification Text:
A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.

- **ICMP length (derived from the IP length) is 24 or more octets.**
- Target Address is not a multicast address.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8391 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Solicitation message that has the IPv6 Unspecified Address (0::0) set in the Source Address field of the containing IPv6 Packet Header but the Destination Address field is not set to a Solicited Node multicast address
Specification Text:
A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- All included options have a length that is greater than zero.
- **If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address.**
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8392 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Solicitation message that has the IPv6 Unspecified Address (0::0) set in the Source Address field of the containing IPv6 Packet Header but the solicitation includes a Source Link-Layer Address option.
Specification Text:
A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address.
- **If the IP source address is the unspecified address, there is no source link-layer address option in the message.**

RQ_000_8393 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Solicitation message in which the Target Address field contains a multicast address

Specification Text:
A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- **Target Address is not a multicast address.**
- All included options have a length that is greater than zero.
- If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8394 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Solicitation message which contains an option in which the Length field is set to zero (0).
Specification Text:
A node MUST silently discard any received Neighbor Solicitation messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- **All included options have a length that is greater than zero.**
- If the IP source address is the unspecified address, the IP destination address is a solicited-node multicast address.
- If the IP source address is the unspecified address, there is no source link-layer address option in the message.

RQ_000_8395 Process Field Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST ignore the contents of the Reserved field in a received Neighbor Solicitation message.
Specification Text:
The contents of the Reserved field, and of any unrecognized options, **MUST be ignored.** Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values.

RQ_000_8396 Process Option Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ignore the contents of any unrecognized option in a received Neighbor Solicitation message.
Specification Text:
The contents of the Reserved field, and **of any unrecognized options, MUST be ignored.** Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values.

RQ_000_8397 Process Option Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ignore any value set in a Target Link-Layer Address option received in a Neighbor Solicitation message
Specification Text:
The contents of any defined options that are not specified to be used with Neighbor Solicitation messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Source Link-Layer Address option.

RQ_000_8398 Process Option Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ignore any value set in a Prefix Information option received in a Neighbor Solicitation message
Specification Text:
The contents of any defined options that are not specified to be used with Neighbor Solicitation messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Source Link-Layer Address option.

RQ_000_8399 Process Option Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST ignore any value set in a Redirected Header option received in a Neighbor Solicitation message
Specification Text:
The contents of any defined options that are not specified to be used with Neighbor Solicitation messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Source Link-Layer Address option.

RQ_000_8400 Process Option Anomalies in NS
RFC2461 7.1.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ignore any value set in an MTU option received in a Neighbor Solicitation message
Specification Text:
The contents of any defined options that are not specified to be used with Neighbor Solicitation messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Source Link-Layer Address option.

RQ_000_8401 Process Field Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor advertisement that does not have the decimal value 255 set into the Hop Limit field in the containing IPv6 Packet Header.
Specification Text:
A node MUST silently discard any received Neighbor Advertisement messages that do not satisfy all of the following validity checks:

- **The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.**
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- If the IP Destination Address is a multicast address the Solicited flag is zero.
- All included options have a length that is greater than zero.

RQ_000_8402 Process Field Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Advertisement message containing an Authentication Header if the packet fails authentication.
Specification Text:
A node MUST silently discard any received Neighbor Advertisement messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- **If the message includes an IP Authentication Header, the message authenticates correctly.**
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- If the IP Destination Address is a multicast address the Solicited flag is zero.
- All included options have a length that is greater than zero.

RQ_000_8403 Process Field Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Advertisement message in which the value set in the ICMPv6 Checksum field is not identical to the checksum value calculated by the node.
Specification Text:
A node MUST silently discard any received Neighbor Advertisement messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- **ICMP Checksum is valid.**
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- If the IP Destination Address is a multicast address the Solicited flag is zero.
- All included options have a length that is greater than zero.

RQ_000_8404 Process Field Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Advertisement message in which the ICMPv6 Code field is set to a non-zero value.
Specification Text:
A node MUST silently discard any received Neighbor Advertisement messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- **ICMP Code is 0.**
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- If the IP Destination Address is a multicast address the Solicited flag is zero.
- All included options have a length that is greater than zero.

RQ_000_8405 Process Field Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor advertisement message in which the ICMPv6 packet length (derived from the Payload Length field in the IPv6 Packet Header) is less than 24 octets.
Specification Text:
A node MUST silently discard any received Neighbor Advertisement messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- **ICMP length (derived from the IP length) is 24 or more octets.**
- Target Address is not a multicast address.
- If the IP Destination Address is a multicast address the Solicited flag is zero.
- All included options have a length that is greater than zero.

RQ_000_8406 Process Field Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Advertisement message in which the Target Address field contains a multicast address
Specification Text:
A node MUST silently discard any received Neighbor Advertisement messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- **Target Address is not a multicast address.**
- If the IP Destination Address is a multicast address the Solicited flag is zero.

- All included options have a length that is greater than zero.

RQ_000_8407 Process Solicited Neighbor Advertisement
RFC2461 7.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Advertisement message that has a multicast address set in the Destination Address field of the containing IPv6 Packet Header and a Solicited Flag set to one (1)
Specification Text:
A node MUST silently discard any received Neighbor Advertisement messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- **If the IP Destination Address is a multicast address the Solicited flag is zero.**
- All included options have a length that is greater than zero.

RQ_000_8408 Process Option Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST silently discard a received Neighbor Advertisement message which contains an option in which the Length field is set to zero (0).
Specification Text:
A node MUST silently discard any received Neighbor Advertisement messages that do not satisfy all of the following validity checks:

- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 24 or more octets.
- Target Address is not a multicast address.
- If the IP Destination Address is a multicast address the Solicited flag is zero.
- **All included options have a length that is greater than zero.**

RQ_000_8409 Process Field Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST ignore the contents of the Reserved field in a received Neighbor advertisement message.
Specification Text:
The contents of the Reserved field, and of any unrecognized options, **MUST be ignored.** Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values.

RQ_000_8410 Process Option Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST ignore the contents of any unrecognized options contained in a received Neighbor Advertisement message.
Specification Text:
The contents of the Reserved field, and **of any unrecognized options, MUST be ignored.** Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values.

RQ_000_8411 Process Option Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST ignore a Source Link-Layer Address option received in a Neighbor Advertisement message.
Specification Text:
The contents of any defined options that are not specified to be used with Neighbor Advertisement messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Target Link-Layer Address option.

RQ_000_8412 Process Option Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST ignore a Prefix Information option received in a Neighbor Advertisement message.
Specification Text:
The contents of any defined options that are not specified to be used with Neighbor Advertisement messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Target Link-Layer Address option.

RQ_000_8413 Process Option Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ignore a Redirected Header option received in a Neighbor Advertisement message.
Specification Text:
The contents of any defined options that are not specified to be used with Neighbor Advertisement messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Target Link-Layer Address option.

RQ_000_8414 Process Option Anomalies in NA
RFC2461 7.1.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ignore an MTU option received in a Neighbor Advertisement message.
Specification Text:
The contents of any defined options that are not specified to be used with Neighbor Advertisement messages MUST be ignored and the packet processed as normal. The only defined option that may appear is the Target Link-Layer Address option.

RQ_000_8415 Address Resolution
RFC2461 7.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST invoke Address Resolution procedures before sending a packet to a Destination Address which has been determined to be on-link but for which the corresponding link-layer address is unknown.
Specification Text:
Address resolution is the process through which a node determines the link-layer address of a neighbor given only its IP address. **Address resolution is performed only on addresses that are determined to be on-link and for which the sender does not know the corresponding link-layer address.** Address resolution is never performed on multicast addresses.

RQ_000_8416 Address Resolution
RFC2461 7.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT invoke Address Resolution procedures before sending a packet to a Destination Address which has been determined to be off-link.
Specification Text:
Address resolution is the process through which a node determines the link-layer address of a neighbor given only its IP address. **Address resolution is performed only on addresses that are determined to be on-link and for which the sender does not know the corresponding link-layer address.** Address resolution is never performed on multicast addresses.

RQ_000_8417 Address Resolution
RFC2461 7.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT invoke Address Resolution procedures before sending a packet to a Destination Address for which the corresponding link-layer address is known.
Specification Text:
Address resolution is the process through which a node determines the link-layer address of a neighbor given only its IP address. **Address resolution is performed only on addresses that are determined to be on-link and for which the sender does not know the corresponding link-layer address.** Address resolution is never performed on multicast addresses.

RQ_000_8418 Address Resolution
RFC2461 7.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT invoke Address Resolution procedures before sending a packet to a Destination Address which is a multicast address.
Specification Text:
Address resolution is the process through which a node determines the link-layer address of a neighbor given only its IP address. Address resolution is performed only on addresses that are determined to be on-link and for which the sender does not know the corresponding link-layer address. **Address resolution is never performed on multicast addresses.**

RQ_000_8419 Initialize
RFC2461 7.2.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST accept and process all packets received at a multicast-capable interface and with the Destination Address field in the packet header set to either the link-local All-Nodes multicast address (FF02:0:0:0:0:0:0:1) or any one of the Solicited Node multicast addresses corresponding to the IP addresses assigned to the interface (FF02:0:0:0:0:1:FFxx:xxxx).
Specification Text:
When a multicast-capable interface becomes enabled the node MUST join the all-nodes multicast address on that interface, as well as the solicited-node multicast address corresponding to each of the IP addresses assigned to the interface.

RQ_000_8420 Address Use
RFC2461 7.2.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When a new address is added (by system management procedures) to one of its multicast-capable interfaces, an IPv6 node MUST accept and process any IPv6 packet in which the Destination Address field is set to the Solicited Node multicast address corresponding to the new address (FF02:0:0:0:0:1:FFxx:xxxx).
Specification Text:
The set of addresses assigned to an interface may change over time. New addresses might be added and old addresses might be removed [RFC 2462]. In such cases the node MUST join and leave the solicited-node multicast address corresponding to the new and old addresses, respectively. Note that multiple unicast addresses may map into the same solicited-node multicast address; a node MUST NOT leave the solicited-node multicast group until all assigned addresses corresponding to that multicast address have been removed.

RQ_000_8421 Address Use
RFC2461 7.2.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When an existing address is removed (by system management procedures) from one of its multicast-capable interfaces, an IPv6 node MUST NOT accept or process any IPv6 packet in which the Destination Address field is set to the Solicited Node multicast address corresponding to the removed address (FF02:0:0:0:0:1:FFxx:xxxx) unless at least one other existing unicast address assigned to the interface maps to the same Solicited-Node multicast address.
Specification Text:
The set of addresses assigned to an interface may change over time. New addresses might be added and old addresses might be removed [ADDRCONF]. In such cases the node MUST join and leave the solicited-node multicast address corresponding to the new and old addresses, respectively. Note that multiple unicast addresses may map into the same solicited-node multicast address; a node MUST NOT leave the solicited-node multicast group until all assigned addresses corresponding to that multicast address have been removed.

RQ_000_8422 Address Use
RFC2461 7.2.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When an existing address is removed (by system management procedures) from one of its multicast-capable interfaces, an IPv6 node MUST NOT accept or process any IPv6 packet in which the Destination Address field is set to the Solicited Node multicast address corresponding to the removed address (FF02:0:0:0:0:1:FFxx:xxxx) if no other existing unicast address assigned to the interface maps to the same Solicited-Node multicast address.

Specification Text:
The set of addresses assigned to an interface may change over time. New addresses might be added and old addresses might be removed [RFC 2462]. In such cases the node MUST join and leave the solicited-node multicast address corresponding to the new and old addresses, respectively. Note that multiple unicast addresses may map into the same solicited-node multicast address; a node MUST NOT leave the solicited-node multicast group until all assigned addresses corresponding to that multicast address have been removed.

RQ_000_8423 Generate NS for Address Resolution
RFC2461 7.2.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
Before sending a packet to an IP address for which the corresponding link-layer address is unknown, an IPv6 node MUST send a Neighbor Solicitation message with the Destination Address field in the containing IPv6 Packet header set to the Solicited-Node multicast address corresponding to the target node's IP address.
Specification Text:
When a node has a unicast packet to send to a neighbor, but does not know the neighbor's link-layer address, it performs address resolution. For multicast-capable interfaces this entails creating a Neighbor Cache entry in the INCOMPLETE state and transmitting a Neighbor Solicitation message targeted at the neighbor. The solicitation is sent to the solicited-node multicast address corresponding to the target address.

RQ_000_8424 Generate NS for Address Resolution
RFC2461 7.2.2 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Solicitation message, an IPv6 node SHOULD set the Source Address field in the containing IPv6 Packet header to the Source Address of the packet that prompted the solicitation if that address is one of the addresses assigned to the outgoing interface.
Specification Text:
If the source address of the packet prompting the solicitation is the same as one of the addresses assigned to the outgoing interface, that address SHOULD be placed in the IP Source Address of the outgoing solicitation. Otherwise, any one of the addresses assigned to the interface should be used. Using the prompting packet's source address when possible insures that the recipient of the Neighbor Solicitation installs in its Neighbor Cache the IP address that is highly likely to be used in subsequent return traffic belonging to the prompting packet's "connection".

RQ_000_8425 Generate NS for Address Resolution
RFC2461 7.2.2 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Solicitation message, an IPv6 node SHOULD set the Source Address field in the containing IPv6 Packet header to one of the addresses assigned to the outgoing interface if the source address of the packet prompting the solicitation is not one of the addresses assigned to the interface.
Specification Text:
If the source address of the packet prompting the solicitation is the same as one of the addresses assigned to the outgoing interface, that address SHOULD be placed in the IP Source Address of the outgoing solicitation. **Otherwise, any one of the addresses assigned to the interface should be used.** Using the prompting packet's source address when possible insures that the recipient of the Neighbor Solicitation installs in its Neighbor Cache the IP address that is highly likely to be used in subsequent return traffic belonging to the prompting packet's "connection".

RQ_000_8426 Generate NS for Address Resolution
RFC2461 7.2.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Solicitation message to be sent to a Solicited-Node multicast address, an IPv6 node MUST include its own link-layer address as a Source Link-Layer Address option in the solicitation.
Specification Text:
If the solicitation is being sent to a solicited-node multicast address, the sender MUST include its link-layer address (if it has one) as a Source Link-Layer Address option. Otherwise, the sender SHOULD include its link-layer address (if it has one) as a Source Link-Layer Address option. Including the source link-layer address in a multicast solicitation is required to give the target an address to which it can send the Neighbor Advertisement. On unicast solicitations, an implementation MAY omit the Source Link-Layer Address option. The assumption here is that if the sender has a peer's link-layer address in its cache, there is a high probability that the peer will also have an entry in its cache for the sender. Consequently, it need not be sent.

RQ_000_8427 Generate NS for Address Resolution
RFC2461 7.2.2 RECOMMENDED
Applies to: Router, Host
Context:

Requirement:
When constructing a Neighbor Solicitation message to be sent to an address that is not a Solicited-Node multicast address, an IPv6 node SHOULD include its own link-layer address as a Source Link-Layer Address option in the solicitation.
Specification Text:
If the solicitation is being sent to a solicited-node multicast address, the sender MUST include its link-layer address (if it has one) as a Source Link-Layer Address option. **Otherwise, the sender SHOULD include its link-layer address (if it has one) as a Source Link-Layer Address option.** Including the source link-layer address in a multicast solicitation is required to give the target an address to which it can send the Neighbor Advertisement. On unicast solicitations, an implementation MAY omit the Source Link-Layer Address option. The assumption here is that if the sender has a peer's link-layer address in its cache, there is a high probability that the peer will also have an entry in its cache for the sender. Consequently, it need not be sent.

RQ_000_8428 Generate NS for Address Resolution
RFC2461 7.2.2 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor Solicitation message to be sent to a unicast address, an IPv6 node MAY omit the Source Link-Layer Address option in the solicitation.
Specification Text:
If the solicitation is being sent to a solicited-node multicast address, the sender MUST include its link-layer address (if it has one) as a Source Link-Layer Address option. Otherwise, the sender SHOULD include its link-layer address (if it has one) as a Source Link-Layer Address option. Including the source link-layer address in a multicast solicitation is required to give the target an address to which it can send the Neighbor Advertisement. **On unicast solicitations, an implementation MAY omit the Source Link-Layer Address option.** The assumption here is that if the sender has a peer's link-layer address in its cache, there is a high probability that the peer will also have an entry in its cache for the sender. Consequently, it need not be sent.

RQ_000_8432 Address Resolution Data Queue Handling
RFC2461 7.2.2 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
While waiting for the address resolution procedure for a particular IP address (neighbor) to complete, an IPv6 node MUST delay sending any packets which are not part of that procedure to that address.

Specification Text:
While waiting for address resolution to complete, the sender MUST, for each neighbor, retain a small queue of packets waiting for address resolution to complete. The queue MUST hold at least one packet, and MAY contain more. However, the number of queued packets per neighbor SHOULD be limited to some small value. When a queue overflows, the new arrival SHOULD replace the oldest entry. Once address resolution completes, the node transmits any queued packets.

RQ_000_8433 Address Resolution Behavior
RFC2461 7.2.2 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
An IPv6 node SHOULD retransmit a Neighbor Solicitation message every 1 second until a valid Neighbor advertisement message is received as a response.
Specification Text:
While awaiting a response, the sender SHOULD retransmit Neighbor Solicitation messages approximately every RetransTimer milliseconds, even in the absence of additional traffic to the neighbor. Retransmissions MUST be rate-limited to at most one solicitation per neighbor every RetransTimer milliseconds.

RQ_000_8434 Address Resolution Behavior
RFC2461 7.2.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
After sending a Neighbor Solicitation message to a particular IP address, an IPv6 node MUST NOT send another Neighbor Solicitation message to the same address within 1 second.
Specification Text:
While awaiting a response, the sender SHOULD retransmit Neighbor Solicitation messages approximately every RetransTimer milliseconds, even in the absence of additional traffic to the neighbor. **Retransmissions MUST be rate-limited to at most one solicitation per neighbor every RetransTimer milliseconds.**

RQ_000_8435 Address Resolution Behavior
RFC2461 7.2.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
If a valid Neighbor Advertisement message has not been received as a response after 3 Neighbor Solicitations have been sent to a particular IP address, an IPv6 node MUST send an ICMPv6 packet in response to each delayed packet awaiting address resolution with the Type field set to 1 (Destination Unreachable) and the Code field set to 3 (Address Unreachable).
Specification Text:
If no Neighbor Advertisement is received after MAX_MULTICAST_SOLICIT solicitations, address resolution has failed. The sender MUST return ICMP destination unreachable indications with code 3 (Address Unreachable) for each packet queued awaiting address resolution.

RQ_000_8436 Process Field Anomalies in NS
RFC2461 7.2.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 host MUST silently discard a received Neighbor Solicitation message in which the Target Address field does not contain:

- a unicast or anycast address assigned to the receiving interface;
- a unicast address for which the receiving IPv6 node is offering proxy service; OR
- a "tentative" address upon which Duplicate Address Detection is being performed.

Specification Text:

A valid Neighbor Solicitation that does not meet any the following requirements MUST be silently discarded:

- **The Target Address is a "valid" unicast or anycast address assigned to the receiving interface [RFC 2462],**
- The Target Address is a unicast address for which the node is offering proxy service, or
- The Target Address is a "tentative" address on which Duplicate Address Detection is being performed [RFC 2462].

RQ_000_8438 Address Resolution

RFC2461 7.2.3 RECOMMENDED

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Solicitation with the Source Address field in the containing IPV6 Packet header set to the IP address of a known neighboring node and with the same neighbor's link-layer address set in the Source Link-Layer Address option.

Requirement:

The IPv6 node SHOULD update its internal information related to the known neighboring node while leaving its categorization as either a host or a router unchanged before sending a Neighbor Advertisement as a response.

Specification Text:

If the Target Address is tentative, the Neighbor Solicitation should be processed as described in RFC 2462. Otherwise, the following description applies. **If the Source Address is not the unspecified address and, on link layers that have addresses, the solicitation includes a Source Link-Layer Address option, then the recipient SHOULD create or update the Neighbor Cache entry for the IP Source Address of the solicitation**. If an entry does not already exist, the node SHOULD create a new one and set its reachability state to STALE as specified in Section 7.3.3. If an entry already exists, and the cached link-layer address differs from the one in the received Source Link-Layer option, the cached address should be replaced by the received address and the entry's reachability state MUST be set to STALE.

If a Neighbor Cache entry is created the IsRouter flag SHOULD be set to FALSE. This will be the case even if the Neighbor Solicitation is sent by a router since the Neighbor Solicitation messages do not contain an indication of whether or not the sender is a router. In the event that the sender is a router, subsequent Neighbor Advertisement or Router Advertisement messages will set the correct IsRouter value. If a Neighbor Cache entry already exists its IsRouter flag MUST NOT be modified.

If the Source Address is the unspecified address the node MUST NOT create or update the Neighbor Cache entry.

After any updates to the Neighbor Cache, the node sends a Neighbor Advertisement response as described in the next section.

RQ_000_8439 Address Resolution

RFC2461 7.2.3 RECOMMENDED

Applies to: Router, Host

Context:

An IPv6 node receives a valid Neighbor Solicitation with the Source Address field in the containing IPV6 Packet header set to an IP address which is not the Unspecified Address (0::0) and not that of a known neighboring node and with an unknown neighbor's link-layer address set in the Source Link-Layer Address option.

Requirement:

The IPv6 node SHOULD create internal information related to the previously unknown neighboring node and categorize it as a host before sending a Neighbor Advertisement as a response.

Specification Text:

If the Target Address is tentative, the Neighbor Solicitation should be processed as described in RFC 2462. Otherwise, the following description applies. **If the Source Address is not the unspecified address and, on link layers that have addresses, the solicitation includes a Source Link-Layer Address option, then the recipient SHOULD create or update the Neighbor Cache entry for the IP Source Address of the solicitation. If an entry does not already exist, the node SHOULD create a new one** and set its reachability state to STALE as specified in Section 7.3.3. If an entry already exists, and the cached link-layer address differs from the one in the received Source Link-Layer option, the cached address should be replaced by the received address and the entry's reachability state MUST be set to STALE.

If a Neighbor Cache entry is created the IsRouter flag SHOULD be set to FALSE. This will be the case even if the Neighbor Solicitation is sent by a router since the Neighbor Solicitation messages do not contain an indication of whether or not the sender is a router. In the event that the sender is a router, subsequent Neighbor Advertisement or Router Advertisement messages will set the correct IsRouter value. If a Neighbor Cache entry already exists its IsRouter flag MUST NOT be modified.

If the Source Address is the unspecified address the node MUST NOT create or update the Neighbor Cache entry.

After any updates to the Neighbor Cache, the node sends a Neighbor Advertisement response as described in the next section.

RQ_000_8440 Address Resolution

RFC2461 7.2.3 RECOMMENDED

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Solicitation with the Source Address field in the containing IPV6 Packet header set to the IP address of a known neighboring node and with a link-layer address which is not the one previously associated with the neighbor set in the Source Link-Layer Address option.

Requirement:

The IPv6 node SHOULD update its internal information to replace the existing link-layer address associated with the neighboring node with the received link-layer address while leaving its categorization as either a host or a router unchanged before sending a Neighbor Advertisement as a response.

Specification Text:

If the Target Address is tentative, the Neighbor Solicitation should be processed as described in RFC 2462. Otherwise, the following description applies. If the Source Address is not the unspecified address and, on link layers that have addresses, the solicitation includes a Source Link-Layer Address option, then the recipient SHOULD create or update the Neighbor Cache entry for the IP Source Address of the solicitation. If an entry does not already exist, the node SHOULD create a new one and set its reachability state to STALE as specified in Section 7.3.3. **If an entry already exists, and the cached link-layer address differs from the one in the received Source Link-Layer option, the cached address should be replaced by the received address and the entry's reachability state MUST be set to STALE.**

If a Neighbor Cache entry is created the IsRouter flag SHOULD be set to FALSE. This will be the case even if the Neighbor Solicitation is sent by a router since the Neighbor Solicitation messages do not contain an indication of whether or not the sender is a router. In the event that the sender is a router, subsequent Neighbor Advertisement or Router Advertisement messages will set the correct IsRouter value. **If a Neighbor Cache entry already exists its IsRouter flag MUST NOT be modified.**

If the Source Address is the unspecified address the node MUST NOT create or update the Neighbor Cache entry.

After any updates to the Neighbor Cache, the node sends a Neighbor Advertisement response as described in the next section.

RQ_000_8441 Process NS for Address Resolution

RFC2461 7.2.3 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Solicitation with the Source Address field in the containing IPV6 Packet header set to the unspecified address (0::0) and a known neighboring node's link-layer address set in the Source Link-Layer Address option.

Requirement:

The IPv6 node MUST NOT update its internal information related to the neighbor associated with the received link-layer address.

Specification Text:

If the Target Address is tentative, the Neighbor Solicitation should be processed as described in RFC 2462. Otherwise, the following description applies. If the Source Address is not the unspecified address and, on link layers that have addresses, the solicitation includes a Source Link-Layer Address option, then the recipient SHOULD create or update the Neighbor Cache entry for the IP Source Address of the solicitation. If an entry does not already exist, the node SHOULD create a new one and set its reachability state to STALE as specified in Section 7.3.3. If an entry already exists, and the cached link-layer address differs from the one in the received Source Link-Layer option, the cached address should be replaced by the received address and the entry's reachability state MUST be set to STALE.

If a Neighbor Cache entry is created the IsRouter flag SHOULD be set to FALSE. This will be the case even if the Neighbor Solicitation is sent by a router since the Neighbor Solicitation messages do not contain an indication of whether or not the sender is a router. In the event that the sender is a router, subsequent Neighbor Advertisement or Router Advertisement messages will set the correct IsRouter value. If a Neighbor Cache entry already exists its IsRouter flag MUST NOT be modified.

If the Source Address is the unspecified address the node MUST NOT create or update the Neighbor Cache entry.

After any updates to the Neighbor Cache, the node sends a Neighbor Advertisement response as described in the next section.

RQ_000_8442 Process NS for Address Resolution

RFC2461 7.2.3 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Solicitation with the Source Address field in the containing IPV6 Packet header set to the unspecified address (0::0) and a previously unknown link-layer address set in the Source Link-Layer Address option.

Requirement:

The IPv6 node MUST NOT create new internal information related to the received link-layer address.

Specification Text:

If the Target Address is tentative, the Neighbor Solicitation should be processed as described in RFC 2462. Otherwise, the following description applies. If the Source Address is not the unspecified address and, on link layers that have addresses, the solicitation includes a Source Link-Layer Address option, then the recipient SHOULD create or update the Neighbor Cache entry for the IP Source Address of the solicitation. If an entry does not already exist, the node SHOULD create a new one and set its reachability state to STALE as specified in Section 7.3.3. If an entry already exists, and the cached link-layer address differs from the one in the received Source Link-Layer option, the cached address should be replaced by the received address and the entry's reachability state MUST be set to STALE.

If a Neighbor Cache entry is created the IsRouter flag SHOULD be set to FALSE. This will be the case even if the Neighbor Solicitation is sent by a router since the Neighbor Solicitation messages do not contain an indication of whether or not the sender is a router. In the event that the sender is a router, subsequent Neighbor Advertisement or Router Advertisement messages will set the correct IsRouter value. If a Neighbor Cache entry already exists its IsRouter flag MUST NOT be modified.

If the Source Address is the unspecified address the node MUST NOT create or update the Neighbor Cache entry.

After any updates to the Neighbor Cache, the node sends a Neighbor Advertisement response as described in the next section.

RQ_000_8443 Process NS for Address Resolution

RFC2461 7.2.4 OPTIONAL

Applies to: Host, Router

Context:

Requirement:

When constructing a Neighbor advertisement message as a response to a valid Neighbor Solicitation message that had the Destination Address field of the containing IPv6 Packet header set to a non-multicast address, an IPv6 node MAY omit the Target Link-Layer Address option in the Advertisement.

Specification Text:

A node sends a Neighbor Advertisement in response to a valid Neighbor Solicitation targeting one of the node's assigned addresses. The Target Address of the advertisement is copied from the Target Address of the solicitation. **If the solicitation's IP Destination Address is not a multicast address, the Target Link-Layer Address option MAY be omitted;** the neighboring node's cached value must already be current in order for the solicitation to have been received. If the solicitation's IP Destination Address is a multicast address, the Target Link-Layer option MUST be included in the advertisement. Furthermore, if the node is a router, it MUST set the Router flag to one; otherwise it MUST set the flag to zero.

RQ_000_8444 Process NS for Address Resolution
RFC2461 7.2.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor advertisement message as a response to a valid Neighbor Solicitation message with a multicast address set in the Destination Address field of the containing IPv6 Packet header, an IPv6 node MUST include the Target Link-Layer Address option in the Advertisement.
Specification Text:
A node sends a Neighbor Advertisement in response to a valid Neighbor Solicitation targeting one of the node's assigned addresses. The Target Address of the advertisement is copied from the Target Address of the solicitation. If the solicitation's IP Destination Address is not a multicast address, the Target Link-Layer Address option MAY be omitted; the neighboring node's cached value must already be current in order for the solicitation to have been received. **If the solicitation's IP Destination Address is a multicast address, the Target Link-Layer option MUST be included in the advertisement.** Furthermore, if the node is a router, it MUST set the Router flag to one; otherwise it MUST set the flag to zero.

RQ_000_8445 Process NS for Address Resolution
RFC2461 7.2.4 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Neighbor advertisement message as a response to a valid Neighbor Solicitation message, an IPv6 router MUST set the Router Flag (R-Flag) to one (1) in the advertisement.
Specification Text:
A node sends a Neighbor Advertisement in response to a valid Neighbor Solicitation targeting one of the node's assigned addresses. The Target Address of the advertisement is copied from the Target Address of the solicitation. If the solicitation's IP Destination Address is not a multicast address, the Target Link-Layer Address option MAY be omitted; the neighboring node's cached value must already be current in order for the solicitation to have been received. If the solicitation's IP Destination Address is a multicast address, the Target Link-Layer option MUST be included in the advertisement. **Furthermore, if the node is a router, it MUST set the Router flag to one**; otherwise it MUST set the flag to zero.

RQ_000_8446 Process NS for Address Resolution
RFC2461 7.2.4 MANDATORY
Applies to: Host
Context:

Requirement:
When constructing a Neighbor advertisement message as a response to a valid Neighbor Solicitation message, an IPv6 host MUST set the Router Flag (R-Flag) to zero (0) in the advertisement.
Specification Text:
A node sends a Neighbor Advertisement in response to a valid Neighbor Solicitation targeting one of the node's assigned addresses. The Target Address of the advertisement is copied from the Target Address of the solicitation. If the solicitation's IP Destination Address is not a multicast address, the Target Link-Layer Address option MAY be omitted; the neighboring node's cached value must already be current in order for the solicitation to have been received. If the solicitation's IP Destination Address is a multicast address, the Target Link-Layer option MUST be included in the advertisement. Furthermore, if the node is a router, it MUST set the Router flag to one; **otherwise it MUST set the flag to zero.**

RQ_000_8447 Process NS for Address Resolution
RFC2461 7.2.4 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor advertisement message which is a response to a valid Neighbor Solicitation message and in which the Target Address field is set to an anycast address, an IPv6 node SHOULD set the Override Flag (O-Flag) to zero (0) in the advertisement.

Specification Text:
If the Target Address is either an anycast address or a unicast address for which the node is providing proxy service, or the Target Link-Layer Address option is not included, **the Override flag SHOULD be set to zero.** Otherwise, the Override flag SHOULD be set to one. Proper setting of the Override flag ensures that nodes give preference to non-proxy advertisements, even when received after proxy advertisements, and also ensures that the first advertisement for an anycast address "wins".

RQ_000_8448 Process NS for Address Resolution
RFC2461 7.2.4 RECOMMENDED
Applies to: Router, Host
Context:

Requirement:
When constructing a Neighbor advertisement message which is a response to a valid Neighbor Solicitation message and in which the Target Address field is set to a unicast address for which it is providing proxy service, an IPv6 node SHOULD set the Override Flag (O-Flag) to zero (0) in the advertisement.
Specification Text:
If the Target Address is either an anycast address or **a unicast address for which the node is providing proxy service,** or the Target Link-Layer Address option is not included, **the Override flag SHOULD be set to zero.** Otherwise, the Override flag SHOULD be set to one. Proper setting of the Override flag ensures that nodes give preference to non-proxy advertisements, even when received after proxy advertisements, and also ensures that the first advertisement for an anycast address "wins".

RQ_000_8449 Process NS for Address Resolution
RFC2461 7.2.4 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor advertisement message which is a response to a valid Neighbor Solicitation message and in which the Target Link-Layer Address option is omitted, an IPv6 node SHOULD set the Override Flag (O-Flag) to zero (0) in the advertisement.
Specification Text:
If the Target Address is either an anycast address or a unicast address for which the node is providing proxy service, or **the Target Link-Layer Address option is not included, the Override flag SHOULD be set to zero.** Otherwise, the Override flag SHOULD be set to one. Proper setting of the Override flag ensures that nodes give preference to non-proxy advertisements, even when received after proxy advertisements, and also ensures that the first advertisement for an anycast address "wins".

RQ_000_8450 Process NS for Address Resolution
RFC2461 7.2.4 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When constructing a Neighbor advertisement message which is a response to a valid Neighbor Solicitation message and in which a Target Link-Layer Address option is included and the Target Address field is set to neither an anycast address nor a unicast address for which it is providing proxy service, an IPv6 node SHOULD set the Override Flag (O-Flag) to one (1) in the advertisement.
Specification Text:
If the Target Address is either an anycast address or a unicast address for which the node is providing proxy service, or the Target Link-Layer Address option is not included, the Override flag SHOULD be set to zero. **Otherwise, the Override flag SHOULD be set to one.** Proper setting of the Override flag ensures that nodes give preference to non-proxy advertisements, even when received after proxy advertisements, and also ensures that the first advertisement for an anycast address "wins".

RQ_000_8451 Process NS for Address Resolution
RFC2461 7.2.4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a valid Neighbor Solicitation message with the Source Address field in the containing IPv6 Packet header set to the Unspecified Address (0::0)
Requirement:
The IPv6 node MUST send a Neighbor Advertisement message from the receiving interface with the Solicited Flag (S-Flag) set to zero (0) and the Destination Address field in the containing IPv6 Packet header set to the link-local All-Nodes multicast address (FF02:0:0:0:0:0:0:1).
Specification Text:
If the source of the solicitation is the unspecified address, the node MUST set the Solicited flag to zero and multicast the advertisement to the all-nodes address. Otherwise, the node MUST set the Solicited flag to one and unicast the advertisement to the Source Address of the solicitation.

RQ_000_8452 Process NS for Address Resolution
RFC2461 7.2.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a valid Neighbor Solicitation message with the Source Address field in the containing IPv6 Packet header set to an address other than the Unspecified Address (0::0)
Requirement:
The IPv6 node MUST send a Neighbor Advertisement message from the receiving interface with the Solicited Flag (S-Flag) set to one (1) and the Destination Address field in the containing IPv6 Packet header set to the unicast address taken from the Source Address field of the received Neighbor Solicitation.
Specification Text:
If the source of the solicitation is the unspecified address, the node MUST set the Solicited flag to zero and multicast the advertisement to the all-nodes address. **Otherwise, the node MUST set the Solicited flag to one and unicast the advertisement to the Source Address of the solicitation.**

RQ_000_8453 Process Anycast NS
RFC2461 7.2.4 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node receives a valid Neighbor Solicitation message in which the Target Address field is set to an Anycast address.
Requirement:
The IPv6 node SHOULD send the Neighbor advertisement response aft a random delay of between 0 and 1 seconds.
Specification Text:
If the Target Address is an anycast address the sender SHOULD delay sending a response for a random time between 0 and MAX_ANYCAST_DELAY_TIME seconds.

RQ_000_8454 Generate NS for Address Resolution
RFC2461 7.2.4 MANDATORY
Applies to: Host, Router
Context:
An IPV6 node receives a valid Neighbor Solicitation that does not include a Source Link-Layer Address option and the node has no link-layer address associated with the address set in the Source Address field of the containing IPv6 Packet header.
Requirement:
The IPv6 node MUST invoke and complete Neighbor Discovery procedures before sending a Neighbor Advertisement response to the solicitation.
Specification Text:
Because unicast Neighbor Solicitations are not required to include a Source Link-Layer Address, it is possible that **a node sending a solicited Neighbor Advertisement does not have a corresponding link-layer address for its neighbor in its Neighbor Cache. In such situations, a node will first have to use Neighbor Discovery to determine the link-layer address of its neighbor (i.e., send out a multicast Neighbor Solicitation).**

RQ_000_8455 Process Neighbor Advertisement
RFC2461 7.2.5 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
An IPv6 node SHOULD silently discard a received Neighbor advertisement in which the Target Address field is set to an address which is unknown to the node.
Specification Text:
When a valid Neighbor Advertisement is received (either solicited or unsolicited), the Neighbor Cache is searched for the target's entry. If no entry exists, the advertisement SHOULD be silently discarded. There is no need to create an entry if none exists, since the recipient has apparently not initiated any communication with the target.

RQ_000_8456 Address Resolution Behavior
RFC2461 7.2.5 RECOMMENDED
Applies to: Router, Host
Context:

Requirement:
An IPv6 node SHOULD silently discard a Neighbor Advertisement message received as a response to a multicast Neighbor Solicitation message if the link-layer has addresses assigned to it but the Neighbor Advertisement does not contain a valid Target Link-Layer Address option.
Specification Text:
If the target's Neighbor Cache entry is in the INCOMPLETE state when the advertisement is received, one of two things happens. If the link layer has addresses and no Target Link-Layer address option is included, the receiving node SHOULD silently discard the received advertisement. Otherwise, the receiving node performs the following steps:

- It records the link-layer address in the Neighbor Cache entry.
- If the advertisement's Solicited flag is set, the state of the entry is set to REACHABLE, otherwise it is set to STALE.
- It sets the IsRouter flag in the cache entry based on the Router flag in the received advertisement.
- It sends any packets queued for the neighbor awaiting address resolution.

Note that the Override flag is ignored if the entry is in the INCOMPLETE state.

RQ_000_8457 Address Resolution Behavior
RFC2461 7.2.5 MANDATORY
Applies to: Host, Router
Context:
In response to a multicast Neighbor Solicitation message, an IPv6 node receives a Neighbor Advertisement message which includes a valid Target Link-Layer Address option and has both the Router Flag field and the Solicited Flag field set to one (1).
Requirement:
The IPv6 node MUST internally associate the Target Link-Layer Address with the address contained in the Source Address field of the received IPv6 Packet header containing the Neighbor advertisement, categorize the neighboring node as a router and reachable and send any packets which have been delayed during the Address Resolution process.
Specification Text:
If the target's Neighbor Cache entry is in the INCOMPLETE state when the advertisement is received, one of two things happens. If the link layer has addresses and no Target Link-Layer address option is included, the receiving node SHOULD silently discard the received advertisement. **Otherwise, the receiving node performs the following steps:**

- **It records the link-layer address in the Neighbor Cache entry.**
- **If the advertisement's Solicited flag is set, the state of the entry is set to REACHABLE,** otherwise it is set to STALE.
- **It sets the IsRouter flag in the cache entry based on the Router flag in the received advertisement.**
- **It sends any packets queued for the neighbor awaiting address resolution.**

Note that the Override flag is ignored if the entry is in the INCOMPLETE state.

RQ_000_8458 Address Resolution Behavior

RFC2461 7.2.5 MANDATORY

Applies to: Host, Router

Context:

In response to a multicast Neighbor Solicitation message, an IPv6 node receives a Neighbor Advertisement message which includes a valid Target Link-Layer Address option and has the Router Flag field set to one (1) and the Solicited Flag field set to zero (0).

Requirement:

The IPv6 node MUST internally associate the Target Link-Layer Address with the address contained in the Source Address field of the received IPv6 Packet header containing the Neighbor advertisement, categorize the neighboring node as a router and unreachable and send any packets which have been delayed during the Address Resolution process.

Specification Text:

If the target's Neighbor Cache entry is in the INCOMPLETE state when the advertisement is received, one of two things happens. If the link layer has addresses and no Target Link-Layer address option is included, the receiving node SHOULD silently discard the received advertisement. **Otherwise, the receiving node performs the following steps:**

- **It records the link-layer address in the Neighbor Cache entry.**
- If the advertisement's Solicited flag is set, the state of the entry is set to REACHABLE, **otherwise it is set to STALE.**
- **It sets the IsRouter flag in the cache entry based on the Router flag in the received advertisement.**
- **It sends any packets queued for the neighbor awaiting address resolution.**

Note that the Override flag is ignored if the entry is in the INCOMPLETE state.

RQ_000_8459 Address Resolution Behavior

RFC2461 7.2.5 MANDATORY

Applies to: Host, Router

Context:

In response to a multicast Neighbor Solicitation message, an IPv6 node receives a Neighbor Advertisement message which includes a valid Target Link-Layer Address option and has the Router Flag field set to zero (0) and the Solicited Flag field set to one (1).

Requirement:

The IPv6 node MUST internally associate the Target Link-Layer Address with the address contained in the Source Address field of the received IPv6 Packet header containing the Neighbor advertisement, categorize the neighboring node as a host and reachable and send any packets which have been delayed during the Address Resolution process.

Specification Text:

If the target's Neighbor Cache entry is in the INCOMPLETE state when the advertisement is received, one of two things happens. If the link layer has addresses and no Target Link-Layer address option is included, the receiving node SHOULD silently discard the received advertisement. **Otherwise, the receiving node performs the following steps:**

- **It records the link-layer address in the Neighbor Cache entry.**
- **If the advertisement's Solicited flag is set, the state of the entry is set to REACHABLE,** otherwise it is set to STALE.
- **It sets the IsRouter flag in the cache entry based on the Router flag in the received advertisement.**
- **It sends any packets queued for the neighbor awaiting address resolution.**

Note that the Override flag is ignored if the entry is in the INCOMPLETE state.

RQ_000_8460 Address Resolution Behavior

RFC2461 7.2.5 MANDATORY

Applies to: Host, Router

Context:

In response to a multicast Neighbor Solicitation message, an IPv6 node receives a Neighbor Advertisement message which includes a valid Target Link-Layer Address option and has both the Router Flag field and the Solicited Flag field set to zero (0).

Requirement:

The IPv6 node MUST internally associate the Target Link-Layer Address with the address contained in the Source Address field of the received IPv6 Packet header containing the Neighbor advertisement, categorize the neighboring node as a host and unreachable and send any packets which have been delayed during the Address Resolution process.

Specification Text:

If the target's Neighbor Cache entry is in the INCOMPLETE state when the advertisement is received, one of two things happens. If the link layer has addresses and no Target Link-Layer address option is included, the receiving node SHOULD silently discard the received advertisement. **Otherwise, the receiving node performs the following steps:**

- **It records the link-layer address in the Neighbor Cache entry.**
- If the advertisement's Solicited flag is set, the state of the entry is set to REACHABLE, **otherwise it is set to STALE.**
- **It sets the IsRouter flag in the cache entry based on the Router flag in the received advertisement.**
- **It sends any packets queued for the neighbor awaiting address resolution.**

Note that the Override flag is ignored if the entry is in the INCOMPLETE state.

RQ_000_8461 Neighbor Unreachability Detection

RFC2461 7.2.5 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a Neighbor Advertisement message with the Override Flag field set to zero (0) and the Target Link-Layer Address option containing an address which is not the same as the link-layer address that the node has previously associated with the neighboring node which it has categorized as reachable.

Requirement:

The IPv6 node MUST re-categorize the neighboring node as unreachable and MUST NOT attempt to verify the reachability of the neighbor until there is an IPv6 packet to be sent to it.

Specification Text:

If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. **If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way;** otherwise, the received advertisement should be ignored and MUST NOT update the cache. If the Override flag is set, both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).
- If the Solicited flag is set, the state of the entry MUST be set to REACHABLE. If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged. An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation. Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet. There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.

- The IsRouter flag in the cache entry MUST be set based on the
  Router flag in the received advertisement. In those cases where
  the IsRouter flag changes from TRUE to FALSE as a result of this
  update, the node MUST remove that router from the Default Router
  List and update the Destination Cache entries for all destinations
  using that neighbor as a router as specified in Section 7.3.3.
  This is needed to detect when a node that is used as a router
  stops forwarding packets due to being configured as a host.

RQ_000_8462 Address Resolution Behavior
RFC2461 7.2.5 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a Neighbor Advertisement message with the Override Flag field set to zero (0) and the Target Link-Layer Address option containing an address which is not the same as the link-layer address that the node has previously associated with the source neighboring node which it has categorized as unreachable.
Requirement:
The IPv6 node MUST ignore the received Neighbor Advertisement
Specification Text:
If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. **If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place:** if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; **otherwise, the received advertisement should be ignored and MUST NOT update the cache.** If the Override flag is set, both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option
  MUST be inserted in the cache (if one is supplied and is different
  than the already recorded address).
- If the Solicited flag is set, the state of the entry MUST be set
  to REACHABLE. If the Solicited flag is zero and the link-layer
  address was updated with a different address the state MUST be set
  to STALE. Otherwise, the entry's state remains unchanged.
  An advertisement's Solicited flag should only be set if the
  advertisement is a response to a Neighbor Solicitation. Because
  Neighbor Unreachability Detection Solicitations are sent to the
  cached link-layer address, receipt of a solicited advertisement
  indicates that the forward path is working. Receipt of an
  unsolicited advertisement, however, suggests that a neighbor has
  urgent information to announce (e.g., a changed link-layer
  address). If the urgent information indicates a change from what
  a node is currently using, the node should verify the reachability
  of the (new) path when it sends the next packet. There is no need
  to update the state for unsolicited advertisements that do not
  change the contents of the cache.
- The IsRouter flag in the cache entry MUST be set based on the
  Router flag in the received advertisement. In those cases where
  the IsRouter flag changes from TRUE to FALSE as a result of this
  update, the node MUST remove that router from the Default Router
  List and update the Destination Cache entries for all destinations
  using that neighbor as a router as specified in Section 7.3.3.
  This is needed to detect when a node that is used as a router
  stops forwarding packets due to being configured as a host.

RQ_000_8463 Address Resolution Behavior
RFC2461 7.2.5 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a Neighbor Advertisement message with the Override Flag field set to one (1) and the Target Link-Layer Address option containing an address which is not the same as the link-layer address that the node has previously associated with the source neighboring node which it has categorized as unreachable.
Requirement:
The IPv6 node MUST make an internal association between the neighboring node's IP address and the link-layer address received in the Target Link-Layer Address option, replacing the existing association.

Specification Text:

If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; otherwise, the received advertisement should be ignored and MUST NOT update the cache. **If the Override flag is set**, both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- **The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).**
- If the Solicited flag is set, the state of the entry MUST be set to REACHABLE. If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged. An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation. Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet. There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.
- The IsRouter flag in the cache entry MUST be set based on the Router flag in the received advertisement. In those cases where the IsRouter flag changes from TRUE to FALSE as a result of this update, the node MUST remove that router from the Default Router List and update the Destination Cache entries for all destinations using that neighbor as a router as specified in Section 7.3.3. This is needed to detect when a node that is used as a router stops forwarding packets due to being configured as a host.

RQ_000_8464 Determine Neighbor Reachability

RFC2461 7.2.5 MANDATORY

Applies to: Router, Host

Context:

An IPv6 node receives a Neighbor Advertisement message with the Override Flag field set to one (1), the Solicited Flag set to one (1) and the Target Link-Layer Address option containing an address which is not the same as the link-layer address that the node has previously associated with the source neighboring node which it has categorized as unreachable.

Requirement:

The IPv6 node MUST re-categorize the neighboring node as reachable.

Specification Text:

If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; otherwise, the received advertisement should be ignored and MUST NOT update the cache. **If the Override flag is set,** both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).
- **If the Solicited flag is set, the state of the entry MUST be set to REACHABLE.** If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged.

An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation. Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet. There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.

- The IsRouter flag in the cache entry MUST be set based on the Router flag in the received advertisement. In those cases where the IsRouter flag changes from TRUE to FALSE as a result of this update, the node MUST remove that router from the Default Router List and update the Destination Cache entries for all destinations using that neighbor as a router as specified in Section 7.3.3. This is needed to detect when a node that is used as a router stops forwarding packets due to being configured as a host.

RQ_000_8465 Neighbor Unreachability Detection

RFC2461 7.2.5 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a Neighbor Advertisement message with the Override Flag field set to one (1), the Solicited Flag field set to zero (0) and the Target Link-Layer Address option containing an address which is not the same as the link-layer address that the node has previously associated with the source neighboring node which it has categorized as unreachable.

Requirement:

The IPv6 node MUST re-categorize the neighboring node as unreachable and make an internal association between the neighboring node's IP address and the link-layer address received in the Target Link-Layer Address option, replacing the existing association

Specification Text:

If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; otherwise, the received advertisement should be ignored and MUST NOT update the cache. **If the Override flag is set,** both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).
- If the Solicited flag is set, the state of the entry MUST be set to REACHABLE**. If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged.**
  An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation. Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet. There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.
- The IsRouter flag in the cache entry MUST be set based on the Router flag in the received advertisement. In those cases where the IsRouter flag changes from TRUE to FALSE as a result of this update, the node MUST remove that router from the Default Router List and update the Destination Cache entries for all destinations using that neighbor as a router as specified in Section 7.3.3. This is needed to detect when a node that is used as a router stops forwarding packets due to being configured as a host.

RQ_000_8466 Form Neighbor Advertisement Header
RFC2461 7.2.5 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When constructing a Neighbor Advertisement message as a response to a received Neighbor Solicitation message, an IPv6 node MUST set the Solicited Flag field to the value one (1)
Specification Text:
If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; otherwise, the received advertisement should be ignored and MUST NOT update the cache. If the Override flag is set, both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).
- If the Solicited flag is set, the state of the entry MUST be set to REACHABLE. If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged. **An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation.** Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet. There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.
- The IsRouter flag in the cache entry MUST be set based on the Router flag in the received advertisement. In those cases where the IsRouter flag changes from TRUE to FALSE as a result of this update, the node MUST remove that router from the Default Router List and update the Destination Cache entries for all destinations using that neighbor as a router as specified in Section 7.3.3. This is needed to detect when a node that is used as a router stops forwarding packets due to being configured as a host.

RQ_000_8467 Start Neighbor Reachability Determination
RFC2461 7.2.5 RECOMMENDED
Applies to: Router, Host
Context:

Requirement:
If an IPv6 node receives an unsolicited Neighbor Advertisement message containing information which is not identical to the information it has previously registered for the advertising node, it SHOULD initiate Neighbor Unreachability procedures to verify the reachability of the new path prior to sending any other IPv6 packets to that node.
Specification Text:
If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; otherwise, the received advertisement should be ignored and MUST NOT update the cache. If the Override flag is set, both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).

- If the Solicited flag is set, the state of the entry MUST be set to REACHABLE. If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged. An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation. Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. **Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet.** There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.
- The IsRouter flag in the cache entry MUST be set based on the Router flag in the received advertisement. In those cases where the IsRouter flag changes from TRUE to FALSE as a result of this update, the node MUST remove that router from the Default Router List and update the Destination Cache entries for all destinations using that neighbor as a router as specified in Section 7.3.3. This is needed to detect when a node that is used as a router stops forwarding packets due to being configured as a host.

RQ_000_8468 Process Neighbor Advertisement

RFC2461 7.2.5 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Advertisement message in which the Router Flag field is set to zero (0)

Requirement:

The IPv6 node MUST categorize the advertising node as a host.

Specification Text:

If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; otherwise, the received advertisement should be ignored and MUST NOT update the cache. If the Override flag is set, both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).
- If the Solicited flag is set, the state of the entry MUST be set to REACHABLE. If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged. An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation. Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet. There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.
- **The IsRouter flag in the cache entry MUST be set based on the Router flag in the received advertisement.** In those cases where the IsRouter flag changes from TRUE to FALSE as a result of this update, the node MUST remove that router from the Default Router List and update the Destination Cache entries for all destinations using that neighbor as a router as specified in Section 7.3.3. This is needed to detect when a node that is used as a router stops forwarding packets due to being configured as a host.

RQ_000_8469 Process Neighbor Advertisement

RFC2461 7.2.5 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Advertisement containing a Router Flag field set to zero (0) from a node that it has previously categorized as a router.

Requirement:

The IPv6 node must no longer use the advertising router as a default router for all the destination prefixes that it has previously associated with that router.

Specification Text:

If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; otherwise, the received advertisement should be ignored and MUST NOT update the cache. If the Override flag is set, both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).
- If the Solicited flag is set, the state of the entry MUST be set to REACHABLE. If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged. An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation. Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet. There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.
- The IsRouter flag in the cache entry MUST be set based on the Router flag in the received advertisement. **In those cases where the IsRouter flag changes from TRUE to FALSE as a result of this update, the node MUST remove that router from the Default Router List and update the Destination Cache entries for all destinations using that neighbor as a router** as specified in Section 7.3.3. This is needed to detect when a node that is used as a router stops forwarding packets due to being configured as a host.

RQ_000_8470 Neighbor Unreachability Detection

RFC2461 7.2.5 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a Neighbor Advertisement message with the Override Flag field set to zero (0) and the Target Link-Layer Address option containing an address which is not the same as the link-layer address that the node has previously associated with the source neighboring node which it has categorized as unreachable.

Requirement:

The IPv6 node MUST invoke Neighbor Unreachability Detection for the sending node.

Specification Text:

The above rules ensure that the cache is updated either when the Neighbor Advertisement takes precedence (i.e., the Override flag is set) or when the Neighbor Advertisement refers to the same link-layer address that is currently recorded in the cache. **If none of the above apply, the advertisement prompts future Neighbor Unreachability Detection (if it is not already in progress) by changing the state in the cache entry.**

RQ_000_8471 Generate Unsolicited Neighbor Advertisement
RFC2461 7.2.6 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MAY send up to 3 unsolicited Neighbor Advertisements in a single sequence from a particular IP Address to the link-local all-nodes multicast address (FF02:0:0:0:0:0:0:2).
Specification Text:
In some cases a node may be able to determine that its link-layer address has changed (e.g., hot-swap of an interface card) and may wish to inform its neighbors of the new link-layer address quickly. In such cases a node MAY send up to MAX_NEIGHBOR_ADVERTISEMENT unsolicited Neighbor Advertisement messages to the all-nodes multicast address. These advertisements MUST be separated by at least RetransTimer seconds.

RQ_000_8472 Generate Unsolicited Neighbor Advertisement
RFC2461 7.2.6 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST separate successive unsolicited Neighbor advertisement messages sent to a particular interface by at least 1 second.
Specification Text:
In some cases a node may be able to determine that its link-layer address has changed (e.g., hot-swap of an interface card) and may wish to inform its neighbors of the new link-layer address quickly. In such cases a node MAY send up to MAX_NEIGHBOR_ADVERTISEMENT unsolicited Neighbor Advertisement messages to the all-nodes multicast address. **These advertisements MUST be separated by at least RetransTimer seconds.**

RQ_000_8473 Form Unsolicited NA Header
RFC2461 7.2.6 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing an unsolicited Neighbor advertisement message to be sent from a particular interface, and IPv6 router MUST set the fields in the message as follows:

NA Field	Value
Target Address	An IP address of the interface
Target Link-Layer Address option	Link-layer address of the interface
Solicited Flag	zero (0)
Router Flag	one (1)

Specification Text:
The Target Address field in the unsolicited advertisement is set to an IP address of the interface, and the Target Link-Layer Address option is filled with the new link-layer address. The Solicited flag MUST be set to zero, in order to avoid confusing the Neighbor Unreachability Detection algorithm. **If the node is a router, it MUST set the Router flag to one;** otherwise it MUST set it to zero. The Override flag MAY be set to either zero or one. In either case, neighboring nodes will immediately change the state of their Neighbor Cache entries for the Target Address to STALE, prompting them to verify the path for reachability. If the Override flag is set to one, neighboring nodes will install the new link-layer address in their caches. Otherwise, they will ignore the new link-layer address, choosing instead to probe the cached address.

RQ_000_8474 Form Unsolicited NA Header
RFC2461 7.2.6 MANDATORY
Applies to: Host
Context:

Requirement:
When constructing an unsolicited Neighbor advertisement message to be sent from a particular interface, and IPv6 host MUST set the fields in the message as follows:

NA Field	Value
Target Address	An IP address of the interface
Target Link-Layer Address option	Link-layer address of the interface
Solicited Flag	zero (0)
Router Flag	zero (0)

Specification Text:
The Target Address field in the unsolicited advertisement is set to an IP address of the interface, and the Target Link-Layer Address option is filled with the new link-layer address. The Solicited flag MUST be set to zero, in order to avoid confusing the Neighbor Unreachability Detection algorithm. **If the node is a router, it MUST set the Router flag to one; otherwise it MUST set it to zero.** The Override flag MAY be set to either zero or one. In either case, neighboring nodes will immediately change the state of their Neighbor Cache entries for the Target Address to STALE, prompting them to verify the path for reachability. If the Override flag is set to one, neighboring nodes will install the new link-layer address in their caches. Otherwise, they will ignore the new link-layer address, choosing instead to probe the cached address.

RQ_000_8475 Start Neighbor Reachability Determination
RFC2461 7.2.6 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an unsolicited Neighbor Advertisement with a new link-layer address from one of its known neighbors.
Requirement:
The IPv6 node MUST invoke Neighbor Unreachability procedures to verify the reachability of the path associated with the new link-layer address.
Specification Text:
The Target Address field in the unsolicited advertisement is set to an IP address of the interface, and the Target Link-Layer Address option is filled with the new link-layer address. The Solicited flag MUST be set to zero, in order to avoid confusing the Neighbor Unreachability Detection algorithm. If the node is a router, it MUST set the Router flag to one; otherwise it MUST set it to zero. The Override flag MAY be set to either zero or one. **In either case, neighboring nodes will immediately change the state of their Neighbor Cache entries for the Target Address to STALE, prompting them to verify the path for reachability.** If the Override flag is set to one, neighboring nodes will install the new link-layer address in their caches. Otherwise, they will ignore the new link-layer address, choosing instead to probe the cached address.

RQ_000_8476 Generate Unsolicited Neighbor Advertisement
RFC2461 7.2.6 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MAY send separate unsolicited Neighbor advertisement messages from a particular interface for each IP address associated with the interface.
Specification Text:
A node that has multiple IP addresses assigned to an interface MAY multicast a separate Neighbor Advertisement for each address. In such a case the node SHOULD introduce a small delay between the sending of each advertisement to reduce the probability of the advertisements being lost due to congestion.

RQ_000_8478 Generate Proxy NA
RFC2461 7.2.6 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node providing proxy service MAY send up to 3 unsolicited Neighbor Advertisement messages to the link-local all-nodes multicast address (FF02:0:0:0:0:0:0:2) in the event that its link-layer address changes.
Specification Text:
A proxy MAY multicast Neighbor Advertisements when its link-layer address changes or when it is configured (by system management or other mechanisms) to proxy for an address. If there are multiple nodes that are providing proxy services for the same set of addresses the proxies SHOULD provide a mechanism that prevents multiple proxies from multicasting advertisements for any one address, in order to reduce the risk of excessive multicast traffic.

RQ_000_8479 Generate Proxy NA
RFC2461 7.2.6 OPTIONAL
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MAY send up to 3 unsolicited Neighbor Advertisement messages to the link-local all-nodes multicast address (FF02:0:0:0:0:0:0:2) in the event that the node is reconfigured by system management procedures to provide proxy service for an address.
Specification Text:
A proxy MAY multicast Neighbor Advertisements when its link-layer address changes or **when it is configured (by system management or other mechanisms) to proxy for an address.** If there are multiple nodes that are providing proxy services for the same set of addresses the proxies SHOULD provide a mechanism that prevents multiple proxies from multicasting advertisements for any one address, in order to reduce the risk of excessive multicast traffic.

RQ_000_8481 Generate Unsolicited Anycast NA
RFC2461 7.2.6 OPTIONAL
Applies to: Router, Host
Context:

Requirement:
An IPv6 node having an anycast address MAY send up to 3 unsolicited Neighbor Advertisements in a single sequence from the anycast address to the link-local all-nodes multicast address (FF02:0:0:0:0:0:0:2).
Specification Text:
Also, **a node belonging to an anycast address MAY multicast unsolicited Neighbor Advertisements for the anycast address when the node's link-layer address changes.**

RQ_000_8482 Address Resolution
RFC2461 7.2.7 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node use the same procedures for performing Address Resolution on an anycast address as is used on a unicast address.
Specification Text:
From the perspective of Neighbor Discovery, anycast addresses are treated just like unicast addresses in most cases. Because an anycast address is syntactically the same as a unicast address, **nodes performing address resolution or Neighbor Unreachability Detection on an anycast address treat it as if it were a unicast address. No special processing takes place.**

RQ_000_8483 Neighbor Unreachability Detection
RFC2461 7.2.7 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node use the same procedures for performing Neighbor Unreachability Detection on an anycast address as is used on a unicast address.
Specification Text:
From the perspective of Neighbor Discovery, anycast addresses are treated just like unicast addresses in most cases. Because an anycast address is syntactically the same as a unicast address, **nodes performing address resolution or Neighbor Unreachability Detection on an anycast address treat it as if it were a unicast address. No special processing takes place.**

RQ_000_8484 Process Anycast NS
RFC2461 7.2.7 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node has received a valid Neighbor Solicitation message for one of its anycast address.
Requirement:
The IPv6 node should delay a random time between 0 and 1 second before sending a Neighbor Advertisement message with the Override Flag field set to zero (0).
Specification Text:
Nodes that have an anycast address assigned to an interface treat them exactly the same as if they were unicast addresses with two exceptions. First, Neighbor Advertisements sent in response to a Neighbor Solicitation SHOULD be delayed by a random time between 0 and MAX_ANYCAST_DELAY_TIME to reduce the probability of network congestion. Second, the Override flag in Neighbor Advertisements SHOULD be set to 0, so that when multiple advertisements are received, the first received advertisement is used rather than the most recently received advertisement.

RQ_000_8485 Generate Proxy NA
RFC2461 7.2.8 OPTIONAL
Applies to: Router
Context:

Requirement:
In order to indicate that it is providing a proxy service to another node, an IPv6 router MAY transmit unsolicited Neighbor advertisements in which the Source Address field of the containing IPv6 Packet header is set to the router's own IP address, the Target Address field is set to the IP address of the other node and the Target Link-Layer Address option is set to the link-layer address of the router.
Specification Text:
Under limited circumstances, **a router MAY proxy for one or more other nodes, that is, through Neighbor Advertisements indicate that it is willing to accept packets not explicitly addressed to itself.** For example, a router might accept packets on behalf of a mobile node that has moved off-link. The mechanisms used by proxy are identical to the mechanisms used with anycast addresses.

RQ_000_8486 Generate Proxy NA
RFC2461 7.2.8 MANDATORY
Applies to: Router
Context:
An IPv6 router receives a Neighbor Solicitation sent to a solicited-node multicast address that corresponds to an IP address assigned to a node for which the router is providing proxy service.
Requirement:
The IPv6 node should delay a random time between 0 and 1 second before sending a Neighbor Advertisement message with the Override Flag field set to zero (0) to the soliciting node.
Specification Text:
Under limited circumstances, a router MAY proxy for one or more other nodes, that is, through Neighbor Advertisements indicate that it is willing to accept packets not explicitly addressed to itself. For example, a router might accept packets on behalf of a mobile node that has moved off-link. **The mechanisms used by proxy are identical to the mechanisms used with anycast addresses.**

A proxy MUST join the solicited-node multicast address(es) that correspond to the IP address(es) assigned to the node for which it is proxying.

RQ_000_8487 Address Use
RFC2461 7.2.8 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPvb6 router that is providing proxy service to another node MUST accept and process packets in which the Source Address field of the header contains a solicited-node multicast address that corresponds to an IP address assigned to the other node (FF02:0:0:0:0:FFxx:xxxx).
Specification Text:
A proxy MUST join the solicited-node multicast address(es) that correspond to the IP address(es) assigned to the node for which it is proxying.

RQ_000_8488 Form Neighbor Advertisement Header
RFC2461 7.2.8 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Neighbor advertisement as a response to a Neighbor solicitation received on behalf of another node for which it is providing proxy service, an IPv6 router MUST set the Override Flag field to zero (0).
Specification Text:
All solicited proxy Neighbor Advertisement messages MUST have the Override flag set to zero. This ensures that if the node itself is present on the link its Neighbor Advertisement (with the Override flag set to one) will take precedence of any advertisement received from a proxy. A proxy MAY send unsolicited advertisements with the Override flag set to one as specified in Section 7.2.6, but doing so may cause the proxy advertisement to override a valid entry created by the node itself.

RQ_000_8489 Generate Proxy NA
RFC2461 7.2.8 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
When constructing an unsolicited Neighbor advertisement to be sent on behalf of another node for which it is providing proxy service, an IPv6 router MAY set the Override Flag field to zero (0).
Specification Text:
All solicited proxy Neighbor Advertisement messages MUST have the Override flag set to zero. This ensures that if the node itself is present on the link its Neighbor Advertisement (with the Override flag set to one) will take precedence of any advertisement received from a proxy. **A proxy MAY send unsolicited advertisements with the Override flag set to one as specified in Section 7.2.6, but doing so may cause the proxy advertisement to override a valid entry created by the node itself.**

RQ_000_8490 Generate Neighbor Advertisement
RFC2461 7.2.8 RECOMMENDED
Applies to: Router
Context:

Requirement:
When an IPv6 router receives Neighbor Solicitation on behalf of another node for which it is providing proxy service, the router SHOULD delay sending the Neighbor Advertisement response to the solicitation by a random time between 0 and 1 second.
Specification Text:
Finally, **when sending a proxy advertisement in response to a Neighbor Solicitation, the sender should delay its response by a random time between 0 and MAX_ANYCAST_DELAY_TIME seconds.**

RQ_000_8491 Neighbor Unreachability Detection
RFC2461 7.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST invoke next-hop determination if it detects that a previously reachable neighboring node has become unreachable.
Specification Text:
When a path to a neighbor appears to be failing, the specific recovery procedure depends on how the neighbor is being used. If the neighbor is the ultimate destination, for example, address resolution should be performed again. If the neighbor is a router, however, attempting to switch to another router would be appropriate. **The specific recovery that takes place is covered under next-hop determination; Neighbor Unreachability Detection signals the need for next-hop determination by deleting a Neighbor Cache entry.**

RQ_000_8492 Neighbor Unreachability Detection
RFC2461 7.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ONLY perform Neighbor Unreachability Detection for neighboring nodes to which unicast packets are sent.
Specification Text:
Neighbor Unreachability Detection is performed only for neighbors to which unicast packets are sent; it is not used when sending to multicast addresses.

RQ_000_8494 Determine Neighbor Reachability
RFC2461 7.3.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST categorize a neighbor as reachable if it receives a valid Neighbor Advertisement message from the node as a response to its own outgoing Neighbor Solicitation.
Specification Text:
A neighbor is considered reachable if the node has recently received a confirmation that packets sent recently to the neighbor were received by its IP layer. Positive confirmation can be gathered in two ways: hints from upper layer protocols that indicate a connection is making "forward progress", or **receipt of a Neighbor Advertisement message that is a response to a Neighbor Solicitation message.**

RQ_000_8499 Neighbor Reachability Probing
RFC2461 7.3.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
If an IPv6 node is unable to determine the reachability of neighboring node by any other means, it MUST send a Neighbor Solicitation message with the neighboring node's IP address set in the Target Address field and in the Destination Address field of the containing IPv6 Packet header.
Specification Text:
In some cases (e.g., UDP-based protocols and routers forwarding packets to hosts) such reachability information may not be readily available from upper-layer protocols. **When no hints are available and a node is sending packets to a neighbor, the node actively probes the neighbor using unicast Neighbor Solicitation messages to verify that the forward path is still working.**

RQ_000_8500 Invalid Reachability Indications
RFC2461 7.3.1 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node sends a Neighbor Solicitation message to a neighboring node
Requirement:
The IPv6 node MUST NOT categorize the target node as reachable if it receives a Router advertisement in which the Solicited Flag field is set to zero from the target node.
Specification Text:
The receipt of a solicited Neighbor Advertisement serves as reachability confirmation, since advertisements with the Solicited flag set to one are sent only in response to a Neighbor Solicitation. **Receipt of other Neighbor Discovery messages such as Router Advertisements** and Neighbor Advertisement **with the Solicited flag set to zero MUST NOT be treated as a reachability confirmation.** Receipt of unsolicited messages only confirm the one-way path from the sender to the recipient node. In contrast, Neighbor Unreachability Detection requires that a node keep track of the reachability of the forward path to a neighbor from the its perspective, not the neighbor's perspective. Note that receipt of a solicited advertisement indicates that a path is working in both directions. The solicitation must have reached the neighbor, prompting it to generate an advertisement. Likewise, receipt of an advertisement indicates that the path from the sender to the recipient is working. However, the latter fact is known only to the recipient; the advertisement's sender has no direct way of knowing that the advertisement it sent actually reached a neighbor. From the perspective of Neighbor Unreachability Detection, only the reachability of the forward path is of interest.

RQ_000_8501 Invalid Reachability Indications
RFC2461 7.3.1 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node sends a Neighbor Solicitation message to a neighboring node
Requirement:
The IPv6 node MUST NOT categorize the target node as reachable if it receives a Neighbor advertisement in which the Solicited Flag field is set to zero from the target node.
Specification Text:
The receipt of a solicited Neighbor Advertisement serves as reachability confirmation, since advertisements with the Solicited flag set to one are sent only in response to a Neighbor Solicitation. **Receipt of** other Neighbor Discovery messages such as Router Advertisements and **Neighbor Advertisement with the Solicited flag set to zero MUST NOT be treated as a reachability confirmation.** Receipt of unsolicited messages only confirm the one-way path from the sender to the recipient node. In contrast, Neighbor Unreachability Detection requires that a node keep track of the reachability of the forward path to a neighbor from the its perspective, not the neighbor's perspective. Note that receipt of a solicited advertisement indicates that a path is working in both directions. The solicitation must have reached the neighbor, prompting it to generate an advertisement. Likewise, receipt of an advertisement indicates that the path from the sender to the recipient is working. However, the latter fact is known only to the recipient; the advertisement's sender has no direct way of knowing that the advertisement it sent actually reached a neighbor. From the perspective of Neighbor Unreachability Detection, only the reachability of the forward path is of interest.

RQ_000_8503 Neighbor Reachability Probing
RFC2461 7.3.2 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node has received no positive confirmation for over 35 seconds that a particular node is reachable.
Requirement:
The IPv6 node MUST send a Neighbor Solicitation message with the unreachable node's IP address set in the Target Address field and in the Destination Address field of the containing IPv6 Packet header.
Specification Text:
DELAY
More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly, and a packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a Neighbor Solicitation and change the state to PROBE.

RQ_000_8504 Neighbor Reachability Probing
RFC2461 7.3.2 "PROBE" MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST retransmit Neighbor Solicitation messages every 1 second until a Neighbor advertisement is received from the target node.
Specification Text:
PROBE
A reachability confirmation is actively sought by retransmitting Neighbor Solicitations every RetransTimer milliseconds until a reachability confirmation is received.

RQ_000_8505 Neighbor Unreachability Detection
RFC2461 7.3.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node is performing Neighbor Unreachability Detection procedures for a given path to a neighboring node.
Requirement:
The IPv6 node MUST continue to send packets not associated with Neighbor Unreachability Detection to the neighboring node's known link-layer address.
Specification Text:
Neighbor Unreachability Detection operates in parallel with the sending of packets to a neighbor. While reasserting a neighbor's reachability, a node continues sending packets to that neighbor using the cached link-layer address. If no traffic is sent to a neighbor, no probes are sent.

RQ_000_8506 Neighbor Unreachability Detection
RFC2461 7.3.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT send Neighbor Solicitations to neighboring nodes that are categorized as unreachable if there are other packets to be sent to the neighbor.
Specification Text:
Neighbor Unreachability Detection operates in parallel with the sending of packets to a neighbor. While reasserting a neighbor's reachability, a node continues sending packets to that neighbor using the cached link-layer address. **If no traffic is sent to a neighbor, no probes are sent.**

RQ_000_8507 Next Hop Determination
RFC2461 7.3.3 RECOMMENDED
Applies to: Router, Host
Context:

Requirement:
An IPv6 node SHOULD invoke next-hop determination procedures for a neighboring node if address resolution has failed for the path to that node.
Specification Text:
When a node needs to perform address resolution on a neighboring address, it creates an entry in the INCOMPLETE state and initiates address resolution as specified in Section 7.2. **If address resolution fails, the entry SHOULD be deleted, so that subsequent traffic to that neighbor invokes the next-hop determination procedure again. Invoking next-hop determination at this point insures that alternate default routers are tried.**

RQ_000_8509 Neighbor Reachability Probing
RFC2461 7.3.3 -6 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node has received no positive confirmation for over 35 seconds that a particular node is reachable.
Requirement:
The implementation retransmits MAX_UNICAST_SOLICIT Neighbor Solicitation messages every RetransTimer milliseconds.
Specification Text:
When ReachableTime milliseconds have passed since receipt of the last reachability confirmation for a neighbor, the Neighbor Cache entry's state changes from REACHABLE to STALE.

Note: An implementation may actually defer changing the state from REACHABLE to STALE until a packet is sent to the neighbor, i.e., there need not be an explicit timeout event associated with the expiration of ReachableTime.

The first time a node sends a packet to a neighbor whose entry is STALE, the sender changes the state to DELAY and a sets a timer to expire in DELAY_FIRST_PROBE_TIME seconds. If the entry is still in the DELAY state when the timer expires, the entry's state changes to PROBE. If reachability confirmation is received, the entry's state changes to REACHABLE.

Upon entering the PROBE state, a node sends a unicast Neighbor Solicitation message to the neighbor using the cached link-layer address. While in the PROBE state, a node retransmits Neighbor Solicitation messages every RetransTimer milliseconds until reachability confirmation is obtained. Probes are retransmitted even if no additional packets are sent to the neighbor. If no response is received after waiting RetransTimer milliseconds after sending the MAX_UNICAST_SOLICIT solicitations, retransmissions cease and the entry SHOULD be deleted. Subsequent traffic to that neighbor will recreate the entry and performs address resolution again.

RQ_000_8510 Neighbor Reachability Probing
RFC2461 7.3.3 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node has received no positive confirmation for over 35 seconds that a particular node is reachable and received no Neighbor Advertisement messages in response to its 3 Neighbor Solicitations to the node.
Requirement:
The IPv6 node SHOULD categorize the node as unreachable until subsequent traffic directed at the neighboring node causes address resolution procedures to be invoked.
Specification Text:
Upon entering the PROBE state, a node sends a unicast Neighbor Solicitation message to the neighbor using the cached link-layer address. While in the PROBE state, a node retransmits Neighbor Solicitation messages every RetransTimer milliseconds until reachability confirmation is obtained. Probes are retransmitted even if no additional packets are sent to the neighbor. **If no response is received after waiting RetransTimer milliseconds after sending the MAX_UNICAST_SOLICIT solicitations, retransmissions cease and the entry SHOULD be deleted. Subsequent traffic to that neighbor will recreate the entry and performs address resolution again.**

RQ_000_8511 Neighbor Reachability Probing
RFC2461 7.3.3 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT transmit Neighbor Solicitation messages to a single neighboring node more frequently than once every 1 second.
Specification Text:
Note that all Neighbor Solicitations are rate-limited on a per-neighbor basis. **A node MUST NOT send Neighbor Solicitations to the same neighbor more frequently than once every RetransTimer milliseconds.**

RQ_000_8512 Start Neighbor Reachability Determination
RFC2461 7.3.3 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a Router Solicitation message from a previously unknown neighboring node on a link.
Requirement:
The IPv6 node MUST register the sending node as a neighbor and MUST verify the neighbor's reachability when next required to send a packet to it.
Specification Text:
A Neighbor Cache entry enters the STALE state when created as a result of receiving packets other than solicited Neighbor Advertisements (i.e., Router Solicitations, Router Advertisements, Redirects, and Neighbor Solicitations). These packets contain the link-layer address of either the sender or, in the case of Redirect, the redirection target. However, receipt of these link-layer addresses does not confirm reachability of the forward-direction path to that node. Placing a newly created Neighbor Cache entry for which the link-layer address is known in the STALE state provides assurance that path failures are detected quickly. In addition, should a cached link-layer address be modified due to receiving one of the above messages the state SHOULD also be set to STALE to provide prompt verification that the path to the new link-layer address is working.

RQ_000_8513 Start Neighbor Reachability Determination
RFC2461 7.3.3 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a Router Advertisement message from a previously unknown neighboring node on a link.
Requirement:
The IPv6 node MUST register the sending node as a neighbor and MUST verify the neighbor's reachability when next required to send a packet to it.
Specification Text:
A Neighbor Cache entry enters the STALE state when created as a result of receiving packets other than solicited Neighbor Advertisements (i.e., Router Solicitations, **Router Advertisements,** Redirects, and Neighbor Solicitations). These packets contain the link-layer address of either the sender or, in the case of Redirect, the redirection target. However, receipt of these link-layer addresses does not confirm reachability of the forward-direction path to that node. Placing a newly created Neighbor Cache entry for which the link-layer address is known in the STALE state provides assurance that path failures are detected quickly. In addition, should a cached link-layer address be modified due to receiving one of the above messages the state SHOULD also be set to STALE to provide prompt verification that the path to the new link-layer address is working.

RQ_000_8514 Start Neighbor Reachability Determination
RFC2461 7.3.3 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a redirect message from a previously unknown neighboring node on a link.
Requirement:
The IPv6 node MUST register the sending node as a neighbor and MUST verify the neighbor's reachability when next required to send a packet to it.
Specification Text:
A Neighbor Cache entry enters the STALE state when created as a result of receiving packets other than solicited Neighbor Advertisements (i.e., Router Solicitations, Router Advertisements, **Redirects,** and Neighbor Solicitations). These packets contain the link-layer address of either the sender or, in the case of Redirect, the redirection target. However, receipt of these link-layer addresses does not confirm reachability of the forward-direction path to that node. Placing a newly created Neighbor Cache entry for which the link-layer address is known in the STALE state provides assurance that path failures are detected quickly. In addition, should a cached link-layer address be modified due to receiving one of the above messages the state SHOULD also be set to STALE to provide prompt verification that the path to the new link-layer address is working.

RQ_000_8515 Start Neighbor Reachability Determination
RFC2461 7.3.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a Neighbor Solicitation message from a previously unknown neighboring node on a link.
Requirement:
The IPv6 node MUST register the sending node as a neighbor and MUST verify the neighbor's reachability when next required to send a packet to it.
Specification Text:
A Neighbor Cache entry enters the STALE state when created as a result of receiving packets other than solicited Neighbor Advertisements (i.e., Router Solicitations, Router Advertisements, Redirects, and **Neighbor Solicitations**). These packets contain the link-layer address of either the sender or, in the case of Redirect, the redirection target. However, receipt of these link-layer addresses does not confirm reachability of the forward-direction path to that node. Placing a newly created Neighbor Cache entry for which the link-layer address is known in the STALE state provides assurance that path failures are detected quickly. In addition, should a cached link-layer address be modified due to receiving one of the above messages the state SHOULD also be set to STALE to provide prompt verification that the path to the new link-layer address is working.

RQ_000_8516 Start Neighbor Reachability Determination
RFC2461 7.3.3 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node receives a Router Solicitation that indicates a known neighbor's link-layer address has been modified.
Requirement:
The IPv6 node SHOULD update its internal information related to the neighboring node and SHOULD verify the neighbor's reachability when next required to send a packet to it.
Specification Text:
A Neighbor Cache entry enters the STALE state when created as a result of receiving packets other than solicited Neighbor Advertisements (i.e., Router Solicitations, Router Advertisements, Redirects, and Neighbor Solicitations). These packets contain the link-layer address of either the sender or, in the case of Redirect, the redirection target. However, receipt of these link-layer addresses does not confirm reachability of the forward-direction path to that node. Placing a newly created Neighbor Cache entry for which the link-layer address is known in the STALE state provides assurance that path failures are detected quickly. **In addition, should a cached link-layer address be modified due to receiving one of the above messages the state SHOULD also be set to STALE to provide prompt verification that the path to the new link-layer address is working.**

RQ_000_8517 Start Neighbor Reachability Determination
RFC2461 7.3.3 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node receives a Router Advertisement that indicates a known neighbor's link-layer address has been modified.
Requirement:
The IPv6 node SHOULD update its internal information related to the neighboring node and SHOULD verify the neighbor's reachability when next required to send a packet to it.
Specification Text:
A Neighbor Cache entry enters the STALE state when created as a result of receiving packets other than solicited Neighbor Advertisements (i.e., Router Solicitations, Router Advertisements, Redirects, and Neighbor Solicitations). These packets contain the link-layer address of either the sender or, in the case of Redirect, the redirection target. However, receipt of these link-layer addresses does not confirm reachability of the forward-direction path to that node. Placing a newly created Neighbor Cache entry for which the link-layer address is known in the STALE state provides assurance that path failures are detected quickly. **In addition, should a cached link-layer address be modified due to receiving one of the above messages the state SHOULD also be set to STALE to provide prompt verification that the path to the new link-layer address is working.**

RQ_000_8518 Start Neighbor Reachability Determination
RFC2461 7.3.3 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 node receives a Redirect that indicates a known neighbor's link-layer address has been modified.
Requirement:
The IPv6 node SHOULD update its internal information related to the neighboring node and SHOULD verify the neighbor's reachability when next required to send a packet to it.
Specification Text:
A Neighbor Cache entry enters the STALE state when created as a result of receiving packets other than solicited Neighbor Advertisements (i.e., Router Solicitations, Router Advertisements, Redirects, and Neighbor Solicitations). These packets contain the link-layer address of either the sender or, in the case of Redirect, the redirection target. However, receipt of these link-layer addresses does not confirm reachability of the forward-direction path to that node. Placing a newly created Neighbor Cache entry for which the link-layer address is known in the STALE state provides assurance that path failures are detected quickly. **In addition, should a cached link-layer address be modified due to receiving one of the above messages the state SHOULD also be set to STALE to provide prompt verification that the path to the new link-layer address is working.**

RQ_000_8519 Start Neighbor Reachability Determination
RFC2461 7.3.3 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node receives a Neighbor Solicitation that indicates a known neighbor's link-layer address has been modified.
Requirement:
The IPv6 node SHOULD update its internal information related to the neighboring node and SHOULD verify the neighbor's reachability when next required to send a packet to it.
Specification Text:
A Neighbor Cache entry enters the STALE state when created as a result of receiving packets other than solicited Neighbor Advertisements (i.e., Router Solicitations, Router Advertisements, Redirects, and Neighbor Solicitations). These packets contain the link-layer address of either the sender or, in the case of Redirect, the redirection target. However, receipt of these link-layer addresses does not confirm reachability of the forward-direction path to that node. Placing a newly created Neighbor Cache entry for which the link-layer address is known in the STALE state provides assurance that path failures are detected quickly. **In addition, should a cached link-layer address be modified due to receiving one of the above messages the state SHOULD also be set to STALE to provide prompt verification that the path to the new link-layer address is working.**

RQ_000_8521 Process Neighbor Advertisement
RFC2461 7.3.3 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a valid Neighbor Advertisement containing a Router Flag field set to zero (0) from a node that it has previously categorized as a router.
Requirement:
The IPv6 node must no longer use the advertising router as a default router for all the destination prefixes that it has previously associated with that router.
Specification Text:
To properly detect the case where a router switches from being a router to being a host (e.g., if its IP forwarding capability is turned off by system management), a node MUST compare the Router flag field in all received Neighbor Advertisement messages with the IsRouter flag recorded in the Neighbor Cache entry. **When a node detects that a neighbor has changed from being a router to being a host, the node MUST remove that router from the Default Router List and update the Destination Cache as described in Section 6.3.5.** Note that a router may not be listed in the Default Router List, even though a Destination Cache entry is using it (e.g., a host was redirected to it). In such cases, all Destination Cache entries that reference the (former) router must perform next-hop determination again before using the entry.

RQ_000_8522 Process Neighbor Advertisement
RFC2461 7.3.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a valid Neighbor Advertisement in which the Router Flag field is set to zero (0) from a neighboring node that it has previously categorized as a router but is not using as a default router.
Requirement:
The IPv6 node MUST perform next-hop determination for all addresses which would currently be directed towards neighboring node.
Specification Text:
To properly detect the case where a router switches from being a router to being a host (e.g., if its IP forwarding capability is turned off by system management), a node MUST compare the Router flag field in all received Neighbor Advertisement messages with the IsRouter flag recorded in the Neighbor Cache entry. **When a node detects that a neighbor has changed from being a router to being a host, the node MUST remove that router from the Default Router List and update the Destination Cache as described in Section 6.3.5. Note that a router may not be listed in the Default Router List, even though a Destination Cache entry is using it (e.g., a host was redirected to it). In such cases, all Destination Cache entries that reference the (former) router must perform next-hop determination again before using the entry.**

RQ_000_8524 Invalid Reachability Indications
RFC2461 7.3.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT use link-specific (proprietary) information to confirm the reachability of a neighboring node.
Specification Text:
In some cases, link-specific information may indicate that a path to a neighbor has failed (e.g., the resetting of a virtual circuit). In such cases, link-specific information may be used to purge Neighbor Cache entries before the Neighbor Unreachability Detection would do so. **However, link-specific information MUST NOT be used to confirm the reachability of a neighbor; such information does not provide end-to-end confirmation between neighboring IP layers.**

RQ_000_8526 Generate Redirect Message
RFC2461 8 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet in which the Source Address field is set to the IP address of a neighboring host and the Destination address is set to the IP Address of another node on the same link.
Requirement:
The IPv6 router MUST send a Redirect message to the sending host with both the Target Address field and the (Redirect) Destination Address field set to the IP address taken from the Destination field in the IPv6 header of the incoming packet.
Specification Text:
Redirect messages are sent by routers to redirect a host to a better first-hop router for a specific destination or **to inform hosts that a destination is in fact a neighbor (i.e., on-link). The latter is accomplished by having the ICMP Target Address be equal to the ICMP Destination Address.**

RQ_000_8527 Determine Redirect Target Address Field
RFC2461 8 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST be able to determine the link-local address of each of its neighboring routers.
Specification Text:
A router MUST be able to determine the link-local address for each of its neighboring routers in order to ensure that the target address in a Redirect message identifies the neighbor router by its link-local address. For static routing this requirement implies that the next-hop router's address should be specified using the link-local address of the router. For dynamic routing this requirement implies that all IPv6 routing protocols must somehow exchange the link-local addresses of neighboring routers.

RQ_000_8528 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard a received Redirect message in which the Source Address field of the containing IPv6 Packet header contains an address that is not a link-local address.
Specification Text:
A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- **IP Source Address is a link-local address.** Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 40 or more octets.
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- The ICMP Target Address is either a link-local address (when redirected to a router) or the same as the ICMP Destination Address (when redirected to the on-link destination).
- All included options have a length that is greater than zero.

RQ_000_8529 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard a received Redirect message in which the Hop Limit field of the containing IPv6 Packet header is set to value other than decimal 255.
Specification Text:
A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- **The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.**
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 40 or more octets.
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- The ICMP Target Address is either a link-local address (when redirected to a router) or the same as the ICMP Destination Address (when redirected to the on-link destination).
- All included options have a length that is greater than zero.

RQ_000_8530 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard a received Redirect message containing an Authentication Header if the packet fails authentication.
Specification Text:
A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- **If the message includes an IP Authentication Header, the message authenticates correctly.**
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 40 or more octets.
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- The ICMP Target Address is either a link-local address (when redirected to a router) or the same as the ICMP Destination Address (when redirected to the on-link destination).
- All included options have a length that is greater than zero.

RQ_000_8531 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard a received Redirect message in which the contents of the ICMPv6 Checksum field does not match the calculated checksum value.
Specification Text:
A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- **ICMP Checksum is valid.**
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 40 or more octets.
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- The ICMP Target Address is either a link-local address (when redirected to a router) or the same as the ICMP Destination Address (when redirected to the on-link destination).
- All included options have a length that is greater than zero.

RQ_000_8532 Process Field Anomalies in Redirect Message

RFC2461 8.1 MANDATORY

Applies to: Host

Context:

Requirement:

An IPv6 host MUST silently discard a received Redirect message in which the ICMPv6 packet length (derived from the Payload Length field in the IPv6 Packet Header) is less than 24 octets.

Specification Text:

A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- **ICMP length (derived from the IP length) is 40 or more octets.**
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- The ICMP Target Address is either a link-local address (when redirected to a router) or the same as the ICMP Destination Address (when redirected to the on-link destination).
- All included options have a length that is greater than zero.

RQ_000_8533 Host Processing of Redirect Message

RFC2461 8.1 MANDATORY

Applies to: Host

Context:

Requirement:

An IPv6 host MUST silently discard a received Redirect message in which the Source Address of the containing IPv6 Packet header is not the same as the address of current first-hop router associated internally with the address received in the Redirect Destination Address field.

Specification Text:

A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 40 or more octets.
- **The IP source address of the Redirect is the same as the current** first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- The ICMP Target Address is either a link-local address (when redirected to a router) or the same as the ICMP Destination Address (when redirected to the on-link destination).
- All included options have a length that is greater than zero.

RQ_000_8534 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard a received Redirect message in which the ICMPv6 Code field is not set to zero (0).
Specification Text:
A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- **ICMP Code is 0.**
- ICMP length (derived from the IP length) is 40 or more octets.
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- The ICMP Target Address is either a link-local address (when redirected to a router) or the same as the ICMP Destination Address (when redirected to the on-link destination).
- All included options have a length that is greater than zero.

RQ_000_8535 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard a received Redirect message in which the (Redirect) Destination Address field contains a multicast address
Specification Text:
A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 40 or more octets.
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- **The ICMP Destination Address field in the redirect message does not contain a multicast address.**
- The ICMP Target Address is either a link-local address (when redirected to a router) or the same as the ICMP Destination Address (when redirected to the on-link destination).
- All included options have a length that is greater than zero.

RQ_000_8536 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard a received Redirect message in which the Target Address field and the Destination Address field contain different values and the Target Address field does not contain a link-local address.
Specification Text:
A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 40 or more octets.
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- **The ICMP Target Address is** either **a link-local address (when redirected to a router)** or the same as the ICMP Destination Address (when redirected to the on-link destination).
- All included options have a length that is greater than zero.

RQ_000_8537 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST silently discard a received Redirect message in which the Target Address field and the Destination Address field contain the same link-local address
Specification Text:
A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 40 or more octets.
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- **The ICMP Target Address is** either a link-local address (when redirected to a router) or **the same as the ICMP Destination Address (when redirected to the on-link destination)**.
- All included options have a length that is greater than zero.

RQ_000_8538 Process Option Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:
The implementation receives a Redirect message containing an option that has a Length field equal to 0.
Requirement:
An IPv6 host MUST silently discard a received Redirect message if the Length field in any of its included options is set to zero (0)
Specification Text:
A host MUST silently discard any received Redirect message that does not satisfy all of the following validity checks:

- IP Source Address is a link-local address. Routers must use their link-local address as the source for Router Advertisement and Redirect messages so that hosts can uniquely identify routers
- The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router.
- If the message includes an IP Authentication Header, the message authenticates correctly.
- ICMP Checksum is valid.
- ICMP Code is 0.
- ICMP length (derived from the IP length) is 40 or more octets.
- The IP source address of the Redirect is the same as the current first-hop router for the specified ICMP Destination Address.
- The ICMP Destination Address field in the redirect message does not contain a multicast address.
- The ICMP Target Address is}} either a link-local address (when redirected to a router) or **the same as the ICMP Destination Address (when redirected to the on-link destination).**

{{- All included options have a length that is greater than zero.

RQ_000_8539 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST ignore the contents of the Reserved field in a received Redirect message.
Specification Text:
The contents of the Reserved field, and of any unrecognized options **MUST be ignored.** Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values.

RQ_000_8540 Process Option Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST ignore the contents of any unrecognized option in a received Redirect message.
Specification Text:
The contents of the Reserved field, and **of any unrecognized options MUST be ignored.** Future, backward-compatible changes to the protocol may specify the contents of the Reserved field or add new options; backward-incompatible changes may use different Code values.

RQ_000_8541 Process Option Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST ignore the contents of a Source Link-Layer option contained in a received Redirect message.
Specification Text:
The contents of any defined options that are not specified to be used with Redirect messages MUST be ignored and the packet processed as normal. The only defined options that may appear are the Target Link-Layer Address option and the Redirected Header option.

RQ_000_8542 Process Option Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST ignore the contents of a Prefix Information option contained in a received Redirect message.
Specification Text:
The contents of any defined options that are not specified to be used with Redirect messages MUST be ignored and the packet processed as normal. The only defined options that may appear are the Target Link-Layer Address option and the Redirected Header option.

RQ_000_8543 Process Option Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST ignore the contents of an MTU option contained in a received Redirect message.
Specification Text:
The contents of any defined options that are not specified to be used with Redirect messages MUST be ignored and the packet processed as normal. The only defined options that may appear are the Target Link-Layer Address option and the Redirected Header option.

RQ_000_8544 Generate Redirect Options
RFC2461 8.1 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Redirect message, an IPv6 router MUST NOT include any options other than the Target Link-Layer Address option and the Redirected Header option.
Specification Text:
The contents of any defined options that are not specified to be used with Redirect messages MUST be ignored and the packet processed as normal. The only defined options that may appear are the Target Link-Layer Address option and the Redirected Header option.

RQ_000_8545 Process Field Anomalies in Redirect Message
RFC2461 8.1 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST accept and process a received Redirect message in which the Target Address field contains an address which is not covered under one of the prefixes established for the link on which the Redirect is received.
Specification Text:
A host MUST NOT consider a redirect invalid just because the Target Address of the redirect is not covered under one of the link's prefixes. Part of the semantics of the Redirect message is that the Target Address is on-link.

RQ_000_8546 Generate Redirect Message
RFC2461 8.2 RECOMMENDED
Applies to: Router
Context:

An IPv6 router receives a packet in which:
- the Source Address field contains the address of a node that the router has categorized as a Neighbor;
- the Destination Address field contains an address which the router determines can be reached more efficiently through a different router on the same link as the sending node; and
- the Destination Address field does not contain a multicast address.

Requirement:

The IPv6 router SHOULD send a Redirect message to the sending node

Specification Text:

A router SHOULD send a redirect message, subject to rate limiting, whenever it forwards a packet that is not explicitly addressed to itself (i.e. a packet that is not source routed through the router) in which:

- the Source Address field of the packet identifies a neighbor, and
- the router determines that a better first-hop node resides on the same link as the sending node for the Destination Address of the packet being forwarded, and
- the Destination Address of the packet is not a multicast address

RQ_000_8547 Generate Redirect Message
RFC2461 8.2 MANDATORY
Applies to: Router
Context:

Requirement:

When constructing a Redirect message, an IPv6 router MUST set the fields in the message as follows:

Field	Value
Target Address	Address to which subsequent packets for the destination should be sent;
Destination Address	Destination Address field from the IPv6 Header of the invoking packet;
Target Link-Layer Address option	Link-layer address associated target address, if available;
Redirected Header option	As much of the forwarded packet as will fit in the remainder of the Redirect packet without exceeding 1280 octets.

Specification Text:

The transmitted redirect packet contains, consistent with the message format given in Section 4.5:

- In the Target Address field: the address to which subsequent packets for the destination SHOULD be sent. If the target is a router, that router's link-local address MUST be used. If the target is a host the target address field MUST be set to the same value as the Destination Address field.
- In the Destination Address field: the destination address of the invoking IP packet.
- In the options:
o Target Link-Layer Address option: link-layer address of the target, if known.
o Redirected Header: as much of the forwarded packet as can fit without the redirect packet exceeding 1280 octets in size.

RQ_000_8549 Generate Redirect Message
RFC2461 8.2 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Redirect message in which the Target Address field and the Destination Address field contain different addresses, an IPv6 router MUST set the Target Address field to contain the link-local address of the target router.
Specification Text:
The transmitted redirect packet contains, consistent with the message format given in Section 4.5:

- **In the Target Address field: the address to which subsequent packets for the destination SHOULD be sent. If the target is a router, that router's link-local address MUST be used**. If the target is a host the target address field MUST be set to the same value as the Destination Address field.
- In the Destination Address field: the destination address of the invoking IP packet.
- In the options:
  o Target Link-Layer Address option: link-layer address of the target, if known.
  o Redirected Header: as much of the forwarded packet as can fit without the redirect packet exceeding 1280 octets in size.

RQ_000_8550 Determine Redirect Target Address Field
RFC2461 8.2 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Redirect message in which the Target Address field contains the address of a host, an IPv6 router MUST set the Target Address and the Destination Address to contain the same non-link-local address.
Specification Text:
The transmitted redirect packet contains, consistent with the message format given in Section 4.5:

- **In the Target Address field: the address to which subsequent packets for the destination SHOULD be sent.** If the target is a router, that router's link-local address MUST be used. **If the target is a host the target address field MUST be set to the same value as the Destination Address field.**
- In the Destination Address field: the destination address of the invoking IP packet.
- In the options:
  o Target Link-Layer Address option: link-layer address of the target, if known.
  o Redirected Header: as much of the forwarded packet as can fit without the redirect packet exceeding 1280 octets in size.

RQ_000_8551 Generate Redirect Message
RFC2461 8.2 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 node MUST limit the rate at which Redirect messages are sent to a single destination.
Specification Text:
A router MUST limit the rate at which Redirect messages are sent, in order to limit the bandwidth and processing costs incurred by the Redirect messages when the source does not correctly respond to the Redirects, or the source chooses to ignore unauthenticated Redirect messages. **More details on the rate-limiting of ICMP error messages can be found in [ICMPv6].**

RQ_000_8552 Router Processing of Redirect Message
RFC2461 8.2 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST NOT update its routing tables upon receipt of a Redirect
Specification Text:
A router MUST NOT update its routing tables upon receipt of a Redirect.

RQ_000_8554 Host Processing of Redirect Message
RFC2461 8.3 RECOMMENDED
Applies to: Host
Context:
An IPv6 host receives a valid Redirect message.
Requirement:
The IPv6 host SHOULD ensure that subsequent packets sent to the address specified in the Destination Address field of the Redirect message are initially routed to the address contained in the Target Address field of the Redirect.
Specification Text:
A host receiving a valid redirect SHOULD update its Destination Cache accordingly so that subsequent traffic goes to the specified target. If no Destination Cache entry exists for the destination, an implementation SHOULD create such an entry.

RQ_000_8556 Host Processing of Redirect Message
RFC2461 8.3 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a valid Redirect message in which the Target Address field contains the address of a neighboring node that the receiving host has previously categorized as reachable and the Target Link-Layer Address option contains the same link-layer address that the host has associated with the Target Address.
Requirement:
The IPv6 host MUST continue to categorize the neighboring target node as reachable using the existing link-layer address.
Specification Text:
If the redirect contains a Target Link-Layer Address option the host either creates or updates the Neighbor Cache entry for the target. In both cases the cached link-layer address is copied from the Target Link-Layer Address option. If a Neighbor Cache entry is created for the target its reachability state MUST be set to STALE as specified in Section 7.3.3. If a cache entry already existed and it is updated with a different link-layer address, its reachability state MUST also be set to STALE. **If the link-layer address is the same as that already in the cache, the cache entry's state remains unchanged.**

RQ_000_8557 Host Processing of Redirect Message
RFC2461 8.3 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a valid Redirect message in which the Target Address field contains the address of a neighboring node that the receiving host has previously categorized as reachable and the Target Link-Layer Address option contains a link-layer address that is not the same as the one that the host has associated with the Target Address.
Requirement:
The IPv6 host MUST update its internal information related to the neighboring node and MUST verify the neighbor's reachability when next required to send a packet to it.
Specification Text:
If the redirect contains a Target Link-Layer Address option the host either creates or updates the Neighbor Cache entry for the target. In both cases the cached link-layer address is copied from the Target Link-Layer Address option. If a Neighbor Cache entry is created for the target its reachability state MUST be set to STALE as specified in Section 7.3.3. **If a cache entry already existed and it is updated with a different link-layer address, its reachability state MUST also be set to STALE.** If the link-layer address is the same as that already in the cache, the cache entry's state remains unchanged.

RQ_000_8558 Host Processing of Redirect Message

RFC2461 8.3 MANDATORY

Applies to: Host

Context:

An IPv6 host receives a valid Redirect message in which the Target Address field contains the address of a node that the receiving host has not previously categorized as a neighbor and the Target Link-Layer Address option contains a link-layer

Requirement:

The IPv6 node MUST categorize the Target node as a neighbor, associate the Target Link-Layer Address with that node and MUST verify the new neighbor's reachability when next required to send a packet to it.

Specification Text:

If the redirect contains a Target Link-Layer Address option the host either creates or updates the Neighbor Cache entry for the target. In both cases the cached link-layer address is copied from the Target Link-Layer Address option. **If a Neighbor Cache entry is created for the target its reachability state MUST be set to STALE as specified in Section 7.3.3.** If a cache entry already existed and it is updated with a different link-layer address, its reachability state MUST also be set to STALE. If the link-layer address is the same as that already in the cache, the cache entry's state remains unchanged.

RQ_000_8559 Host Processing of Redirect Message

RFC2461 8.3 MANDATORY

Applies to: Host

Context:

An IPv6 host receives a valid Redirect message in which the Target Address field and the Destination Address field both contain the address of the same known neighbor.

Requirement:

The IPv6 host MUST NOT change its categorization of the neighboring node as either a router or a host.

Specification Text:

If the Target and Destination Addresses are the same, the host MUST treat the Target as on-link. If the Target Address is not the same as the Destination Address, the host MUST set IsRouter to TRUE for the target. If the Target and Destination Addresses are the same, however, one cannot reliably determine whether the Target Address is a router. Consequently, newly created Neighbor Cache entries should set the IsRouter flag to FALSE, **while existing cache entries should leave the flag unchanged.** If the Target is a router, subsequent Neighbor Advertisement or Router Advertisement messages will update IsRouter accordingly.

RQ_000_8560 Host Processing of Redirect Message

RFC2461 8.3 | MUST; RFC 2461, Appendix D MANDATORY

Applies to: Host

Context:

An IPv6 host receives a valid Redirect message in which the Target Address field and the Destination Address field contain different values.

Requirement:

The IPv6 host MUST categorize the Target node as a router.

Specification Text:

If the Target and Destination Addresses are the same, the host MUST treat the Target as on-link. If the Target Address is not the same as the Destination Address, the host MUST set IsRouter to TRUE for the target. If the Target and Destination Addresses are the same, however, one cannot reliably determine whether the Target Address is a router. Consequently, newly created Neighbor Cache entries should set the IsRouter flag to FALSE, while existing cache entries should leave the flag unchanged. If the Target is a router, subsequent Neighbor Advertisement or Router Advertisement messages will update IsRouter accordingly.

RQ_000_8561 Host Processing of Redirect Message
RFC2461 8.3 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a valid Redirect message in which the Target Address field and the Destination Address field both contain the address of the same previously unknown neighbor.
Requirement:
The IPv6 host MUST categorize the Target node as a neighboring host.
Specification Text:
If the Target and Destination Addresses are the same, the host MUST treat the Target as on-link. If the Target Address is not the same as the Destination Address, the host MUST set IsRouter to TRUE for the target. If the Target and Destination Addresses are the same, however, one cannot reliably determine whether the Target Address is a router. Consequently, **newly created Neighbor Cache entries should set the IsRouter flag to FALSE,** while existing cache entries should leave the flag unchanged. If the Target is a router, subsequent Neighbor Advertisement or Router Advertisement messages will update IsRouter accordingly.

RQ_000_8562 Host Processing of Redirect Message
RFC2461 8.3 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a valid Redirect message
Requirement:
The IPv6 node MUST send subsequent packets to the address contained in the Destination Address field of the received Redirect message via the address contained in the Target Address field as the next hop.
Specification Text:
Redirect messages apply to all flows that are being sent to a given destination. That is, upon receipt of a Redirect for a Destination Address, all Destination Cache entries to that address should be updated to use the specified next-hop, regardless of the contents of the Flow Label field that appears in the Redirected Header option.

RQ_000_8564 Generate Redirect Message
RFC2461 8.3 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST NOT send a Redirect message.
Specification Text:
A host MUST NOT send Redirect messages.

RQ_000_8565 Using Options in Neighbor Discovery Messages
RFC2461 9 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ignore the contents of an unrecognized option in a valid Neighbor Discovery message.
Specification Text:
In order to ensure that future extensions properly coexist with current implementations, all nodes MUST silently ignore any options they do not recognize in received ND packets and continue processing the packet. All options specified in this document MUST be recognized. A node MUST NOT ignore valid options just because the ND message contains unrecognized ones.

RQ_000_8566 Using Options in Neighbor Discovery Messages
RFC2461 9 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST attempt to process any valid option received in a Neighbor Discovery message.
Specification Text:
In order to ensure that future extensions properly coexist with current implementations, all nodes MUST silently ignore any options they do not recognize in received ND packets and continue processing the packet. **All options specified in this document MUST be recognized.** A node MUST NOT ignore valid options just because the ND message contains unrecognized ones.

RQ_000_8567 Using Options in Neighbor Discovery Messages
RFC2461 9 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT ignore any valid options that are received in a Neighbor Discovery message that also contains unrecognized options.
Specification Text:
In order to ensure that future extensions properly coexist with current implementations, all nodes MUST silently ignore any options they do not recognize in received ND packets and continue processing the packet. All options specified in this document MUST be recognized. **A node MUST NOT ignore valid options just because the ND message contains unrecognized ones.**

RQ_000_8572 Using Options in Neighbor Discovery Messages
RFC2461 9 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST process all valid options received in a Neighbor Discovery message regardless of their order within the message.
Specification Text:
Options in Neighbor Discovery packets can appear in any order; receivers MUST be prepared to process them independently of their order. There can also be multiple instances of the same option in a message (e.g., Prefix Information options).

RQ_000_8573 Using Options in Neighbor Discovery Messages
RFC2461 9 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST process all valid instances of the same option within a single Neighbor Discovery message.
Specification Text:
Options in Neighbor Discovery packets can appear in any order; receivers MUST be prepared to process them independently of their order. **There can also be multiple instances of the same option in a message (e.g., Prefix Information options).**

RQ_000_8574 Router Processing of RA
RFC2461 9 OPTIONAL
Applies to: Router
Context:

Requirement:
An IPv6 router MAY send multiple Router advertisement messages with each containing a subset of the required options.
Specification Text:
If the number of included options in a Router Advertisement causes the advertisement's size to exceed the link MTU, the router can send multiple separate advertisements each containing a subset of the options.

RQ_000_8575 Generate Redirect Options
RFC2461 9 MANDATORY
Applies to: Router
Context:

Requirement:
When constructing a Redirect message, an IPv6 router MUST limit the amount of data included in the Redirected Header option such that the entire Redirect message does not exceed 1280 octets.
Specification Text:
The amount of data to include in the Redirected Header option MUST be limited so that the entire redirect packet does not exceed 1280 octets.

RQ_000_8576 Generate Neighbor Discovery Messages
RFC2461 9 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a neighbor Discovery message, an IPv6 node MUST limit the size of the entire packet (IPv6 Header plus Neighbor Discovery message) such that it does not exceed the MTU of the link on which it is to be sent.
Specification Text:
The size of an ND packet including the IP header is limited to the link MTU (which is at least 1280 octets). When adding options to an ND packet a node MUST NOT exceed the link MTU.

RQ_000_8577 ND Protocol Constants and Default Values
RFC2461 10 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST use the following timers and counters when sending and receiving Neighbor Discovery messages:

Timer/Counter	Value
Maximum interval between initial RA messages	16 seconds
Maximum number of initial RA messages	3
Maximum number of final RA messages	3
Minimum delay between RA messages	3 seconds
Maximum delay before sending a RA message	0.5 seconds

Specification Text:
Router constants:

MAX_INITIAL_RTR_ADVERT_INTERVAL	**16 seconds**
MAX_INITIAL_RTR_ADVERTISEMENTS	**3 transmissions**
MAX_FINAL_RTR_ADVERTISEMENTS	**3 transmissions**
MIN_DELAY_BETWEEN_RAS	**3 seconds**
MAX_RA_DELAY_TIME	**0.5 seconds**

Host constants:

MAX_RTR_SOLICITATION_DELAY	1 second
RTR_SOLICITATION_INTERVAL	4 seconds
MAX_RTR_SOLICITATIONS	3 transmissions

```
Node constants:

  MAX_MULTICAST_SOLICIT             3 transmissions
  MAX_UNICAST_SOLICIT               3 transmissions
  MAX_ANYCAST_DELAY_TIME            1 second
  MAX_NEIGHBOR_ADVERTISEMENT        3 transmissions
  REACHABLE_TIME               30,000 milliseconds
  RETRANS_TIMER                 1,000 milliseconds
  DELAY_FIRST_PROBE_TIME            5 seconds
  MIN_RANDOM_FACTOR                 .5
  MAX_RANDOM_FACTOR                 1.5
```

RQ_000_8578 ND Protocol Constants and Default Values
RFC2461 10 MANDATORY
Applies to: Host
Context:

Requirement:

```
An IPv6 host MUST use the following timers and counters when sending and receiving Neighbor
Discovery messages:

  Timer/Counter             | Value
  ==========================+===============
  Maximum interval between  | 4 seconds
  RS messages               +
  Maximum number of         | 3
  repeated RS messages      +
  Maximum delay before      | 1 second
  sending a RS message      +
```

Specification Text:

```
Router constants:

  MAX_INITIAL_RTR_ADVERT_INTERVAL  16 seconds
  MAX_INITIAL_RTR_ADVERTISEMENTS    3 transmissions
  MAX_FINAL_RTR_ADVERTISEMENTS      3 transmissions
  MIN_DELAY_BETWEEN_RAS             3 seconds
  MAX_RA_DELAY_TIME               0.5 seconds

Host constants:

  MAX_RTR_SOLICITATION_DELAY        1 second
  RTR_SOLICITATION_INTERVAL         4 seconds
  MAX_RTR_SOLICITATIONS             3 transmissions

Node constants:

  MAX_MULTICAST_SOLICIT             3 transmissions
  MAX_UNICAST_SOLICIT               3 transmissions
  MAX_ANYCAST_DELAY_TIME            1 second
  MAX_NEIGHBOR_ADVERTISEMENT        3 transmissions
  REACHABLE_TIME               30,000 milliseconds
  RETRANS_TIMER                 1,000 milliseconds
  DELAY_FIRST_PROBE_TIME            5 seconds
  MIN_RANDOM_FACTOR                 .5
  MAX_RANDOM_FACTOR                 1.5
```

RQ_000_8579 ND Protocol Constants and Default Values
RFC2461 10 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST use the following timers and counters when sending and receiving Neighbor Discovery messages:

Timer/Counter	Value
Maximum number of multicast solicitations	3
Maximum number of unicast solicitations	3
Maximum delay before sending an anycast ND message	1 second
Maximum number of repeated NA messages	3
Reachable Timer	30 seconds
Retransmission Timer	1 second
Delay to first probe	5 seconds
Minimum randomization factor	0.5
Maximum randomization factor	1.5

Specification Text:
Router constants:

MAX_INITIAL_RTR_ADVERT_INTERVAL	16 seconds
MAX_INITIAL_RTR_ADVERTISEMENTS	3 transmissions
MAX_FINAL_RTR_ADVERTISEMENTS	3 transmissions
MIN_DELAY_BETWEEN_RAS	3 seconds
MAX_RA_DELAY_TIME	0.5 seconds

Host constants:

MAX_RTR_SOLICITATION_DELAY	1 second
RTR_SOLICITATION_INTERVAL	4 seconds
MAX_RTR_SOLICITATIONS	3 transmissions

Node constants:

MAX_MULTICAST_SOLICIT	**3 transmissions**
MAX_UNICAST_SOLICIT	**3 transmissions**
MAX_ANYCAST_DELAY_TIME	**1 second**
MAX_NEIGHBOR_ADVERTISEMENT	**3 transmissions**
REACHABLE_TIME	**30,000 milliseconds**
RETRANS_TIMER	**1,000 milliseconds**
DELAY_FIRST_PROBE_TIME	**5 seconds**
MIN_RANDOM_FACTOR	**.5**
MAX_RANDOM_FACTOR	**1.5**

RQ_000_8580 Process Redirect Message
RFC2461 11 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST silently ignore a Redirect message received from a router that the node is not currently using for the address contained in the Destination Address field.
Specification Text:
The trust model for redirects is the same as in IPv4. **A redirect is accepted only if received from the same router that is currently being used for that destination.** It is natural to trust the routers on the link. If a host has been redirected to another node (i.e., the destination is on-link) there is no way to prevent the target from issuing another redirect to some other destination. However, this exposure is no worse than it was; the target host, once subverted, could always act as a hidden router to forward traffic elsewhere.

RQ_000_8581 Generate Neighbor Discovery Messages
RFC2461 11 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node SHOULD include an Authentication Header in the containing IPv6 Packet header of a Neighbor Discovery message sent to a destination for which an AH security association exists.
Specification Text:
Neighbor Discovery protocol packet exchanges can be authenticated using the IP Authentication Header [IPv6-AUTH]. **A node SHOULD include an Authentication Header when sending Neighbor Discovery packets if a security association for use with the IP Authentication Header exists for the destination address.** The security associations may have been created through manual configuration or through the operation of some key management protocol.

RQ_000_8583 Process Neighbor Discovery Messages
RFC2461 11 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST ignore any received Neighbor Discovery message in which the Authentication Header fails authentication.
Specification Text:
Received Authentication Headers in Neighbor Discovery packets MUST be verified for correctness and packets with incorrect authentication MUST be ignored.

RQ_000_8584 Process Neighbor Discovery Messages
RFC2461 11 RECOMMENDED
Applies to: Router, Host
Context:

Requirement:
An IPv6 node SHOULD make it possible for received Neighbor Discovery packets to be ignored if they are not authenticated by either the Authentication Header or the Encapsulated Security Payload methods.
Specification Text:
It SHOULD be possible for the system administrator to configure a node to ignore any Neighbor Discovery messages that are not authenticated using either the Authentication Header or Encapsulating Security Payload. The configuration technique for this MUST be documented. Such a switch SHOULD default to allowing unauthenticated messages.

RQ_000_8585 Process Neighbor Discovery Messages
RFC2461 11 RECOMMENDED
Applies to: Router, Host
Context:

Requirement:
Unless configured otherwise by system management procedures, an IPv6 node SHOULD process all received unauthenticated Neighbor Discovery messages.
Specification Text:
It SHOULD be possible for the system administrator to configure a node to ignore any Neighbor Discovery messages that are not authenticated using either the Authentication Header or Encapsulating Security Payload. The configuration technique for this MUST be documented. **Such a switch SHOULD default to allowing unauthenticated messages.**

RQ_000_8586 Process Router Solicitation
RFC2461 Appendix D MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST categorize the sender of a received Router Solicitation message as a host.
Specification Text:
The background for these rules is that the ND messages contain, either implicitly or explicitly, information that indicates whether or not the sender (or Target Address) is a host or a router. The following assumptions are used:

- **The sender of a Router Solicitation is implicitly assumed to be a host since there is no need for routers to send such messages.**
- The sender of a Router Advertisement is implicitly assumed to be a router.
- Neighbor Solicitation messages do not contain either an implicit or explicit indication about the sender. Both hosts and routers send such messages.
- Neighbor Advertisement messages contain an explicit "IsRouter flag", the R-bit.
- The target of the redirect, when the target differs from the destination address in the packet being redirected, is implicitly assumed to be a router. This is a natural assumption since that node is expected to be able to forward the packets towards the destination.
- The target of the redirect, when the target is the same as the destination, does not carry any host vs. router information. All that is known is that the destination (i.e. target) is on-link but it could be either a host or a router.

RQ_000_8587 Process Router Advertisement
RFC2461 Appendix D MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST categorize the sender of a received Router Advertisement message as a router.
Specification Text:
The background for these rules is that the ND messages contain, either implicitly or explicitly, information that indicates whether or not the sender (or Target Address) is a host or a router. The following assumptions are used:

- The sender of a Router Solicitation is implicitly assumed to be a host since there is no need for routers to send such messages.
- **The sender of a Router Advertisement is implicitly assumed to be a router.**
- Neighbor Solicitation messages do not contain either an implicit or explicit indication about the sender. Both hosts and routers send such messages.
- Neighbor Advertisement messages contain an explicit "IsRouter flag", the R-bit.
- The target of the redirect, when the target differs from the destination address in the packet being redirected, is implicitly assumed to be a router. This is a natural assumption since that node is expected to be able to forward the packets towards the destination.
- The target of the redirect, when the target is the same as the destination, does not carry any host vs. router information. All that is known is that the destination (i.e. target) is on-link but it could be either a host or a router.

RQ_000_8588 Process Redirect Message
RFC2461 Appendix D MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST categorize the sender of a received Redirect message as a router if the Target Address field in the Redirect contains a different address to the Destination Address field.

Specification Text:

```
The background for these rules is that the ND messages contain, either implicitly or
explicitly, information that indicates whether or not the sender (or Target Address) is a host
or a router.  The following assumptions are used:

 - The sender of a Router Solicitation is implicitly assumed to be a
   host since there is no need for routers to send such messages.
 - The sender of a Router Advertisement is implicitly assumed to be a
   router.
 - Neighbor Solicitation messages do not contain either an implicit
   or explicit indication about the sender.  Both hosts and routers
   send such messages.
 - Neighbor Advertisement messages contain an explicit "IsRouter
   flag", the R-bit.
 - The target of the redirect, when the target differs from the
   destination address in the packet being redirected, is implicitly
   assumed to be a router.  This is a natural assumption since that
   node is expected to be able to forward the packets towards the
   destination.
 - The target of the redirect, when the target is the same as the
   destination, does not carry any host vs. router information.  All
   that is known is that the destination (i.e. target) is on-link but
   it could be either a host or a router.
```

RQ_000_8589 Host Processing of Redirect Message

RFC2461 Appendix D MANDATORY

Applies to: Host, Router

Context:

Requirement:

```
An IPv6 node MUST NOT re-categorize the sender of a received Redirect message as either a
router or a host if the Target Address field in the Redirect contains the same address as the
Destination Address field.
```

Specification Text:

```
The background for these rules is that the ND messages contain, either implicitly or
explicitly, information that indicates whether or not the sender (or Target Address) is a host
or a router.  The following assumptions are used:

 - The sender of a Router Solicitation is implicitly assumed to be a
   host since there is no need for routers to send such messages.
 - The sender of a Router Advertisement is implicitly assumed to be a
   router.
 - Neighbor Solicitation messages do not contain either an implicit
   or explicit indication about the sender.  Both hosts and routers
   send such messages.
 - Neighbor Advertisement messages contain an explicit "IsRouter
   flag", the R-bit.
 - The target of the redirect, when the target differs from the
   destination address in the packet being redirected, is implicitly
   assumed to be a router.  This is a natural assumption since that
   node is expected to be able to forward the packets towards the
   destination.
 - The target of the redirect, when the target is the same as the
   destination, does not carry any host vs. router information.  All
   that is known is that the destination (i.e. target) is on-link but
   it could be either a host or a router.
```

RQ_000_8590 Process Neighbor Solicitation

RFC2461 Appendix D MANDATORY

Applies to: Host, Router

Context:

Requirement:

```
An IPv6 node MUST NOT re-categorize the sender of a received Neighbor Solicitation message as
either a router or a host.
```

Specification Text:

```
The background for these rules is that the ND messages contain, either implicitly or
explicitly, information that indicates whether or not the sender (or Target Address) is a host
or a router.  The following assumptions are used:

 - The sender of a Router Solicitation is implicitly assumed to be a
   host since there is no need for routers to send such messages.
```

- The sender of a Router Advertisement is implicitly assumed to be a router.
- **Neighbor Solicitation messages do not contain either an implicit or explicit indication about the sender. Both hosts and routers send such messages.**
- Neighbor Advertisement messages contain an explicit "IsRouter flag", the R-bit.
- The target of the redirect, when the target differs from the destination address in the packet being redirected, is implicitly assumed to be a router. This is a natural assumption since that node is expected to be able to forward the packets towards the destination.
- The target of the redirect, when the target is the same as the destination, does not carry any host vs. router information. All that is known is that the destination (i.e. target) is on-link but it could be either a host or a router.

RQ_000_8591 Process Neighbor Discovery Messages
RFC2461 Appendix D MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST categorize the sender of a Neighbor Discovery message as either a router or a host based upon any explicit information contained in the message.
Specification Text:
The rules for setting the IsRouter flag are based on the information content above. **If an ND message contains explicit or implicit information the receipt of the message will cause the IsRouter flag to be updated.** But when there is no host vs. router information in the ND message the receipt of the message MUST NOT cause a change to the IsRouter state. When the receipt of such a message causes a Neighbor Cache entry to be created this document specifies that the IsRouter flag be set to FALSE. There is greater potential for mischief when a node incorrectly thinks a host is a router, than the other way around. In these cases a subsequent Neighbor Advertisement or Router Advertisement message will set the correct IsRouter value.

RQ_000_8592 Process Neighbor Discovery Messages
RFC2461 Appendix D MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST categorize the sender of a Neighbor Discovery message as either a router or a host based upon any implicit information contained in the message.
Specification Text:
The rules for setting the IsRouter flag are based on the information content above. **If an ND message contains explicit or implicit information the receipt of the message will cause the IsRouter flag to be updated.** But when there is no host vs. router information in the ND message the receipt of the message MUST NOT cause a change to the IsRouter state. When the receipt of such a message causes a Neighbor Cache entry to be created this document specifies that the IsRouter flag be set to FALSE. There is greater potential for mischief when a node incorrectly thinks a host is a router, than the other way around. In these cases a subsequent Neighbor Advertisement or Router Advertisement message will set the correct IsRouter value.

RQ_000_8593 Process Neighbor Discovery Messages
RFC2461 Appendix D MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT re-categorize the sender of a Neighbor Discovery message as a router or host if there is neither explicit nor implicit information regarding the sender's status.
Specification Text:
The rules for setting the IsRouter flag are based on the information content above. If an ND message contains explicit or implicit information the receipt of the message will cause the IsRouter flag to be updated. **But when there is no host vs. router information in the ND message the receipt of the message MUST NOT cause a change to the IsRouter state.** When the receipt of such a message causes a Neighbor Cache entry to be created this document specifies that the IsRouter flag be set to FALSE. There is greater potential for mischief when a node incorrectly thinks a host is a router, than the other way around. In these cases a subsequent Neighbor Advertisement or Router Advertisement message will set the correct IsRouter value.

RQ_000_8594 Address Resolution Behavior

RFC2461 7.2.5 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a Neighbor Advertisement message with the Override Flag field set to one (1), the Solicited Flag field set to zero (0) and the Target Link-Layer Address option containing an address which is the same as the link-layer address that the node has previously associated with the source neighboring node which it has categorized as unreachable.

Requirement:

The IPv6 node MUST NOT change its internal information concerning the neighboring node.

Specification Text:

If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; otherwise, the received advertisement should be ignored and MUST NOT update the cache. **If the Override flag is set,** both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).
- If the Solicited flag is set, the state of the entry MUST be set to REACHABLE**. If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged.** An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation. Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet. There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.
- The IsRouter flag in the cache entry MUST be set based on the Router flag in the received advertisement. In those cases where the IsRouter flag changes from TRUE to FALSE as a result of this update, the node MUST remove that router from the Default Router List and update the Destination Cache entries for all destinations using that neighbor as a router as specified in Section 7.3.3. This is needed to detect when a node that is used as a router stops forwarding packets due to being configured as a host.

RQ_000_8595 Form Unsolicited NA Header

RFC2461 4.4 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node receives a valid Neighbor Solicitation message

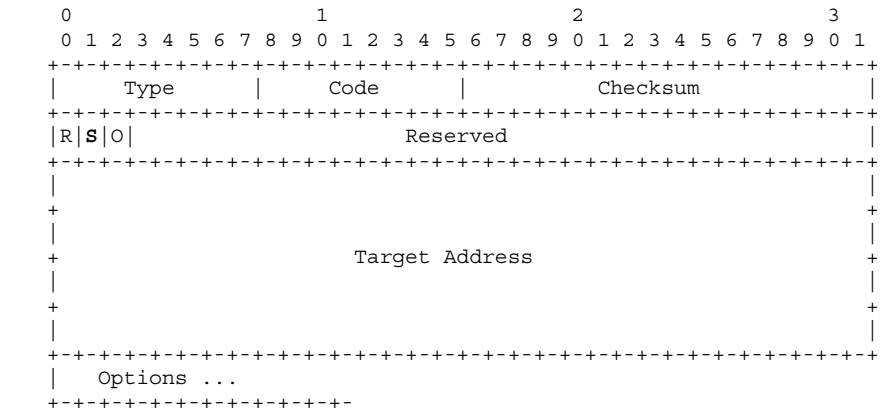
Requirement:

The IPv6 node MUST set the S-Flag (Octet 5, bit 1) to one (1) in the Neighbor Advertisement message sent in response to the received solicitation

Specification Text:

Neighbor Advertisement Message Format

A node sends Neighbor Advertisements in response to Neighbor Solicitations and sends unsolicited Neighbor Advertisements in order to (unreliably) propagate new information quickly.



……

ICMP Fields:

Type	136
Code	0
Checksum	The ICMP checksum. See RFC 2463.
R	Router flag. When set, the R-bit indicates that the sender is a router. The R-bit is used by Neighbor Unreachability Detection to detect a router that changes to a host.
S	**Solicited flag. When set, the S-bit indicates that the advertisement was sent in response to a Neighbor Solicitation from the Destination address.** The S-bit is used as a reachability confirmation for Neighbor Unreachability Detection. It MUST NOT be set in multicast advertisements or in unsolicited unicast advertisements.
O	Override flag. When set, the O-bit indicates that the advertisement should override an existing cache entry and update the cached link-layer address. When it is not set the advertisement will not update a cached link-layer address though it will update an existing Neighbor Cache entry for which no link-layer address is known. It SHOULD NOT be set in solicited advertisements for anycast addresses and in solicited proxy advertisements. It SHOULD be set in other solicited advertisements and in unsolicited advertisements.
Reserved	29-bit unused field. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.
Target Address	For solicited advertisements, the Target Address field in the Neighbor Solicitation message that prompted this advertisement. For an unsolicited advertisement, the address whose link-layer address has changed. The Target Address MUST NOT be a multicast address.

RQ_000_8596 Process Neighbor Advertisement
RFC2461 7.2.5 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a valid Neighbor Advertisement message in which the Router Flag field is set to one (1)
Requirement:
The IPv6 node MUST categorize the advertising node as a router.
Specification Text:
If the target's Neighbor Cache entry is in any state other than INCOMPLETE when the advertisement is received, processing becomes quite a bit more complex. If the Override flag is clear and the supplied link-layer address differs from that in the cache, then one of two actions takes place: if the state of the entry is REACHABLE, set it to STALE, but do not update the entry in any other way; otherwise, the received advertisement should be ignored and MUST NOT update the cache. If the Override flag is set, both the Override flag is clear and the supplied link-layer address is the same as that in the cache, or no Target Link-layer address option was supplied, the received advertisement MUST update the Neighbor Cache entry as follows:

- The link-layer address in the Target Link-Layer Address option MUST be inserted in the cache (if one is supplied and is different than the already recorded address).
- If the Solicited flag is set, the state of the entry MUST be set to REACHABLE. If the Solicited flag is zero and the link-layer address was updated with a different address the state MUST be set to STALE. Otherwise, the entry's state remains unchanged. An advertisement's Solicited flag should only be set if the advertisement is a response to a Neighbor Solicitation. Because Neighbor Unreachability Detection Solicitations are sent to the cached link-layer address, receipt of a solicited advertisement indicates that the forward path is working. Receipt of an unsolicited advertisement, however, suggests that a neighbor has urgent information to announce (e.g., a changed link-layer address). If the urgent information indicates a change from what a node is currently using, the node should verify the reachability of the (new) path when it sends the next packet. There is no need to update the state for unsolicited advertisements that do not change the contents of the cache.
- **The IsRouter flag in the cache entry MUST be set based on the Router flag in the received advertisement.** In those cases where the IsRouter flag changes from TRUE to FALSE as a result of this update, the node MUST remove that router from the Default Router List and update the Destination Cache entries for all destinations using that neighbor as a router as specified in Section 7.3.3. This is needed to detect when a node that is used as a router stops forwarding packets due to being configured as a host.

4.7 Requirements extracted from RFC 2462

RQ_000_1200 Simultaneous Stateless and Stateful Autoconfiguration
RFC2462 1 OPTIONAL
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MAY use stateful and stateless address autoconfiguration simultaneously
Specification Text:
The stateless approach is used when a site is not particularly concerned with the exact addresses hosts use, so long as they are unique and properly routable. The stateful approach is used when a site requires tighter control over exact address assignments. **Both stateful and stateless address autoconfiguration may be used simultaneously**. The site administrator specifies which type of autoconfiguration to use through the setting of appropriate fields in Router Advertisement messages RFC2461.

RQ_000_1210 Detect Duplicate Address (DAD)
RFC2462 5.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node has initiated the Duplicate Address Detection procedure but this has not completed.
Requirement:
The IPv6 node MUST accept Neighbor Solicitation and Neighbor Advertisement messages containing the address of the IPv6 node in the Target Address field but discard any other packets sent to that address.
Specification Text:
An address on which the duplicate Address Detection Procedure is applied is said to be tentative until the procedure has completed successfully. A tentative address is not considered "assigned to an interface" in the traditional sense. That is, **the interface must accept Neighbor Solicitation and Advertisement messages containing the tentative address in the Target Address field, but processes such packets differently from those whose Target Address matches an address assigned to the interface. Other packets addressed to the tentative address should be silently discarded**.

RQ_000_1225 Form Link-local Address
RFC2462 5.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node enables one of its interfaces which has an identifier of 118 bits or less in length
Requirement:
The IPv6 node assigns a link-local address to the interface by appending its identifier to the link-local prefix [FE80::0].
Specification Text:
A node forms a link-local address whenever an interface becomes enabled. An interface may become enabled after any of the following events:

- The interface is initialized at system startup time.

- The interface is reinitialized after a temporary interface failure or after being temporarily disabled by system management.

- The interface attaches to a link for the first time.

- The interface becomes enabled by system management after having been administratively disabled.

A link-local address is formed by prepending the well-known link-local prefix FE80::0 [RFC2373] (of appropriate length) to the interface identifier. If the interface identifier has a length of N bits, the interface identifier replaces the right-most N zero bits of the link-local prefix. If the interface identifier is more than 118 bits in length, autoconfiguration fails and manual configuration is required. Note that interface identifiers will typically be 64-bits long and based on EUI-64 identifiers as described in RFC2373.

A link-local address has an infinite preferred and valid lifetime; it is never timed out.

RQ_000_1231 Stateless Autoconfiguration
RFC2462 4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST initiate Stateless address autoconfiguration for a multicast-capable interface when the interface is enabled.
Specification Text:
Autoconfiguration is performed only on multicast-capable links and begins when a multicast-capable interface is enabled, e.g., during system startup. Nodes (both hosts and routers) begin the autoconfiguration process by generating a link-local address for the interface. A link-local address is formed by appending the interface's identifier to the well-known link-local prefix.

RQ_000_1232 Stateless Autoconfiguration
RFC2462 4 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST form a link-local address for an interface when the interface is enabled.
Specification Text:
Autoconfiguration is performed only on multicast-capable links and begins when a multicast-capable interface is enabled, e.g., during system startup. **Nodes (both hosts and routers) begin the autoconfiguration process by generating a link-local address for the interface.** A link-local address is formed by appending the interface's identifier to the well-known link-local prefix.

RQ_000_1235 Detect Duplicate Address (DAD)
RFC2462 4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a Neighbor Solicitation message with a Target Address field set to the link-local address associated with the interface on which the message is received.

Requirement:
The IPv6 node MUST send a Neighbor Advertisement message in which the Target Address field is set to the same value as that set in the Target Address field of the received Neighbor solicitation message.
Specification Text:
Before the link-local address can be assigned to an interface and used, however, a node must attempt to verify that this "tentative" address is not already in use by another node on the link. Specifically, it sends a Neighbor Solicitation message containing the tentative address as the target. **If another node is already using that address, it will return a Neighbor Advertisement saying so**. If another node is also attempting to use the same address, it will send a Neighbor Solicitation for the target as well. The exact number of times the Neighbor Solicitation is (re)transmitted and the delay time between consecutive solicitations is link-specific and may be set by system management.

RQ_000_1237 Duplicate Address Detection Timers and Counters
RFC2462 4 OPTIONAL
Applies to: Host, Router
Context:
An IPv6 node sends a Neighbor Solicitation message but gets no response.
Requirement:
An IPv6 node MAY retransmit a Neighbor Solicitation message any number of times at any appropriate interval.
Specification Text:
Before the link-local address can be assigned to an interface and used, however, a node must attempt to verify that this "tentative" address is not already in use by another node on the link. Specifically, it sends a Neighbor Solicitation message containing the tentative address as the target. If another node is already using that address, it will return a Neighbor Advertisement saying so. If another node is also attempting to use the same address, it will send a Neighbor Solicitation for the target as well. **The exact number of times the Neighbor Solicitation is (re)transmitted and the delay time between consecutive solicitations is link-specific** and may be set by system management.

RQ_000_1239 Detect Duplicate Address (DAD)

RFC2462 4 MANDATORY

Applies to: Host, Router

Context:

As part of its stateless address autoconfiguration process, an IPv6 node receives a Neighbor Advertisement message in response to its own Neighbor Solicitation.

Requirement:

The IPv6 node MUST terminate address autoconfiguration.

Specification Text:

Before the link-local address can be assigned to an interface and used, however, a node must attempt to verify that this "tentative" address is not already in use by another node on the link. Specifically, it sends a Neighbor Solicitation message containing the tentative address as the target. **If another node is already using that address, it will return a Neighbor Advertisement saying so**. If another node is also attempting to use the same address, it will send a Neighbor Solicitation for the target as well. The exact number of times the Neighbor Solicitation is (re)transmitted and the delay time between consecutive solicitations is link-specific and may be set by system management.

If a node determines that its tentative link-local address is not unique, autoconfiguration stops and manual configuration of the interface is required. To simplify recovery in this case, it should be possible for an administrator to supply an alternate interface identifier that overrides the default identifier in such a way that the autoconfiguration mechanism can then be applied using the new (presumably unique) interface identifier. Alternatively, link-local and other addresses will need to be configured manually.

RQ_000_1244 Stateless Autoconfiguration

RFC2462 4 MANDATORY

Applies to: Host, Router

Context:

As part of its stateless address autoconfiguration process, an IPv6 node receives no response to its own Neighbor Solicitation message.

Requirement:

The IPv6 node MUST assign the tentative link-local address to the interface on which autoconfiguration has completed.

Specification Text:

Once a node ascertains that its tentative link-local address is unique, it assigns it to the interface. At this point, the node has IP-level connectivity with neighboring nodes. The remaining autoconfiguration steps are performed only by hosts; the (auto)configuration of routers is beyond the scope of this document.

RQ_000_1246 Configure Address

RFC2462 4 MANDATORY

Applies to: Router

Context:

Requirement:

An IPv6 router MUST periodically transmit Router Advertisement messages to each of its interfaces specifying whether a receiving host should perform stateful or stateless autoconfiguration.

Specification Text:

The next phase of autoconfiguration involves obtaining a Router Advertisement or determining that no routers are present. **If routers are present, they will send Router Advertisements that specify what sort of autoconfiguration a host should do.** If no routers are present, stateful autoconfiguration should be invoked.

Routers send Router Advertisements periodically, but the delay between successive advertisements will generally be longer than a host performing autoconfiguration will want to wait [RFC2461]. To obtain an advertisement quickly, a host sends one or more Router

RQ_000_1248 Assign Global Address
RFC2462 4 OPTIONAL
Applies to: Host
Context:
An IPv6 host has successfully completed Duplicate Address Detection
Requirement:
The IPv6 host MAY send one or more Router Solicitations to the all-routers multicast group.
Specification Text:
Routers send Router Advertisements periodically, but the delay between successive advertisements will generally be longer than a host performing autoconfiguration will want to wait [DISCOVERY]. To obtain an advertisement quickly, a host sends one or more Router Solicitations to the all-routers multicast group.

RQ_000_1250 Assign Global Address
RFC2462 5.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST use Duplicate Address Detection (DAD) before assigning any unicast address to an interface.
Specification Text:
Duplicate Address Detection is performed on unicast addresses prior to assigning them to an interface whose DupAddrDetectTransmits variable is greater than zero. **Duplicate Address Detection MUST take place on all unicast addresses, regardless of whether they are obtained through stateful, stateless or manual configuration**.

RQ_000_1251 Assign Global Address
RFC2462 5.4 OPTIONAL
Applies to: Host, Router
Context:
An IPv6 node uses Stateless Autoconfiguration and has verified the uniqueness of the link-local address assigned to one of its interfaces.
Requirement:
The IPv6 node MAY decide not to test the uniqueness of each additional address created from an interface identifier that has already been verified as unique.
Specification Text:
Duplicate Address Detection is performed on unicast addresses prior to assigning them to an interface whose DupAddrDetectTransmits variable is greater than zero. Duplicate Address Detection MUST take place on all unicast addresses, regardless of whether they are obtained through stateful, stateless or manual configuration, with the exception of the following cases:

- Duplicate Address Detection MUST NOT be performed on anycast addresses.

- Each individual unicast address SHOULD be tested for uniqueness. **However, when stateless address autoconfiguration is used, address uniqueness is determined solely by the interface identifier, assuming that subnet prefixes are assigned correctly (i.e., if all of an interface's addresses are generated from the same identifier, either all addresses or none of them will be duplicates). Thus, for a set of addresses formed from the same interface identifier, it is sufficient to check that the link-local address generated from the identifier is unique on the link. In such cases, the link-local address MUST be tested for uniqueness, and if no duplicate address is detected, an implementation MAY choose to skip Duplicate Address Detection for additional addresses derived from the same interface identifier.**

RQ_000_1252 Stateful Autoconfiguration
RFC2462 4 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node uses Stateful Address Autoconfiguration to assign addresses to its interfaces.
Requirement:
Using Duplicate Address Detection (DAD), the IPv6 node SHOULD verify the uniqueness of each address assigned to each of its interfaces.
Specification Text:
For safety, all addresses must be tested for uniqueness prior to their assignment to an interface. In the case of addresses created through stateless autoconfig, however, the uniqueness of an address is determined primarily by the portion of the address formed from an interface identifier. Thus, if a node has already verified the uniqueness of a link-local address, additional addresses created from the same interface identifier need not be tested individually. **In contrast, all addresses obtained manually or via stateful address autoconfiguration should be tested for uniqueness individually.** To accommodate sites that believe the overhead of performing Duplicate Address Detection outweighs its benefits, the use of Duplicate Address Detection can be disabled through the administrative setting of a per-interface configuration flag.

RQ_000_1254 Configure Address
RFC2462 4 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MAY invoke Duplicate Address Detection (DAD) in parallel with sending a Router Solicitation message to the interface whose address is being verified.
Specification Text:
To speed the autoconfiguration process, **a host may generate its link-local address (and verify its uniqueness) in parallel with waiting for a Router Advertisement. Because a router may delay responding to a Router Solicitation for a few seconds, the total time needed to complete autoconfiguration can be significantly longer if the two steps are done serially**.

RQ_000_1255 Configure Address
RFC2462 5 MANDATORY
Applies to: Host
Context:
An IPv6 host has interfaces to more than one network
Requirement:
The IPv6 host MUST perform address autoconfiguration independently on each interface.
Specification Text:
Autoconfiguration is performed on a per-interface basis on multicast-capable interfaces. **For multihomed hosts, autoconfiguration is performed independently on each interface.**
Autoconfiguration applies primarily to hosts, with two exceptions. Routers are expected to generate a link-local address using the procedure outlined below. In addition, routers perform Duplicate Address Detection on all addresses prior to assigning them to an interface.

RQ_000_1272 Stateless Autoconfiguration
RFC2462 5.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST form a link-local address for an interface when the interface is enabled.
Specification Text:
A node forms a link-local address whenever an interface becomes enabled. An interface may become enabled after any of the following events:
- The interface is initialized at system startup time.
- The interface is reinitialized after a temporary interface failure or after being temporarily disabled by system management.
- The interface attaches to a link for the first time.
- The interface becomes enabled by system management after having been administratively disabled.

See RQ_COR_1231

RQ_000_1274 Process Invalid SA Syntax
RFC2462 5.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
If stateless address autoconfiguration is to function successfully, an IPv6 MUST NOT permit an interface to be configured with an identifier of more than 118 bits in length.
Specification Text:
A link-local address is formed by prepending the well-known link- local prefix FE80::0 [RFC2373] (of appropriate length) to the interface identifier. If the interface identifier has a length of N bits, the interface identifier replaces the right-most N zero bits of the link-local prefix. **If the interface identifier is more than 118 bits in length, autoconfiguration fails and manual configuration is required. Note that interface identifiers will typically be 64-bits long and based on EUI-64 identifiers as described in RFC2373**.

RQ_000_1276 Form Link-local Address
RFC2462 5.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When assigning a link-local address to an interface, an IPv6 node MUST set infinite preferred and a valid lifetime for the address.
Specification Text:
A link-local address has an infinite preferred and an infinite valid lifetime; it is never timed out.

RQ_000_1277 Stateless Autoconfiguration
RFC2462 5.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT perform Duplicate Address Detection on anycast addresses.
Specification Text:
Duplicate Address Detection is performed on unicast addresses prior to assigning them to an interface whose DupAddrDetectTransmits variable is greater than zero. Duplicate Address Detection MUST take place on all unicast addresses, regardless of whether they are obtained through stateful, stateless or manual configuration, with the exception of the following cases:

- **Duplicate Address Detection MUST NOT be performed on anycast addresses.**

- Each individual unicast address SHOULD be tested for uniqueness. However, when stateless address autoconfiguration is used, address uniqueness is determined solely by the interface identifier, assuming that subnet prefixes are assigned correctly (i.e., if all of an interface's addresses are generated from the same identifier, either all addresses or none of them will be duplicates). Thus, for a set of addresses formed from the same interface identifier, it is sufficient to check that the link-local address generated from the identifier is unique on the link. In such cases, the link-local address MUST be tested for uniqueness, and if no duplicate address is detected, an implementation MAY choose to skip Duplicate Address Detection for additional addresses derived from the same interface identifier.

RQ_000_1279 Stateless Autoconfiguration
RFC2462 5.4.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST ensure that an interface is configured to join the all-nodes multicast address and the solicited-node multicast address of its tentative address before it sends a Neighbor Solicitation message on that interface.
Specification Text:
Before sending a Neighbor Solicitation, an interface MUST join the all-nodes multicast address and the solicited-node multicast address of the tentative address. The former insures that the node receives Neighbor Advertisements from other nodes already using the address; the latter insures that two nodes attempting to use the same address simultaneously detect each other's presence.

RQ_000_1280 Detect Duplicate Address (DAD)
RFC2462 5.4.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When an IPv6 node sends a Neighbor Solicitation message, it MUST set the Target Address field in the message to the tentative address being checked, the Source Address field in the IPv6 Header to the Unspecified Address value 0:0 and the Destination Address field in the IPv6 Header to the solicited-node multicast address of the target address.
Specification Text:
To check an address, a node sends DupAddrDetectTransmits Neighbor Solicitations, each separated by RetransTimer milliseconds. **The solicitation's Target Address is set to the address being checked, the IP source is set to the unspecified address and the IP destination is set to the solicited-node multicast address of the target address**.

RQ_000_1281 Duplicate Address Detection Timers and Counters
RFC2462 5.4.2 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When initializing an interface an IPv6 node SHOULD send the first Neighbor Solicitation message after a random delay of between 0 and 1 seconds.
Specification Text:
If the Neighbor Solicitation is the first message to be sent from an interface after interface (re)initialization, the node should delay sending the message by a random delay between 0 and MAX_RTR_SOLICITATION_DELAY as specified in RFC2461. This serves to alleviate congestion when many nodes start up on the link at the same time, such as after a power failure, and may help to avoid race conditions when more than one node is trying to solicit for the same address at the same time. In order to improve the robustness of the Duplicate Address Detection algorithm, an interface MUST receive and process datagrams sent to the all-nodes multicast address or solicited-node multicast address of the tentative address while delaying transmission of the initial Neighbor Solicitation.

RQ_000_1282 Detect Duplicate Address (DAD)
RFC2462 5.4.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST receive and process datagrams sent to the all-nodes multicast address or solicited-node multicast address of the tentative address while delaying before sending the first Neighbor Solicitation on newly initialized interface.
Specification Text:
If the Neighbor Solicitation is the first message to be sent from an interface after interface (re)initialization, the node should delay sending the message by a random delay between 0 and MAX_RTR_SOLICITATION_DELAY as specified in RFC2461. This serves to alleviate congestion when many nodes start up on the link at the same time, such as after a power failure, and may help to avoid race conditions when more than one node is trying to solicit for the same address at the same time. **In order to improve the robustness of the Duplicate Address Detection algorithm, an interface MUST receive and process datagrams sent to the all-nodes multicast address or solicited-node multicast address of the tentative address while delaying transmission of the initial Neighbor Solicitation**.

RQ_000_1284 Detect Duplicate Address (DAD)
RFC2462 5.4.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a neighbor Solicitation message in which the Target Address field is set to the tentative address which has been assigned by the receiving node to one of its interfaces.
Requirement:
The IPv6 node MUST NOT respond to the Neighbor Solicitation message
Specification Text:
On receipt of a valid Neighbor Solicitation message on an interface, node behavior depends on whether the target address is tentative or not. If the target address is not tentative (i.e., it is assigned to the receiving interface), the solicitation is processed as described in RFC2461. If the target address is tentative, and the source address is a unicast address, the solicitation's sender is performing address resolution on the target; the solicitation should be silently ignored. Otherwise, processing takes place as described below. **In all cases, a node MUST NOT respond to a Neighbor Solicitation for a tentative address**.

RQ_000_1285 Detect Duplicate Address (DAD)
RFC2462 5.4.3 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 node receives a Neighbor Solicitation message with the Target Address field of the message set to the Tentative Address assigned by the receiving IPv6 node to one of its interfaces and the Source Address field in the IPv6 Header set to the Unspecified Address value, 0:0.
Requirement:
The IPv6 node SHOULD discard its own tentative address.
Specification Text:
On receipt of a valid Neighbor Solicitation message on an interface, node behavior depends on whether the target address is tentative or not. If the target address is not tentative (i.e., it is assigned to the receiving interface), the solicitation is processed as described in RFC2461. **If the target address is tentative**, and the source address is a unicast address, the solicitation's sender is performing address resolution on the target; the solicitation should be silently ignored. Otherwise, processing takes place as described below. In all cases, a node MUST NOT respond to a Neighbor Solicitation for a tentative address.

If the source address of the Neighbor Solicitation is the unspecified address, the solicitation is from a node performing Duplicate Address Detection. If the solicitation is from another node, the tentative address is a duplicate and should not be used (by either node). If the solicitation is from the node itself (because the node loops back multicast packets), the solicitation does not indicate the presence of a duplicate address.

RQ_000_1287 Detect Duplicate Address (DAD)
RFC2462 5.4.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a Neighbor Solicitation message from another node with the Target Address field in the message set to a tentative address for which the node is waiting to send a Neighbor Solicitation.
Requirement:
The IPv6 node MUST discard the tentative address and terminate Address Autoconfiguration.
Specification Text:
The following tests identify conditions under which a tentative address is not unique:

- **If a Neighbor Solicitation for a tentative address is received prior to having sent one, the tentative address is a duplicate. This condition occurs when two nodes run Duplicate Address Detection simultaneously, but transmit initial solicitations at different times (e.g., by selecting different random delay values before transmitting an initial solicitation).**

- If the actual number of Neighbor Solicitations received exceeds the number expected based on the loopback semantics (e.g., the interface does not loopback packet, yet one or more solicitations was received), the tentative address is a duplicate. This condition occurs when two nodes run Duplicate Address Detection simultaneously and transmit solicitations at roughly the same

RQ_000_1288 Duplicate Address Detection Timers and Counters
RFC2462 5.4.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node sending Neighbor Solicitation messages using multicast packet loopback receives more Neighbor Solicitation messages, each with the Target Address field set to the same tentative address, than the number expected based upon the loopback semantics
Requirement:
The IPv6 node MUST discard the tentative address and terminate Address Autoconfiguration.
Specification Text:
The following tests identify conditions under which a tentative address is not unique:

- If a Neighbor Solicitation for a tentative address is received prior to having sent one, the tentative address is a duplicate. This condition occurs when two nodes run Duplicate Address Detection simultaneously, but transmit initial solicitations at different times (e.g., by selecting different random delay values before transmitting an initial solicitation).

- **If the actual number of Neighbor Solicitations received exceeds the number expected based on the loopback semantics (e.g., the interface does not loopback packet, yet one or more solicitations was received), the tentative address is a duplicate. This condition occurs when two nodes run Duplicate Address Detection simultaneously and transmit solicitations at roughly the same**

RQ_000_1290 Detect Duplicate Address (DAD)
RFC2462 5.4.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a Neighbor Advertisement message with the Target Address field set to the tentative address assigned to the receiving interface.
Requirement:
The IPv6 node MUST discard the tentative address and terminate Address Autoconfiguration.
Specification Text:
On receipt of a valid Neighbor Advertisement message on an interface, node behavior depends on whether the target address is tentative or matches a unicast or anycast address assigned to the interface. If the target address is assigned to the receiving interface, the solicitation is processed as described in RFC2461. If the target address is tentative, the tentative address is not unique.

RQ_000_1291 Detect Duplicate Address (DAD)
RFC2462 5.4.5 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node using Duplicate Address Discovery (DAD) determines that a tentative address is duplicated in another node.
Requirement:
The IPv6 node SHOULD record the duplicate address as an error in the a system management log.
Specification Text:
A tentative address that is determined to be a duplicate as described above, MUST NOT be assigned to an interface and the node SHOULD log a system management error. If the address is a link-local address formed from an interface identifier, the interface SHOULD be disabled.

RQ_000_1292 Assign Global Address
RFC2462 5.5 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST support the stateless address autoconfiguration mechanism as the default method for constructing valid global addresses.
Specification Text:
Global and site-local addresses are formed by appending an interface identifier to a prefix of appropriate length. Prefixes are obtained from Prefix Information options contained in Router Advertisements. Creation of global and site-local addresses and configuration of other parameters as described in this section SHOULD be locally configurable. **However, the processing described below MUST be enabled by default.**

RQ_000_1294 Assign Global Address
RFC2462 5.5.2 RECOMMENDED
Applies to: Host
Context:
An IPv6 host has determined that there are no routers available on a link for which global addresses need to be established.
Requirement:
The IPv6 host SHOULD invoke stateful address autoconfiguration, DHCPv6, to obtain the necessary information for establishing global addresses.
Specification Text:
If a link has no routers, a host MUST attempt to use stateful autoconfiguration to obtain addresses and other configuration information. An implementation MAY provide a way to disable the invocation of stateful autoconfiguration in this case, but the default SHOULD be enabled.

RQ_000_1296 Use of M-bit
RFC2462 5.5.3 RECOMMENDED
Applies to: Host
Context:
An IPv6 host is not executing the stateful address autoconfiguration protocol, DHCPv6, when it receives a Router Advertisement message in which the M field is set to the boolean value TRUE.
Requirement:
The IPv6 host SHOULD invoke the stateful address autoconfiguration protocol, DHCPv6, to request address and other information.
Specification Text:
On receipt of a valid Router Advertisement (as defined in RFC2461), a host copies the value of the advertisement's M bit into ManagedFlag. If the value of ManagedFlag changes from FALSE to TRUE, and the host is not already running the stateful address autoconfiguration protocol, the host should invoke the stateful address autoconfiguration protocol, requesting both address information and other information. If the value of the ManagedFlag changes from TRUE to FALSE, the host should continue running the stateful address autoconfiguration, i.e., the change in the value of the ManagedFlag has no effect. If the value of the flag stays unchanged, no special action takes place. In particular, a host MUST NOT reinvoke stateful address configuration if it is already participating in the stateful protocol as a result of an earlier advertisement.

RQ_000_1297 Use of M-bit
RFC2462 5.5.3 RECOMMENDED
Applies to: Host
Context:
An IPv6 host is executing the stateful address autoconfiguration protocol, DHCPv6, when it receives a Router Advertisement in which the M field is set to the boolean value FALSE.
Requirement:
The IPv6 host SHOULD continue running the stateful address autoconfiguration protocol, DHCPv6.
Specification Text:
On receipt of a valid Router Advertisement (as defined in RFC2461), a host copies the value of the advertisement's M bit into ManagedFlag. If the value of ManagedFlag changes from FALSE to TRUE, and the host is not already running the stateful address autoconfiguration protocol, the host should invoke the stateful address autoconfiguration protocol, requesting both address information and other information. **If the value of the ManagedFlag changes from TRUE to FALSE, the host should continue running the stateful address autoconfiguration, i.e., the change in the value of the ManagedFlag has no effect**. If the value of the flag stays unchanged, no special action takes place. In particular, a host MUST NOT reinvoke stateful address configuration if it is already participating in the stateful protocol as a result of an earlier advertisement.

RQ_000_1298 Use of M-bit
RFC2462 5.5.3 MANDATORY
Applies to: Host
Context:
An IPv6 host is executing stateless address autoconfiguration when it receives a Router Advertisement in which the M field is set to the same boolean value as was set in the M field of the previously received Router Advertisement message.
Requirement:
The IPv6 host MUST continue running Stateless Address Autoconfiguration.
Specification Text:
On receipt of a valid Router Advertisement (as defined in RFC2461), a host copies the value of the advertisement's M bit into ManagedFlag. If the value of ManagedFlag changes from FALSE to TRUE, and the host is not already running the stateful address autoconfiguration protocol, the host should invoke the stateful address autoconfiguration protocol, requesting both address information and other information. If the value of the ManagedFlag changes from TRUE to FALSE, the host should continue running the stateful address autoconfiguration, i.e., the change in the value of the ManagedFlag has no effect. **If the value of the flag stays unchanged, no special action takes place**. In particular, a host MUST NOT reinvoke stateful address configuration if it is already participating in the stateful protocol as a result of an earlier advertisement.

RQ_000_1299 Use of M-bit
RFC2462 5.5.3 MANDATORY
Applies to: Host
Context:
An IPv6 host is executing the stateful address autoconfiguration protocol, DHCPv6, when it receives a Router Advertisement in which the M field is set to the same boolean value as was set in the M field of the previously received Router Advertisement message.
Requirement:
The IPv6 host MUST continue running the Stateful address autoconfiguration protocol, DHCPv6.
Specification Text:
On receipt of a valid Router Advertisement (as defined in RFC2461), a host copies the value of the advertisement's M bit into ManagedFlag. If the value of ManagedFlag changes from FALSE to TRUE, and the host is not already running the stateful address autoconfiguration protocol, the host should invoke the stateful address autoconfiguration protocol, requesting both address information and other information. If the value of the ManagedFlag changes from TRUE to FALSE, the host should continue running the stateful address autoconfiguration, i.e., the change in the value of the ManagedFlag has no effect. **If the value of the flag stays unchanged, no special action takes place. In particular, a host MUST NOT reinvoke stateful address configuration if it is already participating in the stateful protocol as a result of an earlier advertisement**.

RQ_000_1300 Use of O-Flag
RFC2462 5.5.3 RECOMMENDED
Applies to: Host
Context:
An IPv6 host is executing Stateless Address Autoconfiguration when it receives a Router Advertisement message in which the O field is set to the boolean value TRUE and the M field is set to the value FALSE.
Requirement:
The IPv6 host SHOULD invoke the stateful address autoconfiguration protocol, DHCPv6, to request information other than addresses.
Specification Text:
An advertisement's O flag field is processed in an analogous manner. A host copies the value of the O flag into OtherConfigFlag. If the value of OtherConfigFlag changes from FALSE to TRUE, the host should invoke the stateful autoconfiguration protocol, requesting information (excluding addresses if ManagedFlag is set to FALSE). If the value of the OtherConfigFlag changes from TRUE to FALSE, the host should continue running the stateful address autoconfiguration protocol, i.e., the change in the value of OtherConfigFlag has no effect. If the value of the flag stays unchanged, no special action takes place. In particular, a host MUST NOT reinvoke stateful configuration if it is already participating in the stateful protocol as a result of an earlier advertisement.

RQ_000_1301 Use of O-Flag
RFC2462 5.5.3 RECOMMENDED
Applies to: Host
Context:
An IPv6 host is executing Stateless Address Autoconfiguration when it receives a Router Advertisement message in which the O field is set to the boolean value TRUE and the M field is set to the value TRUE.
Requirement:
The IPv6 host SHOULD invoke the stateful address autoconfiguration protocol, DHCPv6, to request information including addresses.
Specification Text:
An advertisement's O flag field is processed in an analogous manner. A host copies the value of the O flag into OtherConfigFlag. If the value of OtherConfigFlag changes from FALSE to TRUE, the host should invoke the stateful autoconfiguration protocol, requesting information (excluding addresses if ManagedFlag is set to FALSE). If the value of the OtherConfigFlag changes from TRUE to FALSE, the host should continue running the stateful address autoconfiguration protocol, i.e., the change in the value of OtherConfigFlag has no effect. If the value of the flag stays unchanged, no special action takes place. In particular, a host MUST NOT reinvoke stateful configuration if it is already participating in the stateful protocol as a result of an earlier advertisement.

RQ_000_1302 Use of O-Flag
RFC2462 5.5.3 RECOMMENDED
Applies to: Host
Context:
An IPv6 host is executing the stateful address autoconfiguration protocol, DHCPv6, when it receives a Router Advertisement message in which the O field is set to the boolean value FALSE.
Requirement:
The IPv6 host SHOULD continue running the stateful address autoconfiguration protocol, DHCPv6.
Specification Text:
An advertisement's O flag field is processed in an analogous manner. A host copies the value of the O flag into OtherConfigFlag. If the value of OtherConfigFlag changes from FALSE to TRUE, the host should invoke the stateful autoconfiguration protocol, requesting information (excluding addresses if ManagedFlag is set to FALSE). **If the value of the OtherConfigFlag changes from TRUE to FALSE, the host should continue running the stateful address autoconfiguration protocol, i.e., the change in the value of OtherConfigFlag has no effect**. If the value of the flag stays unchanged, no special action takes place. In particular, a host MUST NOT reinvoke stateful configuration if it is already participating in the stateful protocol as a result of an earlier advertisement.

RQ_000_1303 Use of O-Flag
RFC2462 5.5.3 MANDATORY
Applies to: Host
Context:
An IPv6 host is executing stateless address autoconfiguration when it receives a Router Advertisement in which the O field is set to the same boolean value as was set in the O field of the previously received Router Advertisement message.

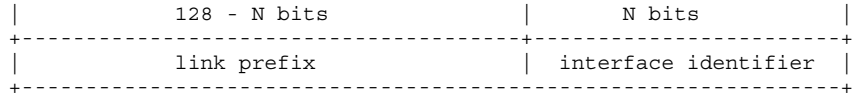
Requirement:
The IPv6 host MUST continue running Stateless Address Autoconfiguration.
Specification Text:
An advertisement's O flag field is processed in an analogous manner. A host copies the value of the O flag into OtherConfigFlag. If the value of OtherConfigFlag changes from FALSE to TRUE, the host should invoke the stateful autoconfiguration protocol, requesting information (excluding addresses if ManagedFlag is set to FALSE). If the value of the OtherConfigFlag changes from TRUE to FALSE, the host should continue running the stateful address autoconfiguration protocol, i.e., the change in the value of OtherConfigFlag has no effect. **If the value of the flag stays unchanged, no special action takes place**. In particular, a host MUST NOT reinvoke stateful configuration if it is already participating in the stateful protocol as a result of an earlier advertisement.

RQ_000_1304 Use of O-Flag
RFC2462 5.5.3 MANDATORY
Applies to: Host
Context:
An IPv6 host is executing the stateful address autoconfiguration protocol, DHCPv6, when it receives a Router Advertisement in which the O field is set to the same boolean value as was set in the O field of the previously received Router Advertisement message.
Requirement:
The IPv6 host MUST continue running the stateful address autoconfiguration protocol, DHCPv6
Specification Text:
An advertisement's O flag field is processed in an analogous manner. A host copies the value of the O flag into OtherConfigFlag. If the value of OtherConfigFlag changes from FALSE to TRUE, the host should invoke the stateful autoconfiguration protocol, requesting information (excluding addresses if ManagedFlag is set to FALSE). If the value of the OtherConfigFlag changes from TRUE to FALSE, the host should continue running the stateful address autoconfiguration protocol, i.e., the change in the value of OtherConfigFlag has no effect. **If the value of the flag stays unchanged, no special action takes place. In particular, a host MUST NOT reinvoke stateful configuration if it is already participating in the stateful protocol as a result of an earlier advertisement**.

RQ_000_1305 Process the Prefix Information Option
RFC2462 5.5.3 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a Router Advertisement message containing a Prefix-Information option in which the A (autonomous) field is set to the boolean value FALSE.
Requirement:
The IPv6 host MUST silently ignore the Prefix-Information Option.
Specification Text:
For each Prefix-Information option in the Router Advertisement:

a) If the Autonomous flag is not set, silently ignore the Prefix Information option.
b) If the prefix is the link-local prefix, silently ignore the Prefix Information option.
c) If the preferred lifetime is greater than the valid lifetime, silently ignore the Prefix Information option. A node MAY wish to log a system management error in this case.

d) If the prefix advertised does not match the prefix of an address already in the list, and the Valid Lifetime is not 0, form an address (and add it to the list) by combining the advertised prefix with the link's interface identifier as follows:



RQ_000_1306 Process the Prefix Information Option
RFC2462 5.5.3 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a Router Advertisement message containing a Prefix-Information option in which the contents of the Prefix field is set to the IPv6 link-local prefix (FE80::)
Requirement:
The IPv6 host MUST silently ignore the Prefix-Information Option.
Specification Text:
For each Prefix-Information option in the Router Advertisement:

a) If the Autonomous flag is not set, silently ignore the Prefix Information option.
b) If the prefix is the link-local prefix, silently ignore the Prefix Information option.
c) If the preferred lifetime is greater than the valid lifetime, silently ignore the Prefix Information option. A node MAY wish to log a system management error in this case.

d) If the prefix advertised does not match the prefix of an address already in the list, and the Valid Lifetime is not 0, form an address (and add it to the list) by combining the advertised prefix with the link's interface identifier as follows:

128 - N bits	N bits
link prefix	interface identifier

RQ_000_1307 Process the Prefix Information Option
RFC2462 5.5.3 MANDATORY
Applies to: Host
Context:
An IPv6 host receives a Router Advertisement message containing a Prefix-Information option in which the Preferred Lifetime field is set to a value greater than the value set in the Valid Lifetime field
Requirement:
The IPv6 host MUST silently ignore the Prefix Information Option.
Specification Text:
For each Prefix-Information option in the Router Advertisement:

a) If the Autonomous flag is not set, silently ignore the Prefix Information option.
b) If the prefix is the link-local prefix, silently ignore the Prefix Information option.
c) If the preferred lifetime is greater than the valid lifetime, silently ignore the Prefix Information option. A node MAY wish to log a system management error in this case.

d) If the prefix advertised does not match the prefix of an address already in the list, and the Valid Lifetime is not 0, form an address (and add it to the list) by combining the advertised prefix with the link's interface identifier as follows:

128 - N bits	N bits
link prefix	interface identifier

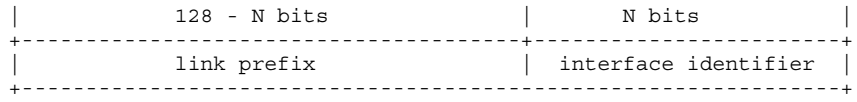
RQ_000_1308 Process the Prefix Information Option
RFC2462 5.5.3 OPTIONAL
Applies to: Host
Context:
An IPv6 host receives a Router Advertisement message containing a Prefix-Information option in which the Preferred Lifetime field is set to a value greater than the value set in the Valid Lifetime field
Requirement:
The IPv6 host MAY record the inconsistency between Preferred and Valid Lifetimes as an error in its system management log.

Specification Text:

For each Prefix-Information option in the Router Advertisement:

a) If the Autonomous flag is not set, silently ignore the Prefix Information option.
b) If the prefix is the link-local prefix, silently ignore the Prefix Information option.
c) If the preferred lifetime is greater than the valid lifetime, silently ignore the Prefix Information option. A node MAY wish to log a system management error in this case.

d) If the prefix advertised does not match the prefix of an address already in the list, and the Valid Lifetime is not 0, form an address (and add it to the list) by combining the advertised prefix with the link's interface identifier as follows:



RQ_000_1309 Process the Prefix Information Option

RFC2462 5.5.3 MANDATORY

Applies to: Host

Context:

An IPv6 host receives a Router Advertisement message containing a Prefix-Information option in which the Prefix field is set to a value which does not match the prefix of a global address already assigned by the host and the Valid Lifetime field is not set to the value zero (0).

Requirement:

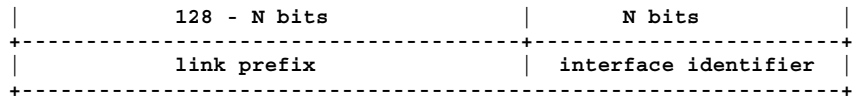
The IPv6 host MUST form a global address by combining the content of the received Prefix field (in the high order bits of the address) with the interface identifier of the link (in the low order bits) on which the Router Advertisement was received and assign the global address to that link if the length of the constructed global address is exactly 128 bits.

Specification Text:

For each Prefix-Information option in the Router Advertisement:

a) If the Autonomous flag is not set, silently ignore the Prefix Information option.
b) If the prefix is the link-local prefix, silently ignore the Prefix Information option.
c) If the preferred lifetime is greater than the valid lifetime, silently ignore the Prefix Information option. A node MAY wish to log a system management error in this case.

d) If the prefix advertised does not match the prefix of an address already in the list, and the Valid Lifetime is not 0, form an address (and add it to the list) by combining the advertised prefix with the link's interface identifier as follows:



RQ_000_1310 Process the Prefix Information Option

RFC2462 5.5.3 MANDATORY

Applies to: Host

Context:

An IPv6 host receives a Router Advertisement message containing a Prefix-Information option in which the Prefix field is set to a value which does not match the prefix of a global address already assigned by the host and the Valid Lifetime field is not set to the value zero (0).

Requirement:

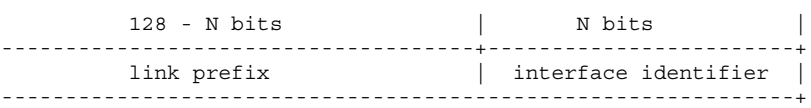
The IPv6 host MUST form a global address by combining the content of the received Prefix field (in the high order bits of the address) with the interface identifier of the link (in the low order bits) on which the Router Advertisement was received and then ignore the Prefix-Information option if the length of the constructed global address is not exactly 128 bits.

Specification Text:

For each Prefix-Information option in the Router Advertisement:

. . . .

d) If the prefix advertised does not match the prefix of an address already in the list, and the Valid Lifetime is not 0, form an address (and add it to the list) by combining the advertised prefix with the link's interface identifier as follows:



If the sum of the prefix length and interface identifier length does not equal 128 bits, the Prefix Information option MUST be ignored. An implementation MAY wish to log a system management error in this case. It is the responsibility of the system administrator to insure that the lengths of prefixes contained in Router Advertisements are consistent with the length of interface identifiers for that link type. Note that interface identifiers will typically be 64-bits long and based on EUI-64 identifiers as described in RFC2373.

RQ_000_1311 Process the Prefix Information Option

RFC2462 5.5.3 OPTIONAL

Applies to: Host

Context:

An IPv6 host receives a Router Advertisement message containing a Prefix-Information option in which the Prefix field is set to a value which does not match the prefix of a global address already assigned by the host and the Valid Lifetime field is not set to the value zero (0). However, the length of the constructed global address (Prefix plus interface identifier) is not exactly 128 bits long.

Requirement:

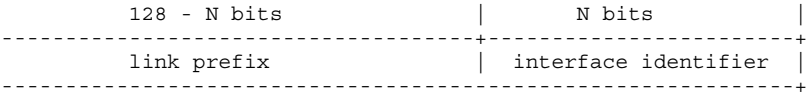
The IPv6 host MAY record an appropriate error in its system management log.

Specification Text:

For each Prefix-Information option in the Router Advertisement:

. . . .

d) If the prefix advertised does not match the prefix of an address already in the list, and the Valid Lifetime is not 0, form an address (and add it to the list) by combining the advertised prefix with the link's interface identifier as follows:



If the sum of the prefix length and interface identifier length does not equal 128 bits, the Prefix Information option MUST be ignored. An implementation MAY wish to log a system management error in this case. It is the responsibility of the system administrator to insure that the lengths of prefixes contained in Router Advertisements are consistent with the length of interface identifiers for that link type. Note that interface identifiers will typically be 64-bits long and based on EUI-64 identifiers as described in RFC2373.

RQ_000_1313 Process the Prefix Information Option

RFC2462 5.5.3 MANDATORY

Applies to: Host

Context:

An IPv6 host receives a Router Advertisement message containing a Prefix-Information option in which the content of the Prefix field matches the prefix of a previously autoconfigured address on the same interface and the value set in the Valid Lifetime field represents a time which is either greater than 2 hours or greater than the remaining lifetime associated with the address.

Requirement:

The IPv6 host MUST set the current lifetime associated with the autoconfigured address to the value set in the Valid Lifetime field in the Prefix-Information option of the received Router Advertisement message.

Specification Text:

For each Prefix-Information option in the Router Advertisement:

. . . .

e) If the advertised prefix matches the prefix of an autoconfigured address (i.e., one obtained via stateless or stateful address autoconfiguration) in the list of addresses associated with the interface, the specific action to perform depends on the Valid Lifetime in the received advertisement and the Lifetime associated with the previously autoconfigured address (which we call StoredLifetime in the discussion that follows):

1) If the received Lifetime is greater than 2 hours or greater than StoredLifetime, update the stored Lifetime of the corresponding address.

2) If the StoredLifetime is less than or equal to 2 hours and the received Lifetime is less than or equal to StoredLifetime, ignore the prefix, unless the Router Advertisement from which this Prefix Information option was obtained has been authenticated (e.g., via IPSec [RFC2402]). If the Router advertisement was authenticated, the StoredLifetime should be set to the Lifetime in the received option.

3) Otherwise, reset the stored Lifetime in the corresponding address to two hours.

RQ_000_1315 Process the Prefix Information Option

RFC2462 5.5.3 MANDATORY

Applies to: Host

Context:

An IPv6 host receives an unauthenticated Router Advertisement message containing a Prefix-Information option in which the content of the Prefix field matches the prefix of a previously autoconfigured address on the same interface and the value set in the Valid Lifetime field represents a time which is less than or equal to the remaining lifetime associated with the address which. itself, is less than or equal to 2 hours.

Requirement:

The IPv6 host MUST ignore the Prefix-Information Option.

Specification Text:

For each Prefix-Information option in the Router Advertisement:

. . . .

e) If the advertised prefix matches the prefix of an autoconfigured address (i.e., one obtained via stateless or stateful address autoconfiguration) in the list of addresses associated with the interface, the specific action to perform depends on the Valid Lifetime in the received advertisement and the Lifetime associated with the previously autoconfigured address (which we call StoredLifetime in the discussion that follows):

1) If the received Lifetime is greater than 2 hours or greater than StoredLifetime, update the stored Lifetime of the corresponding address.

2) If the StoredLifetime is less than or equal to 2 hours and the received Lifetime is less than or equal to StoredLifetime, ignore the prefix, unless the Router Advertisement from which this Prefix Information option was obtained has been authenticated (e.g., via IPSec [RFC2402]). If the Router advertisement was authenticated, the StoredLifetime should be set to the Lifetime in the received option.

3) Otherwise, reset the stored Lifetime in the corresponding address to two hours.

RQ_000_1316 Process the Prefix Information Option

RFC2462 5.5.3 RECOMMENDED

Applies to: Host

Context:

An IPv6 host receives an authenticated Router Advertisement message containing a Prefix-Information option in which the content of the Prefix field matches the prefix of a previously autoconfigured address on the same interface and the value set in the Valid Lifetime field represents a time which is less than or equal to the remaining lifetime associated with the address which. itself, is less than or equal to 2 hours.

Requirement:
The IPv6 host SHOULD set the current lifetime associated with the autoconfigured address to the value set in the Valid Lifetime field in the Prefix-Information option of the received Router Advertisement message.

Specification Text:
For each Prefix-Information option in the Router Advertisement:
. . . .
e) If the advertised prefix matches the prefix of an autoconfigured address (i.e., one obtained via stateless or stateful address autoconfiguration) in the list of addresses associated with the interface, the specific action to perform depends on the Valid Lifetime in the received advertisement and the Lifetime associated with the previously autoconfigured address (which we call StoredLifetime in the discussion that follows):

1) If the received Lifetime is greater than 2 hours or greater than StoredLifetime, update the stored Lifetime of the corresponding address.

2) If the StoredLifetime is less than or equal to 2 hours and the received Lifetime is less than or equal to StoredLifetime, ignore the prefix, **unless the Router Advertisement from which this Prefix Information option was obtained has been authenticated (e.g., via IPSec [RFC2402]). If the Router advertisement was authenticated, the StoredLifetime should be set to the Lifetime in the received option.**

3) Otherwise, reset the stored Lifetime in the corresponding address to two hours.

RQ_000_1317 Process the Prefix Information Option

RFC2462 5.5.3, 13 RECOMMENDED
Applies to: Host

Context:
An IPv6 host receives a Router Advertisement message containing a Prefix-Information option in which the content of the Prefix field matches the prefix of a previously autoconfigured address on the same interface and the value set in the Valid Lifetime field represents a time which is less than or equal to 2 hours the remaining lifetime associated with the address which. itself, is greater than 2 hours.

Requirement:
The IPv6 host SHOULD set the current lifetime associated with the autoconfigured address to two hours.

Specification Text:
For each Prefix-Information option in the Router Advertisement:
. . . .
e) If the advertised prefix matches the prefix of an autoconfigured address (i.e., one obtained via stateless or stateful address autoconfiguration) in the list of addresses associated with the interface, the specific action to perform depends on the Valid Lifetime in the received advertisement and the Lifetime associated with the previously autoconfigured address (which we call StoredLifetime in the discussion that follows):

1) If the received Lifetime is greater than 2 hours or greater than StoredLifetime, update the stored Lifetime of the corresponding address.

2) If the StoredLifetime is less than or equal to 2 hours and the received Lifetime is less than or equal to StoredLifetime}}, ignore the prefix, **unless the Router Advertisement from which this Prefix Information option was obtained has been authenticated (e.g., via IPSec [RFC2402]). If the Router advertisement was authenticated, the StoredLifetime should be set to the Lifetime in the received option.**

{{

3) Otherwise, reset the stored Lifetime in the corresponding address to two hours.

RQ_000_1318 Deprecated Address Use
RFC2462 5.5.4 OPTIONAL
Applies to: Host, Router
Context:
The preferred lifetime of an address associated with an interface on an IPv6 node has expired (it has become deprecated).
Requirement:
The implementation prevents any new communication from using a deprecated address.
Specification Text:
A preferred address becomes deprecated when its preferred lifetime expires. A deprecated address SHOULD continue to be used as a source address in existing communications, but SHOULD NOT be used in new communications if an alternate (non-deprecated) address is available and has sufficient scope. IP and higher layers (e.g., TCP, UDP) MUST continue to accept datagrams destined to a deprecated address since a deprecated address is still a valid address for the interface. **An implementation MAY prevent any new communication from using a deprecated address,** but system management MUST have the ability to disable such a facility, and the facility MUST be disabled by default.

An address (and its association with an interface) becomes invalid when its valid lifetime expires. An invalid address MUST NOT be used as a source address in outgoing communications and MUST NOT be recognized as a destination on a receiving interface.

RQ_000_1319 Deprecated Address Use
RFC2462 5.5.4 RECOMMENDED
Applies to: Host, Router
Context:
The preferred lifetime of an address associated with an interface on an IPv6 node has expired (it has become deprecated).
Requirement:
The IPv6 node SHOULD continue to use the deprecated address only in existing communications
Specification Text:
A preferred address becomes deprecated when its preferred lifetime expires. **A deprecated address SHOULD continue to be used as a source address in existing communications, but SHOULD NOT be used in new communications if an alternate (non-deprecated) address is available and has sufficient scope.** IP and higher layers (e.g., TCP, UDP) MUST continue to accept datagrams destined to a deprecated address since a deprecated address is still a valid address for the interface. An implementation MAY prevent any new communication from using a deprecated address, but system management MUST have the ability to disable such a facility, and the facility MUST be disabled by default.

An address (and its association with an interface) becomes invalid when its valid lifetime expires. An invalid address MUST NOT be used as a source address in outgoing communications and MUST NOT be recognized as a destination on a receiving interface.

RQ_000_1320 Deprecated Address Use
RFC2462 5.5.4 MANDATORY
Applies to: Host, Router
Context:
The preferred lifetime of an address associated with an interface on an IPv6 node has expired (it has become deprecated).
Requirement:
The IPv6 node MUST accept any datagram in which the Destination Address field of the IPv6 Header is set to the deprecated address.
Specification Text:
A preferred address becomes deprecated when its preferred lifetime expires. A deprecated address SHOULD continue to be used as a source address in existing communications, but SHOULD NOT be used in new communications if an alternate (non-deprecated) address is available and has sufficient scope. **IP and higher layers (e.g., TCP, UDP) MUST continue to accept datagrams destined to a deprecated address since a deprecated address is still a valid address for the interface**. An implementation MAY prevent any new communication from using a deprecated address, but system management MUST have the ability to disable such a facility, and the facility MUST be disabled by default.

An address (and its association with an interface) becomes invalid when its valid lifetime expires. An invalid address MUST NOT be used as a source address in outgoing communications and MUST NOT be recognized as a destination on a receiving interface.

RQ_000_1321 Invalid Address
RFC2462 5.5.4 MANDATORY
Applies to: Router, Host
Context:
The valid lifetime of an address associated with an interface on an IPv6 node has expired (it has become invalid).
Requirement:
The IPv6 node MUST NOT use the invalid address in the Source Address field in the header of an outgoing IPv6 packet.
Specification Text:
A preferred address becomes deprecated when its preferred lifetime expires. A deprecated address SHOULD continue to be used as a source address in existing communications, but SHOULD NOT be used in new communications if an alternate (non-deprecated) address is available and has sufficient scope. IP and higher layers (e.g., TCP, UDP) MUST continue to accept datagrams destined to a deprecated address since a deprecated address is still a valid address for the interface. An implementation MAY prevent any new communication from using a deprecated address, but system management MUST have the ability to disable such a facility, and the facility MUST be disabled by default.

An address (and its association with an interface) becomes invalid when its valid lifetime expires. **An invalid address MUST NOT be used as a source address in outgoing communications** and MUST NOT be recognized as a destination on a receiving interface.

RQ_000_1322 Invalid Address
RFC2462 5.5.4 MANDATORY
Applies to: Router, Host
Context:
The valid lifetime of an address associated with an interface on an IPv6 node has expired (it has become invalid).
Requirement:
The IPv6 node MUST NOT accept an IPv6 packet in which the Destination Address field in the header is set to the invalid address.
Specification Text:
A preferred address becomes deprecated when its preferred lifetime expires. A deprecated address SHOULD continue to be used as a source address in existing communications, but SHOULD NOT be used in new communications if an alternate (non-deprecated) address is available and has sufficient scope. IP and higher layers (e.g., TCP, UDP) MUST continue to accept datagrams destined to a deprecated address since a deprecated address is still a valid address for the interface. An implementation MAY prevent any new communication from using a deprecated address, but system management MUST have the ability to disable such a facility, and the facility MUST be disabled by default.

An address (and its association with an interface) becomes invalid when its valid lifetime expires. **An invalid address** MUST NOT be used as a source address in outgoing communications and **MUST NOT be recognized as a destination on a receiving interface.**

RQ_000_1324 Simultaneous Stateless and Stateful Autoconfiguration
RFC2462 5.6 MANDATORY
Applies to: Host
Context:
An IPv6 host has received information using Stateless Address Autoconfiguration which is inconsistent with information received using the stateful address autoconfiguration protocol DHCPv6
Requirement:
The IPv6 host MUST use the most recently received address information regardless of whether it was obtained using Stateless Address Autoconfiguration or DHCPv6.
Specification Text:
It is possible for hosts to obtain address information using both stateless and stateful protocols since both may be enabled at the same time. It is also possible that the values of other configuration parameters such as MTU size and hop limit will be learned from both Router Advertisements and the stateful autoconfiguration protocol. If the same configuration information is provided by multiple sources, the value of this information should be consistent. However, it is not considered a fatal error if information received from multiple sources is inconsistent. Hosts accept the union of all information received via the stateless and stateful protocols. **If inconsistent information is learned different sources, the most recently obtained values always have precedence over information learned earlier**.

RQ_000_1326 Detect Duplicate Address (DAD)
RFC2462 6 OPTIONAL
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MAY use authenticated [RFC2402] Neighbor Discovery packets.
Specification Text:
The use of Duplicate Address Detection opens up the possibility of denial of service attacks. Any node can respond to Neighbor Solicitations for a tentative address, causing the other node to reject the address as a duplicate. This attack is similar to other attacks involving the spoofing of Neighbor Discovery messages and can be addressed by requiring that Neighbor Discovery packets be authenticated [RFC2402].

RQ_000_9013 Manual Address Configuration
RFC2462 4 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
Using Duplicate Address Detection (DAD), an IPv6 node SHOULD verify the uniqueness of each address assigned manually to each of its interfaces.
Specification Text:
For safety, all addresses must be tested for uniqueness prior to their assignment to an interface. In the case of addresses created through stateless autoconfig, however, the uniqueness of an address is determined primarily by the portion of the address formed from an interface identifier. Thus, if a node has already verified the uniqueness of a link-local address, additional addresses created from the same interface identifier need not be tested individually. **In contrast, all addresses obtained manually or via stateful address autoconfiguration should be tested for uniqueness individually.** To accommodate sites that believe the overhead of performing Duplicate Address Detection outweighs its benefits, the use of Duplicate Address Detection can be disabled through the administrative setting of a per-interface configuration flag.

RQ_000_9022 Detect Duplicate Address (DAD)
RFC2462 5.4.5 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node using Duplicate Address Discovery (DAD) determines that a tentative address is duplicated in another node.
Requirement:
The IPv6 node MUST NOT assign the duplicated tentative address to an interface.
Specification Text:
A tentative address that is determined to be a duplicate as described above, MUST NOT be assigned to an interface and the node SHOULD log a system management error. If the address is a link-local address formed from an interface identifier, the interface SHOULD be disabled.

RQ_000_9023 Stateless Autoconfiguration
RFC2462 5.4.5 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node using Duplicate Address Discovery (DAD) determines that a tentative link-local address is duplicated in another node.
Requirement:
The IPv6 node SHOULD disable the interface associated with the duplicated link-local address.
Specification Text:
A tentative address that is determined to be a duplicate as described above, MUST NOT be assigned to an interface and the node SHOULD log a system management error. ((If the address is a link-local address formed from an interface identifier, the interface SHOULD be disabled}}.

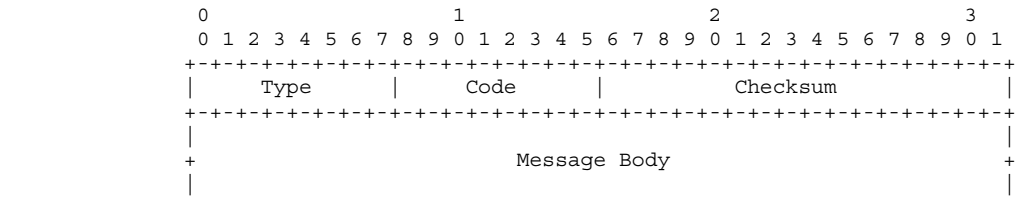
RQ_000_9026 Detect Duplicate Address (DAD)
RFC2462 5.4 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node has sent the configured number of Neighbor Solicitation messages with a specific tentative address set in the Target Address field of each message and has received no neighbor Advertisement messages in response.
Requirement:
The IPv6 node SHOULD process the tentative address as unique.
Specification Text:
The following subsections describe specific tests a node performs to verify an address's uniqueness. **An address is considered unique if none of the tests indicate the presence of a duplicate address within RetransTimer milliseconds after having sent DupAddrDetectTransmits Neighbor Solicitations. Once an address is determined to be unique, it may be assigned to an interface**.

4.8 Requirements extracted from RFC 2463

RQ_000_1404 Generate ICMPv6 Messages
RFC2463 2.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST set the Next Header field to the value 58 (fifty-eight) in the IPv6 header or IPv6 Extension Header immediately preceding an ICMPv6 header
Specification Text:
Every ICMPv6 message is preceded by an IPv6 header and zero or more IPv6 extension headers. The ICMPv6 header is identified by a Next Header value of 58 in the immediately preceding header. (NOTE: this is different than the value used to identify ICMP for IPv4.)

The ICMPv6 messages have the following general format:



The type field indicates the type of the message. Its value determines the format of the remaining data.

The code field depends on the message type. It is used to create an additional level of message granularity.

The checksum field is used to detect data corruption in the ICMPv6 message and parts of the IPv6 header.

RQ_000_1406 Determine ICMPv6 Message Source Address
RFC2463 2.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node having more than one unicast address receives a packet sent to one of these unicast addresses which causes an ICMPv6 message to be sent as a response.
Requirement:
The IPv6 node MUST use the unicast address to which the incoming message was sent as the Source IPv6 Address when calculating the value to be inserted in the Checksum field of the ICMPv6 response.
Specification Text:
A node that sends an ICMPv6 message has to determine both the Source and Destination IPv6 Addresses in the IPv6 header before calculating the checksum. **If the node has more than one unicast address, it must choose the Source Address of the message as follows:**

(a) **If the message is a response to a message sent to one of the node's unicast addresses, the Source Address of the reply must be that same address.**

(b) If the message is a response to a message sent to a multicast or anycast group in which the node is a member, the Source Address of the reply must be a unicast address belonging to the interface on which the multicast or anycast packet was received.
(c) If the message is a response to a message sent to an address that does not belong to the node, the Source Address should be that unicast address belonging to the node that will be most helpful in diagnosing the error. For example, if the message is a response to a packet forwarding action that cannot complete successfully, the Source Address should be a unicast address belonging to the interface on which the packet forwarding failed.
(d) Otherwise, the node's routing table must be examined to determine which interface will be used to transmit the message to its destination, and a unicast address belonging to that interface must be used as the Source Address of the message.

RQ_000_1407 Determine ICMPv6 Message Source Address

RFC2463 2.2 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node having more than one unicast address receives a packet sent to an address which is not one of its own unicast addresses and the packet causes an ICMPv6 message to be sent as a response.

Requirement:

The IPv6 node MUST use one of its own unicast addresses as the IPv6 Source Address when calculating the value to be inserted in the checksum field of the ICMPv6 response message.

Specification Text:

A node that sends an ICMPv6 message has to determine both the Source and Destination IPv6 Addresses in the IPv6 header before calculating the checksum. **If the node has more than one unicast address, it must choose the Source Address of the message as follows:**

(a) If the message is a response to a message sent to one of the node's unicast addresses, the Source Address of the reply must be that same address.
(b) **If the message is a response to a message sent to a multicast or anycast group in which the node is a member, the Source Address of the reply must be a unicast address belonging to the interface on which the multicast or anycast packet was received.**
(c) If the message is a response to a message sent to an address that does not belong to the node, the Source Address should be that unicast address belonging to the node that will be most helpful in diagnosing the error. For example, if the message is a response to a packet forwarding action that cannot complete successfully, the Source Address should be a unicast address belonging to the interface on which the packet forwarding failed.
(d) Otherwise, the node's routing table must be examined to determine which interface will be used to transmit the message to its destination, and a unicast address belonging to that interface must be used as the Source Address of the message.

RQ_000_1408 Determine ICMPv6 Message Source Address

RFC2463 2.2 RECOMMENDED

Applies to: Host, Router

Context:

An IPv6 node having more than one unicast address receives a packet sent to an address which is not one of its own unicast addresses and the packet causes an ICMPv6 message to be sent as a response.

Requirement:

The IPv6 node SHOULD select a source address for use in calculating the value to be inserted in the Checksum field of the ICMPv6 response message according to the rules that would be used to select the source address for any other packet originated by the node, given the destination address of the packet

Specification Text:

A node that sends an ICMPv6 message has to determine both the Source and Destination IPv6 Addresses in the IPv6 header before calculating the checksum. **If the node has more than one unicast address, it must choose the Source Address of the message as follows:**

(a) If the message is a response to a message sent to one of the node's unicast addresses, the Source Address of the reply must be that same address.

(b) **If the message is a response to a message sent to a multicast or anycast group in which the node is a member, the Source Address of the reply must be a unicast address belonging to the interface on which the multicast or anycast packet was received.**
(c) If the message is a response to a message sent to an address that does not belong to the node, the Source Address should be that unicast address belonging to the node that will be most helpful in diagnosing the error. For example, if the message is a response to a packet forwarding action that cannot complete successfully, the Source Address should be a unicast address belonging to the interface on which the packet forwarding failed.
(d) **Otherwise, the node's routing table must be examined to determine which interface will be used to transmit the message to its destination, and a unicast address belonging to that interface must be used as the Source Address of the message.**

RQ_000_1409 Determine ICMPv6 Message Source Address
RFC2463 2.2 OPTIONAL
Applies to: Host, Router
Context:
An IPv6 node having more than one unicast address receives a packet sent to an address which is not one of its own unicast addresses and the packet causes an ICMPv6 message to be sent as a response.
Requirement:
The IPv6 node MAY select a source address for use in calculating the value to be inserted in the Checksum field of the ICMPv6 response message in away that would lead to a more informative choice of address reachable from the destination of the ICMPv6 packet.
Specification Text:
A node that sends an ICMPv6 message has to determine both the Source and Destination IPv6 Addresses in the IPv6 header before calculating the checksum. **If the node has more than one unicast address, it must choose the Source Address of the message as follows:**

(a) If the message is a response to a message sent to one of the node's unicast addresses, the Source Address of the reply must be that same address.
(b) If the message is a response to a message sent to a multicast or anycast group in which the node is a member, the Source Address of the reply must be a unicast address belonging to the interface on which the multicast or anycast packet was received.
(c) **If the message is a response to a message sent to an address that does not belong to the node, the Source Address should be that unicast address belonging to the node that will be most helpful in diagnosing the error. For example, if the message is a response to a packet forwarding action that cannot complete successfully, the Source Address should be a unicast address belonging to the interface on which the packet forwarding failed**.
(d) Otherwise, the node's routing table must be examined to determine which interface will be used to transmit the message to its destination, and a unicast address belonging to that interface must be used as the Source Address of the message.

RQ_000_1410 Compute Checksum
RFC2463 2.3 -2 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node constructs an ICMPv6 packet for transmission
Requirement:
The IPv6 node MUST calculate the value to be inserted into the Checksum field of the ICMPv6 Header as the 16-bit one's complement of the one's complement sum of the entire ICMPv6 message starting with the ICMPv6 message type field and preceded by a "pseudo-header" of IPv6 header fields, as described in RFC 2460, comprising the 128-bit Source and Destination Addresses, the ICMPv6 packet length in octets and a Next Header field set to fifty-eight (58). The Checksum field itself is assumed to be set to the value of zero (0).
Specification Text:
The checksum is the 16-bit one's complement of the one's complement sum of the entire ICMPv6 message starting with the ICMPv6 message type field, prepended with a "pseudo-header" of IPv6 header fields, as specified in RFC 2460, section 8.1. The Next Header value used in the pseudo-header is 58. (NOTE: the inclusion of a pseudo-header in the ICMPv6 checksum is a change from IPv4; see RFC 2460 for the rationale for this change.)

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

RQ_000_1411 Process ICMPv6 Error Messages
RFC2463 2.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an ICMPv6 error message of unknown type.
Requirement:
The IPv6 node MUST pass the ICMPv6 error message to the upper-layer process that originated the packet that caused the error
Specification Text:
Implementations MUST observe the following rules when processing ICMPv6 messages (from RFC-1122):

(a) If an ICMPv6 error message of unknown type is received, it MUST be passed to the upper layer.
(b) If an ICMPv6 informational message of unknown type is received, it MUST be silently discarded.
(c) Every ICMPv6 error message (type < 128) includes as much of the IPv6 offending (invoking) packet (the packet that caused the error) as will fit without making the error message packet exceed the minimum IPv6 MTU [RFC 2460].
(d) In those cases where the internet-layer protocol is required to pass an ICMPv6 error message to the upper-layer process, the upper-layer protocol type is extracted from the original packet (contained in the body of the ICMPv6 error message) and used to select the appropriate upper-layer process to handle the error.

RQ_000_1412 Process ICMPv6 Information Messages
RFC2463 2.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an ICMPv6 error message of unknown type.
Requirement:
The IPv6 node MUST silently ignore the unknown ICMPv6 message.
Specification Text:
Implementations MUST observe the following rules when processing ICMPv6 messages (from RFC-1122):

(a) If an ICMPv6 error message of unknown type is received, it MUST be passed to the upper layer.
(b) If an ICMPv6 informational message of unknown type is received, it MUST be silently discarded.
(c) Every ICMPv6 error message (type < 128) includes as much of the IPv6 offending (invoking) packet (the packet that caused the error) as will fit without making the error message packet exceed the minimum IPv6 MTU [RFC 2460].
(d) In those cases where the internet-layer protocol is required to pass an ICMPv6 error message to the upper-layer process, the upper-layer protocol type is extracted from the original packet (contained in the body of the ICMPv6 error message) and used to select the appropriate upper-layer process to handle the error.

RQ_000_1413 Generate ICMPv6 Error Messages
RFC2463 2.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST include in any ICMPv6 error message as much of the IPv6 offending (invoking) packet (the packet that caused the error) as possible without making the error message packet exceed
the minimum IPv6 MTU
Specification Text:
Implementations MUST observe the following rules when processing ICMPv6 messages (from RFC-1122):

(a) If an ICMPv6 error message of unknown type is received, it MUST be passed to the upper layer.
(b) If an ICMPv6 informational message of unknown type is received, it MUST be silently discarded.

(c) Every ICMPv6 error message (type < 128) includes as much of the IPv6 offending (invoking) packet (the packet that caused the error) as will fit without making the error message packet exceed the minimum IPv6 MTU [RFC 2460].
(d) In those cases where the internet-layer protocol is required to pass an ICMPv6 error message to the upper-layer process, the upper-layer protocol type is extracted from the original packet (contained in the body of the ICMPv6 error message) and used to select the appropriate upper-layer process to handle the error.

RQ_000_1415 Process ICMPv6 Error Messages
RFC2463 2.4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an ICMPv6 error message but the size of the original message causing the error message to be sent is such that information regarding the upper-layer protocol is not present in the returned packet information.
Requirement:
The IPv6 node MUST silently drop the ICMPv6 error message after any IPv6-layer processing.
Specification Text:
Implementations MUST observe the following rules when processing ICMPv6 messages (from RFC-1122):

(a) If an ICMPv6 error message of unknown type is received, it MUST be passed to the upper layer.
(b) If an ICMPv6 informational message of unknown type is received, it MUST be silently discarded.
(c) Every ICMPv6 error message (type < 128) includes as much of the IPv6 offending (invoking) packet (the packet that caused the error) as will fit without making the error message packet exceed the minimum IPv6 MTU [RFC 2460].
(d) In those cases where the internet-layer protocol is required to pass an ICMPv6 error message to the upper-layer process, the upper-layer protocol type is extracted from the original packet (contained in the body of the ICMPv6 error message) and used to select the appropriate upper-layer process to handle the error.

If the original packet had an unusually large amount of extension headers, it is possible that the upper-layer protocol type may not be present in the ICMPv6 message, due to truncation of the original packet to meet the minimum IPv6 MTU (RFC 2460) limit. In that case, the error message is silently dropped after any IPv6-layer processing.

RQ_000_1416 Process ICMPv6 Error Messages
RFC2463 2.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT send an ICMPv6 error message as a response to a received ICMPv6 error message.
Specification Text:
Implementations MUST observe the following rules when processing ICMPv6 messages (from [RFC-1122]):

……

(e) An ICMPv6 error message MUST NOT be sent as a result of receiving:

(e.1) an ICMPv6 error message, or

(e.2) a packet destined to an IPv6 multicast address (there are two exceptions to this rule: (1) the Packet Too Big Message - Section 3.2 - to allow Path MTU discovery to work for IPv6 multicast, and (2) the Parameter Problem Message, Code 2 - Section 3.4 - reporting an unrecognized IPv6 option that has the Option Type highest-order two bits set to 10), or

(e.3) a packet sent as a link-layer multicast, (the exception from e.2 applies to this case too), or

(e.4) a packet sent as a link-layer broadcast, (the exception from e.2 applies to this case too), or

(e.5) a packet whose source address does not uniquely identify a single node -- e.g., the IPv6 Unspecified Address, an IPv6 multicast address, or an address known by the ICMP message sender to be an IPv6 anycast address.

RQ_000_1417 Process ICMPv6 Error Messages

RFC2463 2.4 MANDATORY

Applies to: Host, Router

Context:

Requirement:

An IPv6 node MUST NOT send an ICMPv6 error message as a response to a received IPv6 packet sent to a multicast address unless it is to report a Packet Too Big Message or a Parameter Problem Message, Code 2.

Specification Text:

Implementations MUST observe the following rules when processing ICMPv6 messages (from [RFC-1122]):

……

(e) An ICMPv6 error message MUST NOT be sent as a result of receiving:

(e.1) an ICMPv6 error message, or

(e.2) a packet destined to an IPv6 multicast address (there are two exceptions to this rule: (1) the Packet Too Big Message - Section 3.2 - to allow Path MTU discovery to work for IPv6 multicast, and (2) the Parameter Problem Message, Code 2 - Section 3.4 - reporting an unrecognized IPv6 option that has the Option Type highest-order two bits set to 10), or

(e.3) a packet sent as a link-layer multicast, (the exception from e.2 applies to this case too), or

(e.4) a packet sent as a link-layer broadcast, (the exception from e.2 applies to this case too), or

(e.5) a packet whose source address does not uniquely identify a single node -- e.g., the IPv6 Unspecified Address, an IPv6 multicast address, or an address known by the ICMP message sender to be an IPv6 anycast address.

RQ_000_1419 Process ICMPv6 Error Messages

RFC2463 2.4 MANDATORY

Applies to: Host, Router

Context:

Requirement:

An IPv6 node MUST NOT send an ICMPv6 error message as a response to a received IPv6 packet sent as a link-layer multicast unless it is to report a Packet Too Big Message or a Parameter Problem Message, Code 2.

Specification Text:

Implementations MUST observe the following rules when processing ICMPv6 messages (from [RFC-1122]):

……

(e) An ICMPv6 error message MUST NOT be sent as a result of receiving:

(e.1) an ICMPv6 error message, or

(e.2) a packet destined to an IPv6 multicast address (there are two exceptions to this rule: (1) the Packet Too Big Message - Section 3.2 - to allow Path MTU discovery to work for IPv6 multicast, and (2) the Parameter Problem Message, Code 2 - Section 3.4 - reporting an unrecognized IPv6 option that has the Option Type highest-order two bits set to 10), or

(e.3) a packet sent as a link-layer multicast, (the exception from e.2 applies to this case too), or

(e.4) a packet sent as a link-layer broadcast, (the exception from e.2 applies to this case too), or

(e.5) a packet whose source address does not uniquely identify a single node -- e.g., the IPv6 Unspecified Address, an IPv6 multicast address, or an address known by the ICMP message sender to be an IPv6 anycast address.

RQ_000_1421 Process ICMPv6 Error Messages

RFC2463 2.4 MANDATORY

Applies to: Router, Host

Context:

Requirement:

An IPv6 node MUST NOT send an ICMPv6 error message as a response to a received IPv6 packet sent as a link-layer broadcast unless it is to report a Packet Too Big Message or a Parameter Problem Message, Code 2.

Specification Text:

Implementations MUST observe the following rules when processing ICMPv6 messages (from [RFC-1122]):

……

(e) An ICMPv6 error message MUST NOT be sent as a result of receiving:

(e.1) an ICMPv6 error message, or

(e.2) a packet destined to an IPv6 multicast address (there are two exceptions to this rule: (1) the Packet Too Big Message - Section 3.2 - to allow Path MTU discovery to work for IPv6 multicast, and (2) the Parameter Problem Message, Code 2 - Section 3.4 - reporting an unrecognized IPv6 option that has the Option Type highest-order two bits set to 10), or

(e.3) a packet sent as a link-layer multicast, (the exception from e.2 applies to this case too), or

(e.4) a packet sent as a link-layer broadcast, (the exception from e.2 applies to this case too), or

(e.5) a packet whose source address does not uniquely identify a single node -- e.g., the IPv6 Unspecified Address, an IPv6 multicast address, or an address known by the ICMP message sender to be an IPv6 anycast address.

RQ_000_1423 Process ICMPv6 Error Messages
RFC2463 2.4, 7, 12 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT send an ICMPv6 error message as a response to a received IPv6 packet in which the Source Address field does not uniquely identify a single node.
Specification Text:
Implementations MUST observe the following rules when processing ICMPv6 messages (from [RFC-1122]):

……

(e) An ICMPv6 error message MUST NOT be sent as a result of receiving:

(e.1) an ICMPv6 error message, or

(e.2) a packet destined to an IPv6 multicast address (there are two exceptions to this rule: (1) the Packet Too Big Message - Section 3.2 - to allow Path MTU discovery to work for IPv6 multicast, and (2) the Parameter Problem Message, Code 2 - Section 3.4 - reporting an unrecognized IPv6 option that has the Option Type highest-order two bits set to 10), or

(e.3) a packet sent as a link-layer multicast, (the exception from e.2 applies to this case too), or

(e.4) a packet sent as a link-layer broadcast, (the exception from e.2 applies to this case too), or

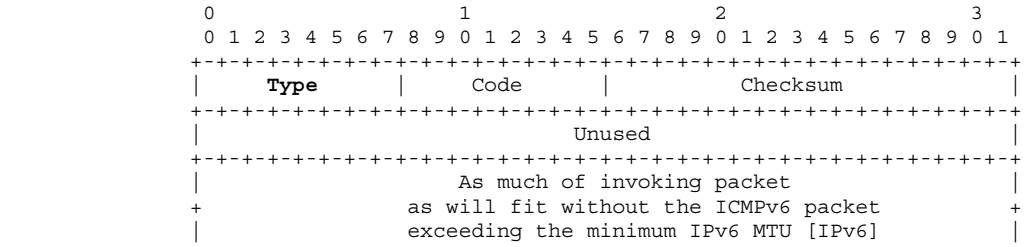
(e.5) a packet whose source address does not uniquely identify a single node -- e.g., the IPv6 Unspecified Address, an IPv6 multicast address, or an address known by the ICMP message sender to be an IPv6 anycast address.

RQ_000_1427 Limit ICMP Bandwidth and Forwarding Costs
RFC2463 2.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST control the rate at which ICMPv6 error messages are sent to a single destination.
Specification Text:
Implementations MUST observe the following rules when processing ICMPv6 messages (from [RFC-1122]):

...
(f) **Finally, in order to limit the bandwidth and forwarding costs incurred sending ICMPv6 error messages, an IPv6 node MUST limit the rate of ICMPv6 error messages it sends. This situation may occur when a source sending a stream of erroneous packets fails to heed the resulting ICMPv6 error messages.** There are a variety of ways of implementing the rate-limiting function, for example:
(f.1) Timer-based - for example, limiting the rate of transmission of error messages to a given source, or to any source, to at most once every T milliseconds.
(f.2) Bandwidth-based - for example, limiting the rate at which error messages are sent from a particular interface to some fraction F of the attached link's bandwidth. The limit parameters (e.g., T or F in the above examples) MUST be configurable for the node, with a conservative default value (e.g., T = 1 second, NOT 0 seconds, or F = 2 percent, NOT 100 percent).

RQ_000_1432 Generate Destination Unreachable Message
RFC2463 3.1 RECOMMENDED
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet which cannot be delivered to its destination address for reasons other than congestion.
Requirement:
The IPv6 router SHOULD send an ICMPv6 message to the originator of the packet with the Type field in the ICMPv6 Header set to the value 1 (Destination Unreachable).
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type **1**

Code
0 - no route to destination
1 - communication with destination administratively prohibited
2 - (not assigned)
3 - address unreachable
4 - port unreachable

Unused This field is unused for all code values. It must be initialized to zero by the sender and ignored by the receiver.

Description

A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

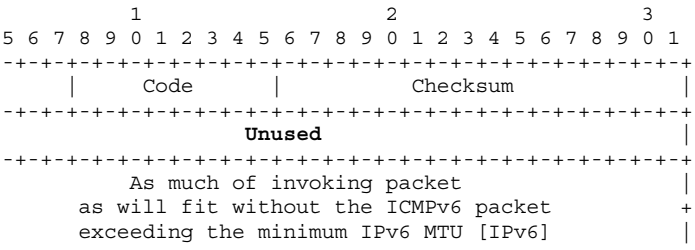
If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender.

Upper layer notification

A node receiving the ICMPv6 Destination Unreachable message MUST notify the upper-layer process.

RQ_000_1433 Process Destination Unreachable Message
RFC2463 3.1 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an ICMPv6 Destination Unreachable Message.
Requirement:
The IPv6 node MUST ignore any value set in the Unused field (octets 5 to 8) in the ICMPv6 Destination Unreachable message.
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 1

Code
0 - no route to destination
1 - communication with destination administratively prohibited
2 - (not assigned)
3 - address unreachable
4 - port unreachable

Unused **This field is unused for all code values. It must be initialized to zero by the sender and ignored by the receiver.**

Description

A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

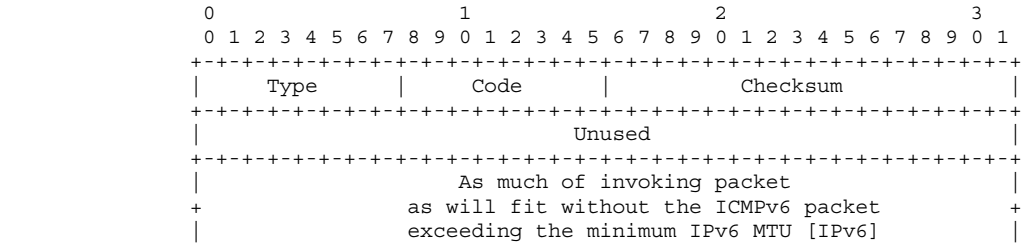
If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender.

Upper layer notification

A node receiving the ICMPv6 Destination Unreachable message MUST notify the upper-layer process.

RQ_000_1435 Generate Destination Unreachable Message
RFC2463 3.1 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet which cannot be forwarded to its Destination Address as a result of network congestion.
Requirement:
The IPv6 router MUST NOT send an ICMPv6 Destination Unreachable Message as a response to the originating node.
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 1

Code
0 - no route to destination
1 - communication with destination administratively prohibited
2 - (not assigned)
3 - address unreachable
4 - port unreachable

Unused This field is unused for all code values. It must be initialized to zero by the sender and ignored by the receiver.

Description

A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. **(An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)**

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

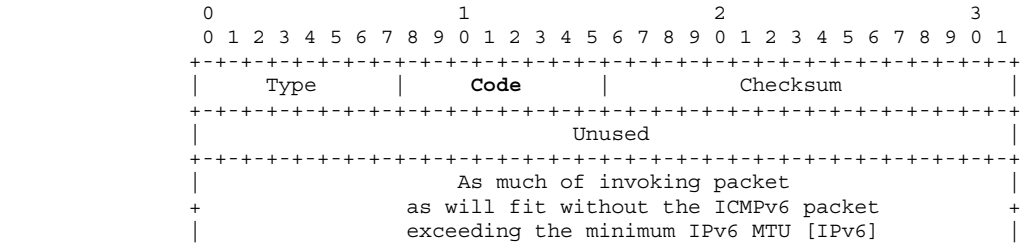
If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender.

Upper layer notification

A node receiving the ICMPv6 Destination Unreachable message MUST notify the upper-layer process.

RQ_000_1436 Destination Unreachable Code Field Value
RFC2463 3.1 MANDATORY
Applies to: Router
Context:
An IPv6 router constructs an ICMPv6 Destination Unreachable message as a response to a received IPv6 packet which cannot be delivered to its Destination Address because the router does not have a matching entry in its routing table.
Requirement:
The IPv6 router MUST set the ICMPv6 Code field to the value zero (0).
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 1

Code
0 - no route to destination
1 - communication with destination administratively prohibited
2 - (not assigned)
3 - address unreachable
4 - port unreachable

Unused This field is unused for all code values. It must be initialized to zero by the sender and ignored by the receiver.

Description

A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

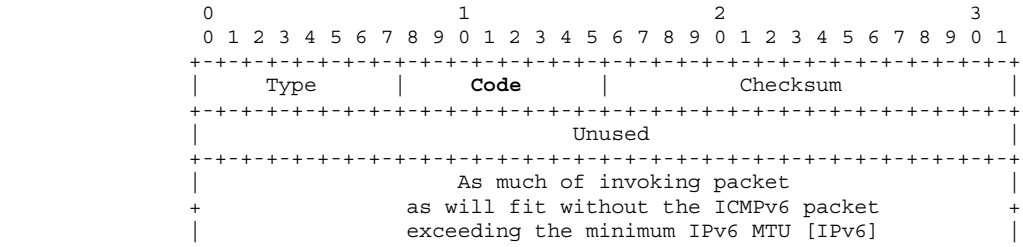
If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender.

Upper layer notification

A node receiving the ICMPv6 Destination Unreachable message MUST notify the upper-layer process.

RQ_000_1437 Destination Unreachable Code Field Value
RFC2463 3.1 MANDATORY
Applies to: Router
Context:
An IPv6 router constructs an ICMPv6 Destination Unreachable message as a response to a received IPv6 packet which cannot be delivered to its Destination Address due to administrative prohibition such as a "firewall filter".
Requirement:
The IPv6 router MUST set the ICMPv6 Code field to the value 1.
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 1

Code
0 - no route to destination
1 - communication with destination administratively prohibited
2 - (not assigned)
3 - address unreachable
4 - port unreachable

Unused This field is unused for all code values. It must be initialized to zero by the sender and ignored by the receiver.

Description

A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

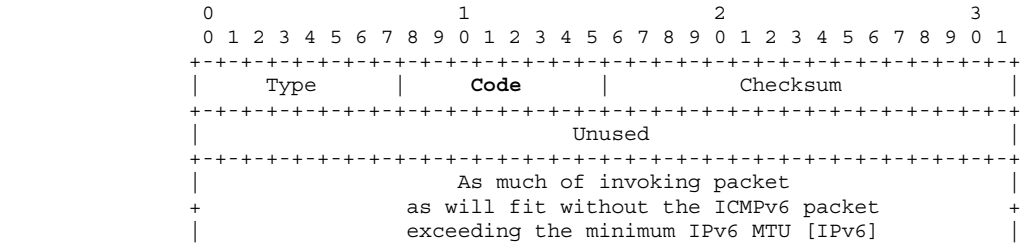
If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender.

Upper layer notification

A node receiving the ICMPv6 Destination Unreachable message MUST notify the upper-layer process.

RQ_000_1438 Destination Unreachable Code Field Value
RFC2463 3.1 MANDATORY
Applies to: Router
Context:
An IPv6 router constructs an ICMPv6 Destination Unreachable message as a response to a received IPv6 packet which cannot be delivered to its Destination Address due to any reason than the lack of a matching entry in the routing table or administrative prohibition.
Requirement:
The IPv6 router MUST set the ICMPv6 Code field to the value 3.
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 1

Code
0 - no route to destination
1 - communication with destination administratively prohibited
2 - (not assigned)
3 - address unreachable
4 - port unreachable

Unused This field is unused for all code values. It must be initialized to zero by the sender and ignored by the receiver.

Description

A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

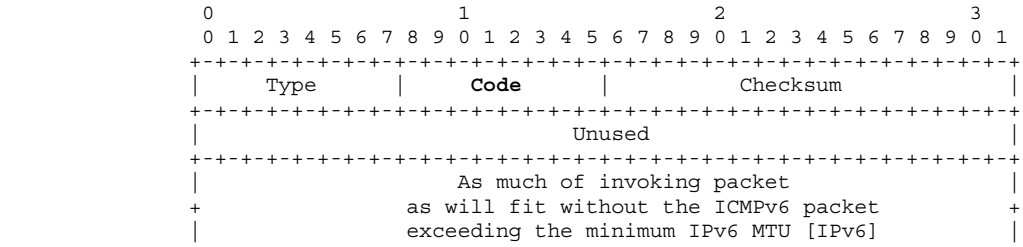
If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender.

Upper layer notification

A node receiving the ICMPv6 Destination Unreachable message MUST notify the upper-layer process.

RQ_000_1441 Destination Unreachable Code Field Value
RFC2463 3.1 MANDATORY
Applies to: Router
Context:
An IPv6 router constructs an ICMPv6 Destination Unreachable message as a response to a received IPv6 packet for which the transport protocol (e.g., UDP) has no listener and the transport protocol has no alternative means to inform the sender.
Requirement:
The IPv6 router MUST set the ICMPv6 Code field to the value 4.
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 1

Code
0 - no route to destination
1 - communication with destination administratively prohibited
2 - (not assigned)
3 - address unreachable
4 - port unreachable

Unused This field is unused for all code values. It must be initialized to zero by the sender and ignored by the receiver.

Description

A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

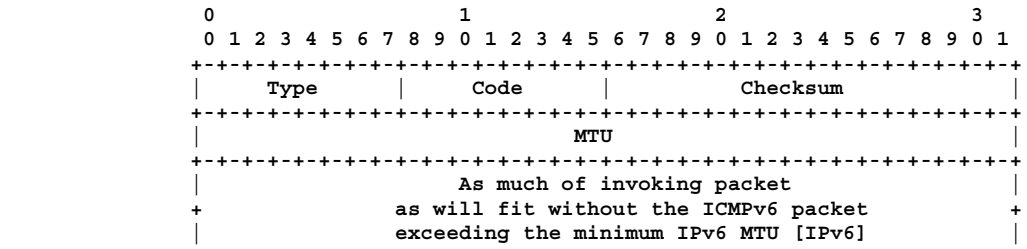
If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender.

Upper layer notification

A node receiving the ICMPv6 Destination Unreachable message MUST notify the upper-layer process.

RQ_000_1443 Generate Packet Too Big Message
RFC2463 3.2 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet which it cannot forward to the packet's destination address because the packet is larger than the MTU of the outgoing link
Requirement:
The IPv6 router MUST send an ICMPv6 message to the originating node with the Type Field (octet 1) set to 2 (Packet Too Big), the Code Field (octet 2) set to zero (0), the Checksum Field (octets 3 and 4) set to the calculated checksum, the MTU Field (octets 5 to 8) set to the Maximum Transmission Unit of the next-hop link and the Message Body Field set to contain as much of invoking packet as will fit without the ICMPv6 packet exceeding the minimum IPv6 MTU.
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type	**2**
Code	**Set to 0 (zero) by the sender and ignored by the receiver**
MTU	**The Maximum Transmission Unit of the next-hop link.**

Description

A Packet Too Big MUST be sent by a router in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link. The information in this message is used as part of the Path MTU Discovery process [PMTU].

Sending a Packet Too Big Message makes an exception to one of the rules of when to send an ICMPv6 error message, in that unlike other messages, it is sent in response to a packet received with an IPv6 multicast destination address, or a link-layer multicast or link-layer broadcast address.

Upper layer notification

An incoming Packet Too Big message MUST be passed to the upper-layer process.

RQ_000_1444 Process Packet Too Big Message

RFC2463 3.2 MANDATORY

Applies to: Host, Router

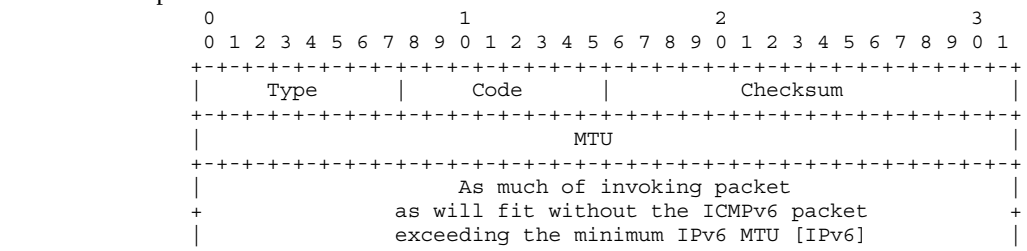
Context:

An IPv6 node receives an ICMPv6 Packet Too Big message

Requirement:

The IPv6 node MUST ignore the contents of the Code field in the ICMPv6 Packet Too Big message.

Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 2

Code **Set to 0 (zero) by the sender and ignored by the receiver**

MTU The Maximum Transmission Unit of the next-hop link.

Description

A Packet Too Big MUST be sent by a router in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link. The information in this message is used as part of the Path MTU Discovery process [PMTU].

Sending a Packet Too Big Message makes an exception to one of the rules of when to send an ICMPv6 error message, in that unlike other messages, it is sent in response to a packet received with an IPv6 multicast destination address, or a link-layer multicast or link-layer broadcast address.

Upper layer notification

An incoming Packet Too Big message MUST be passed to the upper-layer process.

RQ_000_1447 Generate Time Exceeded Message

RFC2463 3.3 MANDATORY

Applies to: Router

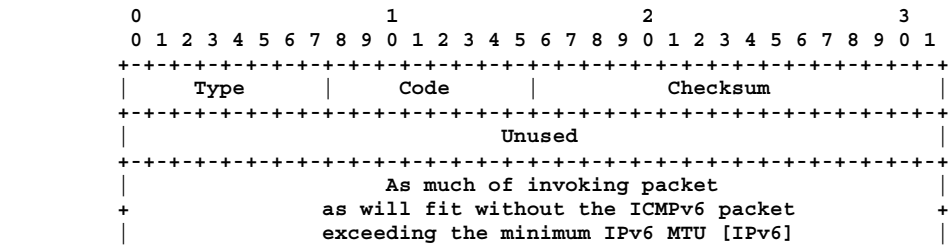
Context:

An IPv6 router receives a packet for which the router is not the destination and in which the Hop Limit field is set to either zero (0) or one (1)

Requirement:

The IPv6 router MUST discard the received packet and send an ICMPv6 message to the packet's originator with the Type Field (octet 1) set to 3 (Time Exceeded), the Code Field (octet 2) set to 0 (hop limit exceeded in transit), the Checksum Field (octets 3 and 4) set to the calculated checksum, the Unused field (octets 5 to 8) set to 0 and the Message Body Field set to contain as much of invoking packet as will fit without the ICMPv6 packet exceeding the minimum IPv6 MTU.

Specification Text:



IPv6 Fields:

Destination Address
Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 3

Code 0 - hop limit exceeded in transit

1 - fragment reassembly time exceeded

Unused This field is unused for all code values. It must be initialized to zero by the sender and ignored by the receiver.

Description

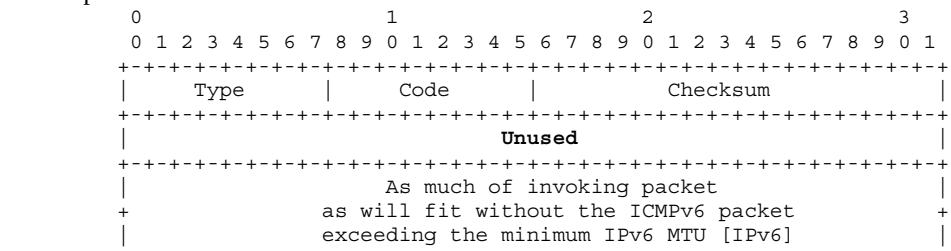
If a router receives a packet with a Hop Limit of zero, or a router decrements a packet's Hop Limit to zero, it MUST discard the packet and send an ICMPv6 Time Exceeded message with Code 0 to the source of the packet. This indicates either a routing loop or too small an initial Hop Limit value.

The rules for selecting the Source Address of this message are defined in section 2.2.

Upper layer notification

An incoming Time Exceeded message MUST be passed to the upper-layer process.

RQ_000_1448 Process Time Exceeded Message
RFC2463 3.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an ICMPv6 Time Exceeded message
Requirement:
The IPv6 node MUST ignore the contents of the Unused field (octets 5 to 8) in the ICMPv6 Time Exceeded message.
Specification Text:



IPv6 Fields:

Destination Address
Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 3

Code 0 - hop limit exceeded in transit

1 - fragment reassembly time exceeded

Unused **This field is unused for all code values.**
It must be initialized to zero by the sender
and ignored by the receiver.

Description

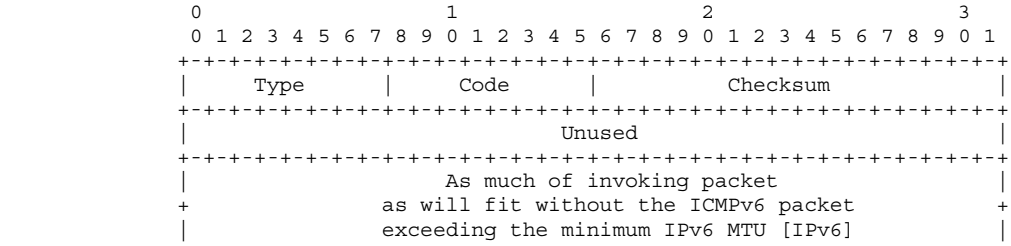
If a router receives a packet with a Hop Limit of zero, or a router decrements a packet's Hop Limit to zero, it MUST discard the packet and send an ICMPv6 Time Exceeded message with Code 0 to the source of the packet. This indicates either a routing loop or too small an initial Hop Limit value.

The rules for selecting the Source Address of this message are defined in section 2.2.

Upper layer notification

An incoming Time Exceeded message MUST be passed to the upper-layer process.

RQ_000_1449 Generate Time Exceeded Message
RFC2463 3.3 MANDATORY
Applies to: Router
Context:
An IPv6 router receives a packet for which it is not the destination and which has a Hop Limit field set to a value of zero (0).
Requirement:
The IPv6 router MUST ignore the packet and send an ICMPv6 Time Exceeded message with Code field set to zero (0) to the source of the packet.
Specification Text:



IPv6 Fields:

Destination Address
Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type 3

Code **0 - hop limit exceeded in transit**

1 - fragment reassembly time exceeded

Unused This field is unused for all code values.
It must be initialized to zero by the sender
and ignored by the receiver.

Description

If a router receives a packet with a Hop Limit of zero, or a router decrements a packet's Hop Limit to zero, **it MUST discard the packet and send an ICMPv6 Time Exceeded message with Code 0 to the source of the packet.** This indicates either a routing loop or too small an initial Hop Limit value.

The rules for selecting the Source Address of this message are defined in section 2.2.

Upper layer notification

An incoming Time Exceeded message MUST be passed to the upper-layer process.

RQ_000_1450 Generate Time Exceeded Message

RFC2463 3.3 MANDATORY

Applies to: Router

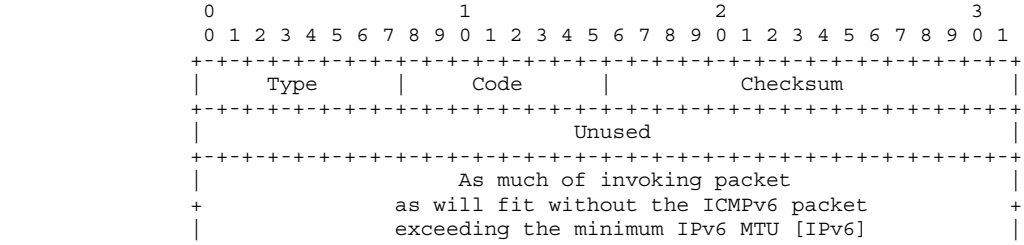
Context:

An IPv6 router receives a packet for which it is not the destination and which has a Hop Limit field set to a value of one (1)

Requirement:

The IPv6 router MUST ignore the packet and send an ICMPv6 Time Exceeded message with Code field set to zero (0) to the source of the packet.

Specification Text:



IPv6 Fields:

Destination Address
Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type	3
Code	**0 - hop limit exceeded in transit**
	1 - fragment reassembly time exceeded
Unused	This field is unused for all code values. It must be initialized to zero by the sender and ignored by the receiver.

Description

If a router receives a packet with a Hop Limit of zero, or a router decrements a packet's Hop Limit to zero, it MUST discard the packet and send an ICMPv6 Time Exceeded message with Code 0 to the source of the packet. This indicates either a routing loop or too small an initial Hop Limit value.

The rules for selecting the Source Address of this message are defined in section 2.2.

Upper layer notification

An incoming Time Exceeded message MUST be passed to the upper-layer process.

RQ_000_1453 Generate Parameter Problem Message

RFC2463 3.4 RECOMMENDED

Applies to: Router, Host

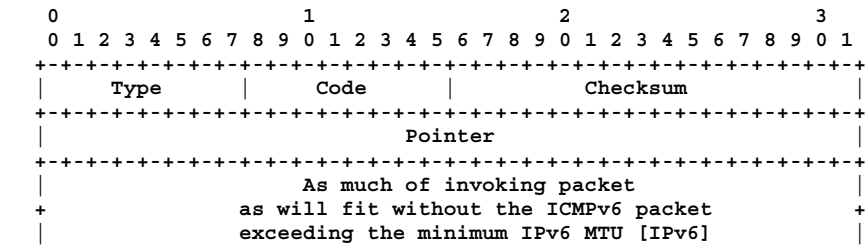
Context:

An IPv6 node constructs an ICMPv6 message to be sent in response to an incoming IPv6 packet which it is unable to process because it contains erroneous data in a header field or extension header field.

Requirement:

The IPv6 node MUST construct the ICMPv6 message with the Destination Address in the IPv6 Header set to the Source Address taken from the received offending packet, the ICMPv6 Type Field (octet 1) set to 4 (Parameter Problem), the Code Field (octet 2) set to zero (0), the Checksum Field (octets 3 and 4) set to the calculated checksum, the Pointer Field set to the octet offset within the invoking packet where the error was detected and the Message Body Field set to contain as much of invoking packet as will fit without the ICMPv6 packet exceeding the minimum IPv6 MTU.

Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type	**4**
Code	**0 - erroneous header field encountered**
	1 - unrecognized Next Header type encountered
	2 - unrecognized IPv6 option encountered
Pointer	**Identifies the octet offset within the invoking packet where the error was detected.**
	The pointer will point beyond the end of the ICMPv6 packet if the field in error is beyond what can fit in the maximum size of an ICMPv6 error message.

Description

If an IPv6 node processing a packet finds a problem with a field in the IPv6 header or extension headers such that it cannot complete processing the packet, it MUST discard the packet **and SHOULD send an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem.**

The pointer identifies the octet of the original packet's header where the error was detected. For example, an ICMPv6 message with Type field = 4, Code field = 1, and Pointer field = 40 would indicate that the IPv6 extension header following the IPv6 header of the original packet holds an unrecognized Next Header field value.

Upper layer notification

A node receiving this ICMPv6 message MUST notify the upper-layer process.

RQ_000_1455 Process IPv6 Header

RFC2463 3.4 MANDATORY

Applies to: Host, Router

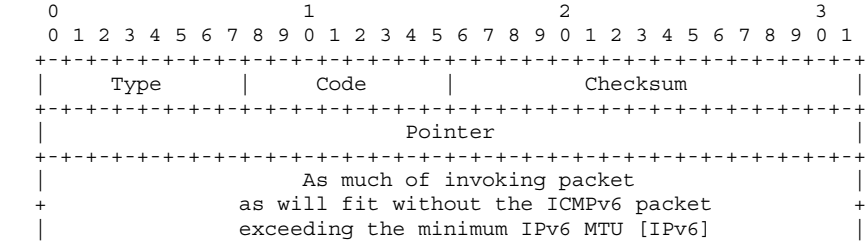
Context:

An IPv6 node receives an IPv6 packet which it is unable to process as a result of an error in one or more of the IPv6 Header fields or Extension Header fields.

Requirement:

The IPv6 node MUST discard the received packet.

Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type	4
Code	0 - erroneous header field encountered
	1 - unrecognized Next Header type encountered
	2 - unrecognized IPv6 option encountered
Pointer	Identifies the octet offset within the invoking packet where the error was detected.
	The pointer will point beyond the end of the ICMPv6 packet if the field in error is beyond what can fit in the maximum size of an ICMPv6 error message.

Description

If an IPv6 node processing a packet finds a problem with a field in the IPv6 header or extension headers such that it cannot complete processing the packet, it MUST discard the packet and SHOULD send an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem.

The pointer identifies the octet of the original packet's header where the error was detected. For example, an ICMPv6 message with Type field = 4, Code field = 1, and Pointer field = 40 would indicate that the IPv6 extension header following the IPv6 header of the original packet holds an unrecognized Next Header field value.

Upper layer notification

A node receiving this ICMPv6 message MUST notify the upper-layer process.

RQ_000_1459 Generate Echo Request Message

RFC2463 4.1 MANDATORY

Applies to: Host, Router

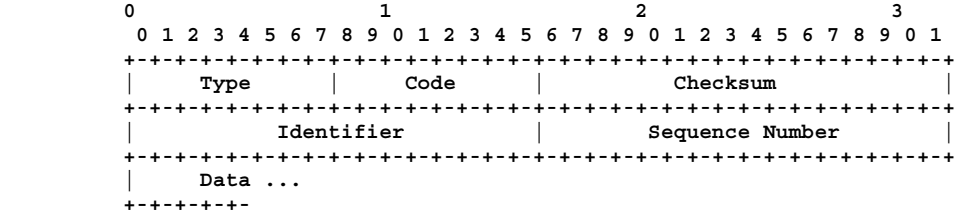
Context:

An IPv6 node is requested to send an Echo Request

Requirement:

The IPv6 node MUST construct and send an ICMPv6 message with the Type Field (octet 1) set to 128 (Echo Request), the Code Field (octet 2) set to zero (0), the Checksum Field (octets 3 and 4) set to the calculated checksum, the Identifier Field (octets 5 and 6) set to a unique integer value to aid in matching Echo Replies to this Echo Request, the Sequence Number Field (octets 7 and 8) set to an additional integer value to aid in matching Echo Replies to this Echo Request and the Data Field (octets 9 onwards) set to contain zero or more octets of arbitrary data.

Specification Text:



IPv6 Fields:

Destination Address

Any legal IPv6 address.

ICMPv6 Fields:

Type **128**

Code **0**

Identifier **An identifier to aid in matching Echo Replies to this Echo Request. May be zero.**

Sequence Number

A sequence number to aid in matching Echo Replies to this Echo Request. May be zero.

Data **Zero or more octets of arbitrary data.**

Description

Every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and sends corresponding Echo Replies. A node SHOULD also implement an application-layer interface for sending Echo Requests and receiving Echo Replies, for diagnostic purposes.

Upper layer notification

Echo Request messages MAY be passed to processes receiving ICMP messages.

RQ_000_1460 Process Echo Request Message

RFC2463 4.1 MANDATORY

Applies to: Host, Router

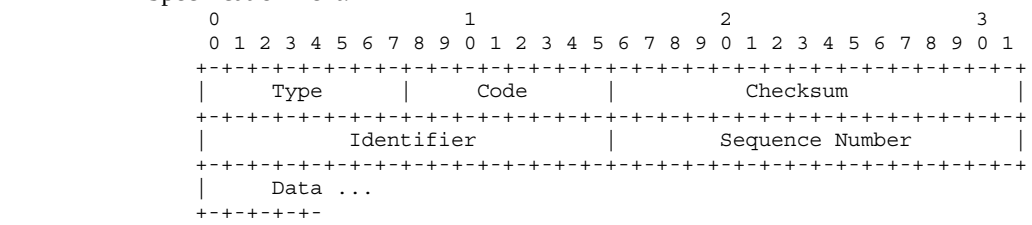
Context:

In IPv6 node receives an ICMPv6 Echo Request message.

Requirement:

The IPv6 node MUST send a corresponding Echo Reply message to the originator of the Echo Request.

Specification Text:



IPv6 Fields:

Destination Address

Any legal IPv6 address.

ICMPv6 Fields:

Type 128

Code 0

Identifier An identifier to aid in matching Echo Replies to this Echo Request. May be zero.

Sequence Number

A sequence number to aid in matching Echo Replies to this Echo Request. May be zero.

Data Zero or more octets of arbitrary data.

Description

Every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and sends corresponding Echo Replies. A node SHOULD also implement an application-layer interface for sending Echo Requests and receiving Echo Replies, for diagnostic purposes.

Upper layer notification

Echo Request messages MAY be passed to processes receiving ICMP messages.

RQ_000_1463 Process Echo Request Message

RFC2463 4.2 MANDATORY

Applies to: Host, Router

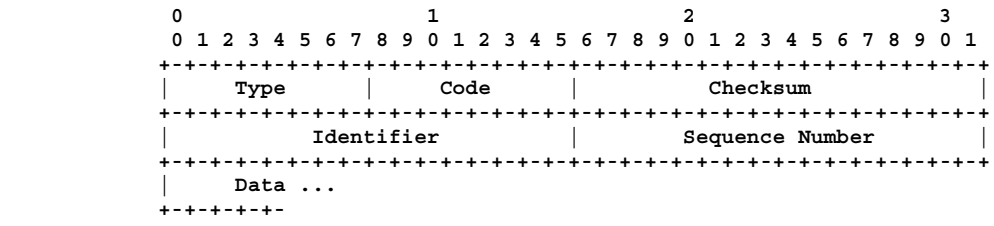
Context:

An IPv6 node receives an ICMPv6 Echo Request message sent to one of its valid unicast addresses.

Requirement:

The IPv6 node MUST send an ICMPv6 message to the originator of the incoming Echo Request message with the Type Field (octet 1) set to 129 (Echo Reply), the Code Field (octet 2) set to zero (0), the Checksum Field (octets 3 and 4) set to the calculated checksum, the Identifier Field (octets 5 and 6) set to the value received in the Identifier field in the invoking Echo Request message, the Sequence Number Field (octets 7 and 8) set to the value received in the Sequence Number field in the invoking Echo Request message and the Data Field (octets 9 onwards) set to the value received in the Data field in the invoking Echo Request message.

Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking Echo Request packet.

ICMPv6 Fields:

Type	**129**
Code	**0**
Identifier	**The identifier from the invoking Echo Request message.**
Sequence Number	**The sequence number from the invoking Echo Request message.**
Data	**The data from the invoking Echo Request message.**

Description

Every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and sends corresponding Echo Replies. A node SHOULD also implement an application-layer interface for sending Echo Requests and receiving Echo Replies, for diagnostic purposes.

The source address of an Echo Reply sent in response to a unicast Echo Request message MUST be the same as the destination address of that Echo Request message.

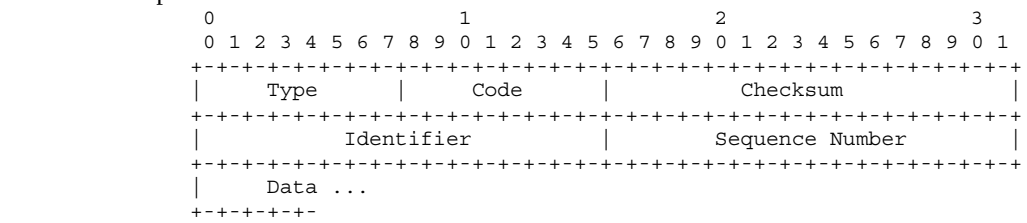
An Echo Reply SHOULD be sent in response to an Echo Request message sent to an IPv6 multicast address. The source address of the reply MUST be a unicast address belonging to the interface on which the multicast Echo Request message was received.

The data received in the ICMPv6 Echo Request message MUST be returned entirely and unmodified in the ICMPv6 Echo Reply message.

Upper layer notification

Echo Reply messages MUST be passed to the process that originated an Echo Request message. It may be passed to processes that did not originate the Echo Request message.

RQ_000_1464 Process Echo Request Message
RFC2463 4.2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an ICMPv6 Echo Request message sent to one of its valid unicast addresses
Requirement:
The IPv6 node MUST set the Source Address field in the IPv6 Header of its corresponding Echo Reply message to the value of the Destination Address in the incoming Echo Request message.
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking Echo Request packet.

ICMPv6 Fields:

Type	129
Code	0
Identifier	The identifier from the invoking Echo Request message.
Sequence Number	The sequence number from the invoking Echo Request message.
Data	The data from the invoking Echo Request message.

Description

Every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and sends corresponding Echo Replies. A node SHOULD also implement an application-layer interface for sending Echo Requests and receiving Echo Replies, for diagnostic purposes.

The source address of an Echo Reply sent in response to a unicast Echo Request message MUST be the same as the destination address of that Echo Request message.

An Echo Reply SHOULD be sent in response to an Echo Request message sent to an IPv6 multicast address. The source address of the reply MUST be a unicast address belonging to the interface on which the multicast Echo Request message was received.

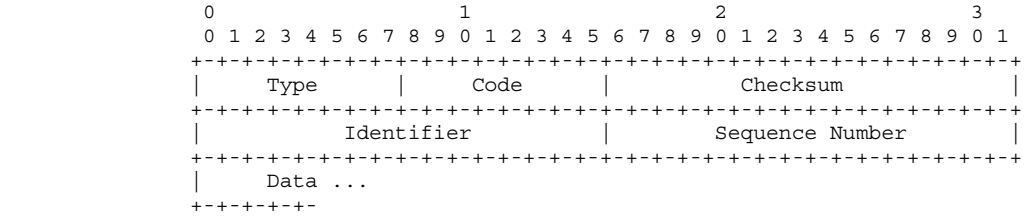
The data received in the ICMPv6 Echo Request message MUST be returned entirely and unmodified in the ICMPv6 Echo Reply message.

Upper layer notification

Echo Reply messages MUST be passed to the process that originated an Echo Request message. It may be passed to processes that did not originate the Echo Request message.

RQ_000_1465 Process Echo Request Message
RFC2463 4.2 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node receives an ICMPv6 Echo Request message sent to a multicast address of which the receiving node is a member.
Requirement:
The IPv6 node SHOULD send an Echo Reply in response to the request.

Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking Echo Request packet.

ICMPv6 Fields:

Type	129
Code	0
Identifier	The identifier from the invoking Echo Request message.
Sequence Number	The sequence number from the invoking Echo Request message.
Data	The data from the invoking Echo Request message.

Description

Every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and sends corresponding Echo Replies. A node SHOULD also implement an application-layer interface for sending Echo Requests and receiving Echo Replies, for diagnostic purposes.

The source address of an Echo Reply sent in response to a unicast Echo Request message MUST be the same as the destination address of that Echo Request message.

An Echo Reply SHOULD be sent in response to an Echo Request message sent to an IPv6 multicast address. The source address of the reply MUST be a unicast address belonging to the interface on which the multicast Echo Request message was received.

The data received in the ICMPv6 Echo Request message MUST be returned entirely and unmodified in the ICMPv6 Echo Reply message.

Upper layer notification

Echo Reply messages MUST be passed to the process that originated an Echo Request message. It may be passed to processes that did not originate the Echo Request message.

RQ_000_1466 Process Echo Request Message

RFC2463 4.2 MANDATORY

Applies to: Host, Router

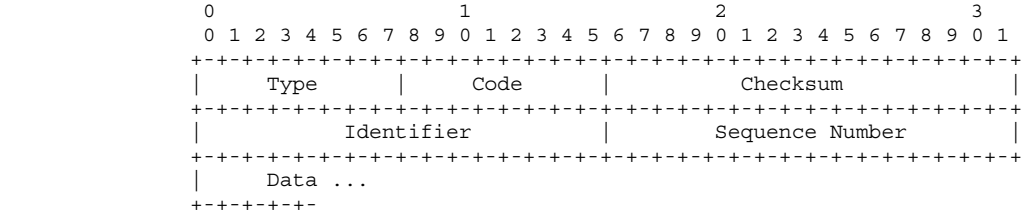
Context:

An IPv6 node sends an ICMPv6 Echo Reply in response to receiving an ECHO Request sent to a multicast address of which the receiving node is a member.

Requirement:

The IPv6 node MUST set the Source Address field in its ICMPv6 Echo Reply to a unicast address belonging to the interface on which the multicast Echo Request message was received.

Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking Echo Request packet.

ICMPv6 Fields:

Type	129
Code	0
Identifier	The identifier from the invoking Echo Request message.
Sequence Number	The sequence number from the invoking Echo Request message.
Data	The data from the invoking Echo Request message.

Description

Every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and sends corresponding Echo Replies. A node SHOULD also implement an application-layer interface for sending Echo Requests and receiving Echo Replies, for diagnostic purposes.

The source address of an Echo Reply sent in response to a unicast Echo Request message MUST be the same as the destination address of that Echo Request message.

An Echo Reply SHOULD be sent in response to an Echo Request message sent to an IPv6 multicast address. **The source address of the reply MUST be a unicast address belonging to the interface on which the multicast Echo Request message was received**.

The data received in the ICMPv6 Echo Request message MUST be returned entirely and unmodified in the ICMPv6 Echo Reply message.

Upper layer notification

Echo Reply messages MUST be passed to the process that originated an Echo Request message. It may be passed to processes that did not originate the Echo Request message.

RQ_000_1467 Process Echo Request Message

RFC2463 4.2 MANDATORY

Applies to: Router, Host

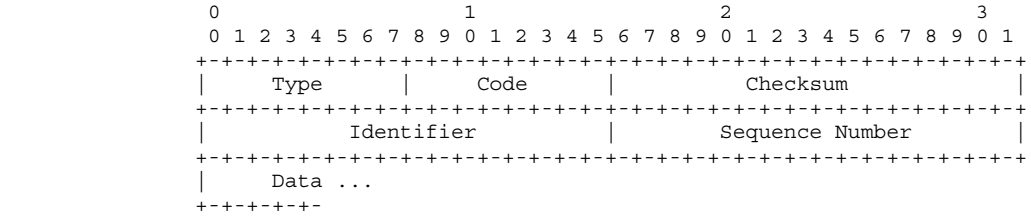
Context:

An IPv6 node sends an ICMPv6 Echo Reply in response to receiving an Echo Request

Requirement:

The IPv6 node MUST set the Data field in the ICMPv6 Echo Reply to the complete and unmodified contents of the Data field in the corresponding Echo Request message.

Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking Echo Request packet.

ICMPv6 Fields:

Type	129
Code	0
Identifier	The identifier from the invoking Echo Request message.

```
 Sequence       The sequence number from the invoking Echo Request
 Number         message.

 Data           The data from the invoking Echo Request message.

Description

Every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and
sends corresponding Echo Replies.  A node SHOULD also implement an application-layer interface
for sending Echo Requests and receiving Echo Replies, for diagnostic purposes.

The source address of an Echo Reply sent in response to a unicast Echo Request message MUST be
the same as the destination address of that Echo Request message.

An Echo Reply SHOULD be sent in response to an Echo Request message sent to an IPv6 multicast
address.  The source address of the reply MUST be a unicast address belonging to the interface
on which the multicast Echo Request message was received.

The data received in the ICMPv6 Echo Request message MUST be returned entirely and unmodified
in the ICMPv6 Echo Reply message.


Upper layer notification

Echo Reply messages MUST be passed to the process that originated an Echo Request message.  It
may be passed to processes that did not originate the Echo Request message.
```

RQ_000_1468 Process Echo Reply Message

RFC2463 4.1 MANDATORY

Applies to: Host, Router

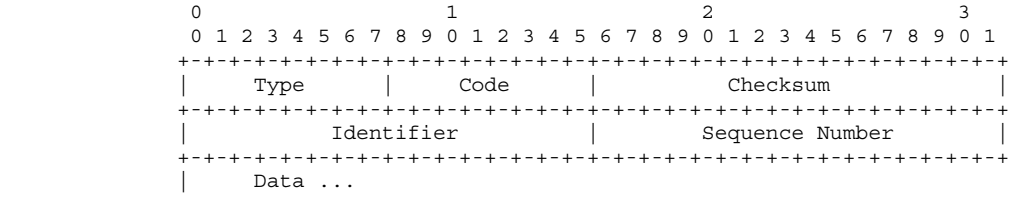
Context:

An IPv6 node receives an ICMPv6 Echo Reply messages in response to its Echo Request message.

Requirement:

The IPv6 node MUST pass the Echo Reply messages to the [upper-layer] process that originated the original Echo Request message.

Specification Text:




```
IPv6 Fields:

 Destination Address

  Copied from the Source Address field of the invoking
  Echo Request packet.

ICMPv6 Fields:

 Type           129

 Code           0

 Identifier     The identifier from the invoking Echo Request message.

 Sequence       The sequence number from the invoking Echo Request
 Number         message.

 Data           The data from the invoking Echo Request message.

Description

Every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and
sends corresponding Echo Replies.  A node SHOULD also implement an application-layer interface
for sending Echo Requests and receiving Echo Replies, for diagnostic purposes.

The source address of an Echo Reply sent in response to a unicast Echo Request message MUST be
the same as the destination address of that Echo Request message.
```

An Echo Reply SHOULD be sent in response to an Echo Request message sent to an IPv6 multicast address. The source address of the reply MUST be a unicast address belonging to the interface on which the multicast Echo Request message was received.

The data received in the ICMPv6 Echo Request message MUST be returned entirely and unmodified in the ICMPv6 Echo Reply message.

Upper layer notification

Echo Reply messages MUST be passed to the process that originated an Echo Request message. It may be passed to processes that did not originate the Echo Request message.

RQ_000_1471 Protect ICMP Messages from Attacks
RFC2463 5.1 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
An IPv6 node that implements ICMPv6 SHOULD include an Authentication Header (AH) in any transmitted ICMPv6 messages if a Security Association (SA) exists between the node and the destination address.
Specification Text:
ICMP protocol packet exchanges can be authenticated using the IP Authentication Header [RFC 4302]. **A node SHOULD include an Authentication Header when sending ICMP messages if a security association for use with the IP Authentication Header exists for the destination address.** The security associations may have been created through manual configuration or through the operation of some key management protocol.

Received Authentication Headers in ICMP packets MUST be verified for correctness and packets with incorrect authentication MUST be ignored and discarded.

It SHOULD be possible for the system administrator to configure a node to ignore any ICMP messages that are not authenticated using either the Authentication Header or Encapsulating Security Payload. Such a switch SHOULD default to allowing unauthenticated messages.

Confidentiality issues are addressed by the IP Security Architecture and the IP Encapsulating Security Payload documents [RFC 4301, RFC 4303].

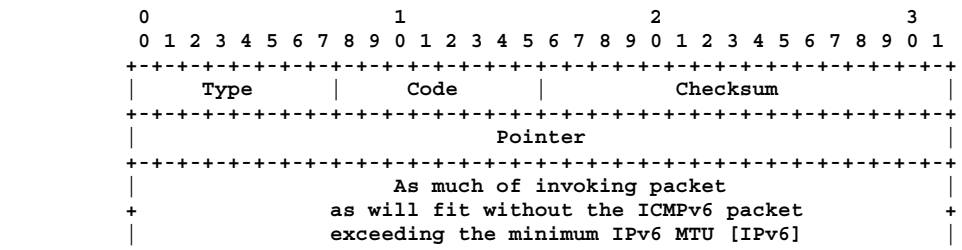
RQ_000_1472 Protect ICMP Messages from Attacks
RFC2463 5.1 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an ICMPv6 message in which there is an IPv6 Authentication Header which cannot be correctly authenticated.
Requirement:
The IPv6 node MUST ignore the contents of the ICMPv6 packet.
Specification Text:
ICMP protocol packet exchanges can be authenticated using the IP Authentication Header [RFC 4302]. A node SHOULD include an Authentication Header when sending ICMP messages if a security association for use with the IP Authentication Header exists for the destination address. The security associations may have been created through manual configuration or through the operation of some key management protocol.

Received Authentication Headers in ICMP packets MUST be verified for correctness and packets with incorrect authentication MUST be ignored and discarded.

It SHOULD be possible for the system administrator to configure a node to ignore any ICMP messages that are not authenticated using either the Authentication Header or Encapsulating Security Payload. Such a switch SHOULD default to allowing unauthenticated messages.

Confidentiality issues are addressed by the IP Security Architecture and the IP Encapsulating Security Payload documents [RFC 4301, RFC 4303].

RQ_000_1478 Generate Parameter Problem Message
RFC2463 3.4 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node constructs an ICMPv6 message to be sent in response to an incoming IPv6 packet which it is unable to process because it contains an unrecognized value in a Next Header field
Requirement:
The IPv6 node MUST construct the ICMPv6 message with the Destination Address in the IPv6 Header set to the Source Address taken from the received offending packet, the ICMPv6 Type Field (octet 1) set to 4 (Parameter Problem), the Code Field (octet 2) set to 1, the Checksum Field (octets 3 and 4) set to the calculated checksum, the Pointer Field set to the octet offset within the invoking packet where the error was detected and the Message Body Field set to contain as much of invoking packet as will fit without the ICMPv6 packet exceeding the minimum IPv6 MTU.
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type **4**

Code 0 - erroneous header field encountered

1 - unrecognized Next Header type encountered

2 - unrecognized IPv6 option encountered

Pointer **Identifies the octet offset within the invoking packet where the error was detected.**

The pointer will point beyond the end of the ICMPv6 packet if the field in error is beyond what can fit in the maximum size of an ICMPv6 error message.

Description

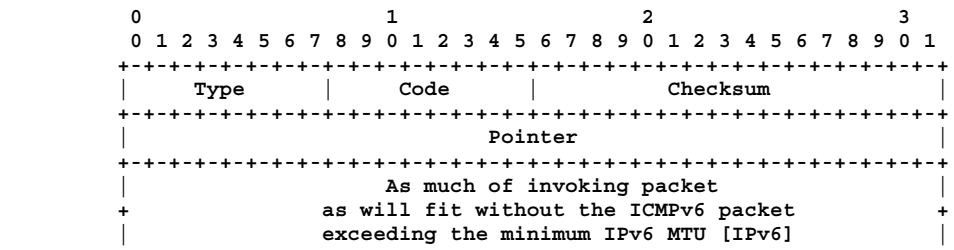
If an IPv6 node processing a packet finds a problem with a field in the IPv6 header or extension headers such that it cannot complete processing the packet, it MUST discard the packet and SHOULD send an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem.

The pointer identifies the octet of the original packet's header where the error was detected. For example, an ICMPv6 message with Type field = 4, Code field = 1, and Pointer field = 40 would indicate that the IPv6 extension header following the IPv6 header of the original packet holds an unrecognized Next Header field value.

Upper layer notification

A node receiving this ICMPv6 message MUST notify the upper-layer process.

RQ_000_1480 Generate Parameter Problem Message
RFC2463 3.4 RECOMMENDED
Applies to: Router, Host
Context:
An IPv6 node constructs an ICMPv6 message to be sent in response to an incoming IPv6 packet which it is unable to process because it contains an unrecognized Ipv6 option
Requirement:
The IPv6 node MUST construct the ICMPv6 message with the Destination Address in the IPv6 Header set to the Source Address taken from the received offending packet, the ICMPv6 Type Field (octet 1) set to 4 (Parameter Problem), the Code Field (octet 2) set to 2, the Checksum Field (octets 3 and 4) set to the calculated checksum, the Pointer Field set to the octet offset within the invoking packet where the error was detected and the Message Body Field set to contain as much of invoking packet as will fit without the ICMPv6 packet exceeding the minimum IPv6 MTU.
Specification Text:



IPv6 Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMPv6 Fields:

Type **4**

Code 0 - erroneous header field encountered

1 - unrecognized Next Header type encountered

2 - unrecognized IPv6 option encountered

Pointer **Identifies the octet offset within the invoking packet where the error was detected.**

The pointer will point beyond the end of the ICMPv6 packet if the field in error is beyond what can fit in the maximum size of an ICMPv6 error message.

Description

If an IPv6 node processing a packet finds a problem with a field in the IPv6 header or extension headers such that it cannot complete processing the packet, it MUST discard the packet and SHOULD send an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem.

The pointer identifies the octet of the original packet's header where the error was detected. For example, an ICMPv6 message with Type field = 4, Code field = 1, and Pointer field = 40 would indicate that the IPv6 extension header following the IPv6 header of the original packet holds an unrecognized Next Header field value.

Upper layer notification

A node receiving this ICMPv6 message MUST notify the upper-layer process.

4.9 Requirements extracted from RFC 2464

RQ_000_8000 IPv6 in Ethernet Frame
RFC2464 2 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node is configured for the transmission and receipt of packets within an Ethernet frame
Requirement:
The IPv6 node MUST use a default MTU size of 1500 octets.
Specification Text:
The default MTU size for IPv6 [RFC2460] packets on an Ethernet is 1500 octets. This size may be reduced by a Router Advertisement [RFC2461] containing an MTU option which specifies a smaller MTU, or by manual configuration of each node. If a Router Advertisement received on an Ethernet interface has an MTU option specifying an MTU larger than 1500, or larger than a manually configured value, that MTU option may be logged to system management but must be otherwise ignored.

RQ_000_8001 IPv6 in Ethernet Frame
RFC2464 2 OPTIONAL
Applies to: Host, Router
Context:
An IPv6 node is configured for the transmission and receipt of packets within an Ethernet frame and receives a Router Advertisement message containing an MTU option that specifies an MTU smaller than the default size of 1500 bytes but greater than or equal to 1280 octets.
Requirement:
The node MAY set the MTU to the size specified in the Router Advertisement's MTU option.
Specification Text:
The default MTU size for IPv6 [RFC2460] packets on an Ethernet is 1500 octets. **This size may be reduced by a Router Advertisement [RFC2461] containing an MTU option which specifies a smaller MTU**, or by manual configuration of each node. If a Router Advertisement received on an Ethernet interface has an MTU option specifying an MTU larger than 1500, or larger than a manually configured value, that MTU option may be logged to system management but must be otherwise ignored.

RQ_000_8002 IPv6 in Ethernet Frame
RFC2464 2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node is configured for transmission and receipt of packets within an Ethernet frame and a manual configuration request is received to set the default MTU size to less than 1500 octets but greater than 1280 octets.
Requirement:
The IPv6 node MUST set its default MTU size to the manually configured value.
Specification Text:
The default MTU size for IPv6 [RFC2460] packets on an Ethernet is 1500 octets. **This size may be reduced** by a Router Advertisement [RFC2461] containing an MTU option which specifies a smaller MTU, or **by manual configuration of each node.** If a Router Advertisement received on an Ethernet interface has an MTU option specifying an MTU larger than 1500, or larger than a manually configured value, that MTU option may be logged to system management but must be otherwise ignored.

RQ_000_8003 IPv6 in Ethernet Frame
RFC2464 2 OPTIONAL
Applies to: Host, Router
Context:
An IPv6 node is configured for transmission and receipt of packets within an Ethernet frame and receives a Router Advertisement message containing an MTU option specifying an MTU larger than the current default value (1500 octets or a manually configured value).
Requirement:
The IPv6 MAY log the MTU option request.
Specification Text:
The default MTU size for IPv6 [RFC2460] packets on an Ethernet is 1500 octets. This size may be reduced by a Router Advertisement [RFC2461] containing an MTU option which specifies a smaller MTU, or by manual configuration of each node. **If a Router Advertisement received on an Ethernet interface has an MTU option specifying an MTU larger than 1500**, or larger than a manually configured value, **that MTU option may be logged to system management** but must be otherwise ignored.

RQ_000_8004 IPv6 in Ethernet Frame
RFC2464 2 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node is configured for transmission and receipt of packets within an Ethernet frame and receives a Router Advertisement message containing an MTU option specifying an MTU larger than current default value (1500 octets or a manually configured value).
Requirement:
The IPv6 node MUST leave ignore the request to increase the MTU beyond 1500octets
Specification Text:
The default MTU size for IPv6 [RFC2460] packets on an Ethernet is 1500 octets. This size may be reduced by a Router Advertisement [RFC2461] containing an MTU option which specifies a smaller MTU, or by manual configuration of each node. **If a Router Advertisement received on an Ethernet interface has an MTU option specifying an MTU larger than 1500**, or larger than a manually configured value, that MTU option may be logged to system management but **must be otherwise ignored**.

RQ_000_8007 IPv6 in Ethernet Frame
RFC2464 3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node is configured for transmission and receipt of IPv6 packets within Ethernet frames.
Requirement:
When constructing an IPv6 packet within an Ethernet frame, the IPv6 node MUST set the Ethernet Type code in the Ethernet frame to the value 86DD hexadecimal.
Specification Text:
IPv6 packets are transmitted in standard Ethernet frames. The Ethernet header contains the Destination and Source Ethernet addresses and **the Ethernet type code, which must contain the value 86DD hexadecimal.** The data field contains the IPv6 header followed immediately by the payload, and possibly padding octets to meet the minimum frame size for the Ethernet link.

RQ_000_8008 IPv6 in Ethernet Frame
RFC2464 3 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node is configured for transmission and receipt of IPv6 packets within Ethernet frames.
Requirement:
When constructing an IPv6 packet within an Ethernet frame, the IPv6 node MUST set the Ethernet data field to contain the IPv6 header followed immediately by the IPv6 payload and any padding octets required to meet the Ethernet link's minimum frame size.
Specification Text:
IPv6 packets are transmitted in standard Ethernet frames. The Ethernet header contains the Destination and Source Ethernet addresses and the Ethernet type code, which must contain the value 86DD hexadecimal. **The data field contains the IPv6 header followed immediately by the payload, and possibly padding octets to meet the minimum frame size for the Ethernet link.**

RQ_000_8009 Stateless Autoconfiguration
RFC2464 4 -3 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When constructing an EUI-64 Interface Identifier from an IEEE 802 (Ethernet) address, an IPv6 node MUST set the most significant 3 octets of the identifier to the contents most significant 3 octets of the IEEE 802 address but with the next-to-lowest bit in the highest order octet complemented, the fourth and fifth octets together to the hexadecimal value FFFF and the least significant 3 octets to the value held in the least significant 3 octets of the IEEE 802 address.
Specification Text:
The OUI of the Ethernet address (the first three octets) becomes the company_id of the EUI-64 (the first three octets). The fourth and fifth octets of the EUI are set to the fixed value FFFE hexadecimal. The last three octets of the Ethernet address become the last three octets of the EUI-64.

The Interface Identifier is then formed from the EUI-64 by complementing the "Universal/Local" (U/L) bit, which is the next-to- lowest order bit of the first octet of the EUI-64. Complementing this bit will generally change a 0 value to a 1, since an interface's built-in address is expected to be from a universally administered address space and hence have a globally unique value. A universally administered IEEE 802 address or an EUI-64 is signified by a 0 in the U/L bit position, while a globally unique IPv6 Interface Identifier is signified by a 1 in the corresponding position.

RQ_000_8010 Stateless Autoconfiguration
RFC2464 4 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
When constructing an EUI-64 Interface Identifier from an IEEE 802 (Ethernet) address, an IPv6 node SHOULD NOT use a MAC address which has been set manually or by software.
Specification Text:
A different MAC address set manually or by software should not be used to derive the Interface Identifier. If such a MAC address must be used, its global uniqueness property should be reflected in the value of the U/L bit.

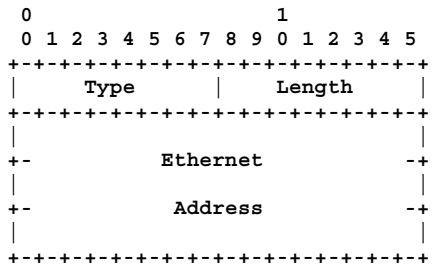
RQ_000_8012 Stateless Autoconfiguration
RFC2464 4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST construct a 64 bit IPv6 address prefix for stateless autoconfiguration over Ethernet.
Specification Text:
An IPv6 address prefix used for stateless autoconfiguration [RFC2462] of an Ethernet interface must have a length of 64 bits.

RQ_000_8013 Form Link-local Address
RFC2464 5 MANDATORY
Applies to: Host, Router
Context:
The implementation needs to form a link local address.
Requirement:
An IPv6 node MUST construct a link-local address for an Ethernet interface by appending the Interface Identifier to the prefix FE80::/64 (FE80 0000 0000 000 + IPv6 Interface Identifier).
Specification Text:
The IPv6 link-local address [AARCH] for an Ethernet interface is formed by appending the Interface Identifier, as defined above (4), to the prefix FE80::/64.

RQ_000_8014 Generate Extension Header Options
RFC2464 6 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing an IPv6 packet for unicast transmission over Ethernet, an IPv6 node MUST set the Type field in the Source Link-layer Address option to the value 1, the Length field to the value 1 and following 6 octets to the 48-bit Ethernet IEEE 802 address.
Specification Text:
The procedure for mapping IPv6 unicast addresses into Ethernet link-layer addresses is described in [RFC2461]. The Source/Target Link-layer Address option has the following form when the link layer is Ethernet.



Option fields:

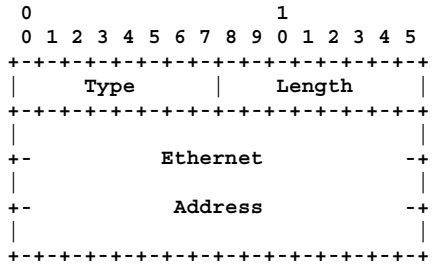
Type **1 for Source Link-layer address.**
2 for Target Link-layer address.

Length **1 (in units of 8 octets).**

Ethernet Address
The 48 bit Ethernet IEEE 802 address, in canonical bit order. This is the address the interface currently responds to, and may be different from the built-in address used to derive the Interface Identifier.

RQ_000_8015 Generate Extension Header Options
RFC2464 6 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing an IPv6 packet for unicast transmission over Ethernet, an IPv6 node MUST set the Type field in the Source Link-layer Address option to the value 2, the Length field to the value 1 and following 6 octets to the 48-bit Ethernet IEEE 802 address.
Specification Text:
The procedure for mapping IPv6 unicast addresses into Ethernet link-layer addresses is described in [RFC2461]. The Source/Target Link-layer Address option has the following form when the link layer is Ethernet.



Option fields:

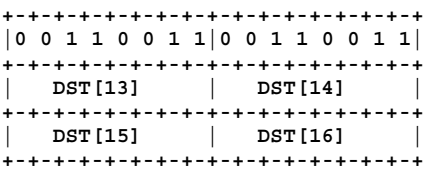
Type 1 for Source Link-layer address.
2 for Target Link-layer address.

Length **1 (in units of 8 octets).**

Ethernet Address
The 48 bit Ethernet IEEE 802 address, in canonical bit order. This is the address the interface currently responds to, and may be different from the built-in address used to derive the Interface Identifier.

RQ_000_8016 IPv6 in Ethernet Frame
RFC2464 7 MANDATORY
Applies to: Router, Host
Context:

Requirement:
When constructing an IPv6 packet for multicast transmission over Ethernet, an IPv6 node MUST append the last 4 octets of the IPv6 multicast address to two octets having the hexadecimal value 3333
Specification Text:
An IPv6 packet with a multicast destination address DST, consisting of the sixteen octets DST[1] through DST[16], is transmitted to the Ethernet multicast address whose first two octets are the value 3333 hexadecimal and whose last four octets are the last four octets of DST.



4.10 Requirements extracted from RFC 2675

RQ_000_8800 Jumbograms
RFC2675 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node that is capable of attaching to links with MTUs of greater than 65,575 octets MUST support IPv6 Jumbograms.
Specification Text:
Jumbograms are relevant only to IPv6 nodes that may be attached to links with a link MTU greater than 65,575 octets, and need not be implemented or understood by IPv6 nodes that do not support attachment to links with such large MTUs.

RQ_000_8801 Jumbograms
RFC2675 1 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node that is not capable of attaching to links with MTUs of greater than 65,575 octets MAY support IPv6 Jumbograms.
Specification Text:
The Jumbo Payload option is relevant only for IPv6 nodes that may be attached to links with a link MTU greater than 65,575 octets (that is, 65,535 + 40, where 40 octets is the size of the IPv6 header). **The Jumbo Payload option need not be implemented or understood by IPv6 nodes that do not support attachment to links with MTU greater than 65,575.**

RQ_000_8802 Jumbograms
RFC2675 1 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 MUST NOT make it possible for a particular link's MTU to be configured to a value greater than 65,575 octets if there are nodes attached to that link that do not support the Jumbo Payload option.
Specification Text:
On links with configurable MTUs, the MTU must not be configured to a value greater than 65,575 octets if there are nodes attached to that link that do not support the Jumbo Payload option and it can not be guaranteed that the Jumbo Payload option will not be sent to those nodes.

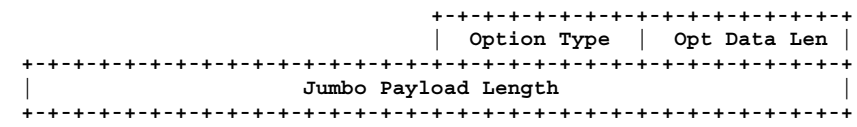
RQ_000_8804 Generate Jumbograms
RFC2675 2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing an IPv6 packet, an IPv6 node MUST place any Jumbo Payload in the Hop-by-Hop Options Header immediately following the IPv6 Header and with the following fields and contents:

Field Descriptor	Position in Hop-by-Hop Options	Contents
Option Type	Octet 3	C2 (hexadecimal)
Opt Data Length	Octet 4	4
Jumbo Payload Length	Octets 5 to 8	Length of the IPv6 packet in octets (>65,535), excluding the IPv6 Header including the Hop-by-Hop Options Header

The implementation places the Jumbo Payload option in an IPv6 Hop-by-Hop Options header immediately following the IPv6 header. The Option Type field is set to 0xC2 (hex, 8 bits) and the Opt Dat Len field is set to 4 (8 bits). The option's Length field is set to the length of the IPv6 packet in octets excluding the IPv6 header but including the Hop-by-Hop Options header and any other extension headers present. The Length value must be greater than 65,535.

Specification Text:
The Jumbo Payload option is carried in an IPv6 Hop-by-Hop Options header, immediately following the IPv6 header. This option has an alignment requirement of 4n + 2. (See RFC2460 Section 4.2 for discussion of option alignment.) The option has the following format:



Option Type 8-bit value C2 (hexadecimal).
Opt Data Len 8-bit value 4.
Jumbo Payload Length 32-bit unsigned integer. Length of the IPv6 packet in octets, excluding the IPv6 header but including the Hop-by-Hop Options header and any other extension headers present. Must be greater than 65,535.

RQ_000_8805 Generate Jumbograms
RFC2675 3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing an IPv6 packet which includes a Jumbo Payload Option, an IPv6 node MUST set the Payload Length field in the IPv6 Header to zero (0).

Specification Text:
The Payload Length field in the IPv6 header must be set to zero in every packet that carries the Jumbo Payload option.

RQ_000_8806 Process Jumbograms
RFC2675 3 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node supports the Jumbo Payload option.

Requirement:
If the IPv6 node receives an IPv6 packet in which the Payload Length field is set to zero (0), the Next Header field is set to zero (0) but the overall packet extends beyond the IPv6 Header, it MUST process the Hop-by-Hop Options header to the payload's actual length.

Specification Text:
If a node that understands the Jumbo Payload option receives a packet whose IPv6 header carries a Payload Length of zero and a Next Header value of zero (meaning that a Hop-by-Hop Options header follows), and whose link-layer framing indicates the presence of octets beyond the IPv6 header, the node must proceed to process the Hop-by-Hop Options header in order to determine the actual length of the payload from the Jumbo Payload option.

RQ_000_8807 Generate Jumbograms
RFC2675 3 CONDITIONAL
[if RQ_000_1064 then MANDATORY]
Applies to: Host, Router
Context:

Requirement:
When constructing an IPv6 packet which includes a Fragment Header, an IPv6 node MUST NOT also include a Jumbo Payload option in the packet.
Specification Text:
The Jumbo Payload option must not be used in a packet that carries a Fragment header.

RQ_000_8808 Generate Jumbograms
RFC2675 3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST ensure that any higher-layer protocol uses the value contained in the Jumbo Payload Length field of the Jumbo Payload option (if present) for checksum purposes rather than the Payload Length field in the IPv6 packet header.
Specification Text:
Higher-layer protocols that use the IPv6 Payload Length field to compute the value of the Upper-Layer Packet Length field in the checksum pseudo-header described in RFC2460, Section 8.1 must instead **use the Jumbo Payload Length field for that computation, for packets that carry the Jumbo Payload option.**

RQ_000_8809 Process Jumbograms
RFC2675 3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node that supports the Jumbo Payload option receives a packet in which the Payload Length field in the IPv6 Header is set to zero (0), the Next Header field is set to zero (Hop-by-Hop Options header) but there is no Jumbo Payload option present.
Requirement:
The IPv6 node MUST send an ICMPv6 Error Message to the sending address with the Type field set to 4, the Code field set to zero (0) and the Pointer field set to the position of the high-order octet of the IPv6 Payload Length field.
Specification Text:
Nodes that understand the Jumbo Payload option are required to detect a number of possible format errors, and if the erroneous packet was not destined to a multicast address, report the error by sending an ICMP Parameter Problem message [RFC2463] to the packet's source. The following list of errors specifies the values to be used in the Code and Pointer fields of the Parameter Problem message:

```
  error: IPv6 Payload Length = 0 and
         IPv6 Next Header = Hop-by-Hop Options and
         Jumbo Payload option not present
           Code: 0
           Pointer: high-order octet of the IPv6
                    Payload Length
  error: IPv6 Payload Length != 0 and
         Jumbo Payload option present
           Code: 0
           Pointer: Option Type field of the Jumbo
                    Payload option
  error: Jumbo Payload option present and
         Jumbo Payload Length < 65,536
           Code: 0
           Pointer: high-order octet of the Jumbo
                    Payload Length
```

```
  error: Jumbo Payload option present and
         Fragment header present
           Code: 0
           Pointer: high-order octet of the
                    Fragment header.
```

RQ_000_8810 Process Jumbograms

RFC2675 3 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node that supports the Jumbo Payload option receives a packet in which the Payload Length field in the IPv6 Header is not set to zero (0), but there is a Jumbo Payload option present.

Requirement:

The IPv6 node MUST send an ICMPv6 Error Message to the sending address with the Type field set to 4, the Code field set to zero (0) and the Pointer field set to the position of the Option Type field in the Jumbo Payload option.

Specification Text:

Nodes that understand the Jumbo Payload option are required to detect a number of possible format errors, and if the erroneous packet was not destined to a multicast address, report the error by sending an ICMP Parameter Problem message [RFC2463] to the packet's source. The following list of errors specifies the values to be used in the Code and Pointer fields of the Parameter Problem message:

```
  error: IPv6 Payload Length = 0 and
         IPv6 Next Header = Hop-by-Hop Options and
         Jumbo Payload option not present
           Code: 0
           Pointer: high-order octet of the IPv6
                    Payload Length
  error: IPv6 Payload Length != 0 and
         Jumbo Payload option present
           Code: 0
           Pointer: Option Type field of the Jumbo
                    Payload option
  error: Jumbo Payload option present and
         Jumbo Payload Length < 65,536
           Code: 0
           Pointer: high-order octet of the Jumbo
                    Payload Length
  error: Jumbo Payload option present and
         Fragment header present
           Code: 0
           Pointer: high-order octet of the
                    Fragment header.
```

RQ_000_8811 Process Jumbograms

RFC2675 3 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node that supports the Jumbo Payload option receives a packet which legitimately contains a Jumbo Payload option in which the Jumbo Payload Length field is set to a value less than decimal 65,536.

Requirement:

The IPv6 node MUST send an ICMPv6 Error Message to the sending address with the Type field set to 4, the Code field set to zero (0) and the Pointer field set to the position of the high-order octet of the Jumbo Payload Length field.

Specification Text:

Nodes that understand the Jumbo Payload option are required to detect a number of possible format errors, and if the erroneous packet was not destined to a multicast address, report the error by sending an ICMP Parameter Problem message [RFC2463] to the packet's source. The following list of errors specifies the values to be used in the Code and Pointer fields of the Parameter Problem message:

```
  error: IPv6 Payload Length = 0 and
         IPv6 Next Header = Hop-by-Hop Options and
         Jumbo Payload option not present
           Code: 0
           Pointer: high-order octet of the IPv6
                    Payload Length
  error: IPv6 Payload Length != 0 and
         Jumbo Payload option present
           Code: 0
```

```
          Pointer: Option Type field of the Jumbo
                   Payload option
  error: Jumbo Payload option present and
         Jumbo Payload Length < 65,536
           Code: 0
           Pointer: high-order octet of the Jumbo
                    Payload Length
  error: Jumbo Payload option present and
         Fragment header present
           Code: 0
           Pointer: high-order octet of the
                    Fragment header.
```

RQ_000_8812 Process Jumbograms

RFC2675 3 MANDATORY

Applies to: Router, Host

Context:

An IPv6 node that supports the Jumbo Payload option receives a packet which contains both a valid Jumbo Payload option and a Fragment Header

Requirement:

The IPv6 node MUST send an ICMPv6 Error Message to the sending address with the Type field set to 4, the Code field set to zero (0) and the Pointer field set to the position of the high-order octet of the Fragment Header.

Specification Text:

Nodes that understand the Jumbo Payload option are required to detect a number of possible format errors, and if the erroneous packet was not destined to a multicast address, report the error by sending an ICMP Parameter Problem message [RFC2463] to the packet's source. The following list of errors specifies the values to be used in the Code and Pointer fields of the Parameter Problem message:

```
  error: IPv6 Payload Length = 0 and
         IPv6 Next Header = Hop-by-Hop Options and
         Jumbo Payload option not present
           Code: 0
           Pointer: high-order octet of the IPv6
                    Payload Length
  error: IPv6 Payload Length != 0 and
         Jumbo Payload option present
           Code: 0
           Pointer: Option Type field of the Jumbo
                    Payload option
  error: Jumbo Payload option present and
         Jumbo Payload Length < 65,536
           Code: 0
           Pointer: high-order octet of the Jumbo
                    Payload Length
  error: Jumbo Payload option present and
         Fragment header present
           Code: 0
           Pointer: high-order octet of the
                    Fragment header.
```

RQ_000_8813 Process Hop by Hop Header

RFC2675 3 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node that does not support the Jumbo Payload option receives a packet in which the Payload Length field in the IPv6 Header is set to zero (0) and the Next Header field is set to zero (Hop-by-Hop Options header).

Requirement:

The IPv6 node MUST send an ICMPv6 Error Message to the sending address with the Type field set to 4, the Code field set to zero (0) and the Pointer field set to the high-order octet of the IPv6 Payload Length field.

Specification Text:

A node that does not understand the Jumbo Payload option is expected to respond to erroneously-received jumbograms as follows, according to the IPv6 specification:

```
  error: IPv6 Payload Length = 0 and
         IPv6 Next Header = Hop-by-Hop Options
           Code: 0
           Pointer: high-order octet of the IPv6
                    Payload Length
```

```
error: IPv6 Payload Length != 0 and
       Jumbo Payload option present
         Code: 2
         Pointer: Option Type field of the Jumbo
                  Payload option
```

RQ_000_8814 Process IPv6 Packet

RFC2675 3 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node that does not support the Jumbo Payload option receives a packet in which the Payload Length field in the IPv6 Header is not set to zero (0) but there is a Jumbo Payload option present.

Requirement:

The IPv6 node MUST send an ICMPv6 Error Message to the sending address with the Type field set to 4, the Code field set to zero (0) and the Pointer field set to the Option Type field of the Jumbo Payload option.

Specification Text:

A node that does not understand the Jumbo Payload option is expected to respond to erroneously-received jumbograms as follows, according to the IPv6 specification:

```
error: IPv6 Payload Length = 0 and
       IPv6 Next Header = Hop-by-Hop Options
         Code: 0
         Pointer: high-order octet of the IPv6
                  Payload Length
error: IPv6 Payload Length != 0 and
       Jumbo Payload option present
         Code: 2
         Pointer: Option Type field of the Jumbo
                  Payload option
```

RQ_000_8815 UDP Jumbograms

RFC2675 4 MANDATORY

Applies to: Host, Router

Context:

Requirement:

When constructing a UDP packet in which the overall length of the packet is greater than 65,535 octets, an IPv6 node that supports the Jumbo Payload option MUST set the Length field in the UDP Header to zero (0), set the Jumbo Payload Length field in the Jumbo Payload option to the actual length of the UDP Header plus data and calculate the UDP checksum from the value in the Jumbo payload Length field.

Specification Text:

The specific requirements for sending a UDP jumbogram are as follows:

When sending a UDP packet, if and only if the length of the UDP header plus UDP data is greater than 65,535, set the Length field in the UDP header to zero.

The IPv6 packet carrying such a large UDP packet will necessarily include a Jumbo Payload option in a Hop-by-Hop Options header; set the Jumbo Payload Length field of that option to be the actual length of the UDP header plus data, plus the length of all IPv6 extension headers present between the IPv6 header and the UDP header.

For generating the UDP checksum, use the actual length of the UDP header plus data, NOT zero, in the checksum pseudo-header [RFC2460, Section 8.1].

RQ_000_8816 UDP Jumbograms
RFC2675 4 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a UDP packet in which the Length field is set to zero and a Jumbo Payload option is present in the IPv6 Header.
Requirement:
For the purposes of verifying the UDP packet checksum, The IPv6 node MUST calculate the actual length of the UDP Header plus data as the value in the IPv6 Jumbo Payload Length field minus the length of all IPv6 extension headers between the IPv6 Header and the UDP Header.
Specification Text:
The specific requirements for receiving a UDP jumbogram are as follows:

When receiving a UDP packet, if and only if the Length field in the UDP header is zero, calculate the actual length of the UDP header plus data from the IPv6 Jumbo Payload Length field minus the length of all extension headers present between the IPv6 header and the UDP header.

In the unexpected case that the UDP Length field is zero but no Jumbo Payload option is present (i.e., the IPv6 packet is not a jumbogram), use the Payload Length field in the IPv6 header, in place of the Jumbo Payload Length field, in the above calculation.

For verifying the received UDP checksum, use the calculated length of the UDP header plus data, NOT zero, in the checksum pseudo-header.

RQ_000_8817 UDP Jumbograms
RFC2675 4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a UDP packet in which the Length field is set to zero and no Jumbo Payload option is present in the IPv6 Header.
Requirement:
For the purposes of verifying the UDP packet checksum, The IPv6 node MUST calculate the actual length of the UDP Header plus data as the value in the IPv6 Payload Length field minus the length of all IPv6 extension headers between the IPv6 Header and the UDP Header.
Specification Text:
The specific requirements for receiving a UDP jumbogram are as follows:

When receiving a UDP packet, if and only if the Length field in the UDP header is zero, calculate the actual length of the UDP header plus data from the IPv6 Jumbo Payload Length field minus the length of all extension headers present between the IPv6 header and the UDP header.

In the unexpected case that the UDP Length field is zero but no Jumbo Payload option is present (i.e., the IPv6 packet is not a jumbogram), use the Payload Length field in the IPv6 header, in place of the Jumbo Payload Length field, in the above calculation.

For verifying the received UDP checksum, use the calculated length of the UDP header plus data, NOT zero, in the checksum pseudo-header.

RQ_000_8818 TCP Jumbograms
RFC2675 5.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When establishing a TCP connection on a interface where the MTU minus 60 is greater than or equal to 65,535, an IPv6 node MUST send a Maximum Segment Size (MSS) of 65,535 in its initial TCP negotiation.
Specification Text:
When determining what MSS value to send, if the MTU of the directly attached interface minus 60 [IPv6, Section 8.3] is greater than or equal to 65,535, then set the MSS value to 65,535.

RQ_000_8819 TCP Jumbograms
RFC2675 5.1 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives a TCP Jumbogram with the Maximum Segment Size value in the TCP header set to 65,535.
Requirement:
The IPv6 node MUST assume an infinite Maximum Segment Size (MSS) and calculate the actual MSS by subtracting 60 from the value established by performing IPv6 Path MTU Discovery over the path to the TCP peer.
Specification Text:
When an MSS value of 65,535 is received, it is to be treated as infinity. The actual MSS is determined by subtracting 60 from the value learned by performing Path MTU Discovery [RFC1981] over the path to the TCP peer.

RQ_000_8820 TCP Jumbograms
RFC2675 5.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a TCP packet in which the URG bit field is to be set to one (1), an IPv6 node MUST set the Urgent Pointer to the offset in octets between the TCP Sequence Number field and the urgent Pointer field if that offset is less than 65,535.
Specification Text:
When a TCP packet is to be sent with an Urgent Pointer (i.e., the URG bit set), first calculate the offset from the Sequence Number to the Urgent Pointer. If the offset is less than 65,535, fill in the Urgent field and continue with the normal TCP processing. If the offset is greater than 65,535, and the offset is greater than or equal to the length of the TCP data, fill in the Urgent Pointer with 65,535 and continue with the normal TCP processing. Otherwise, the TCP packet must be split into two pieces. The first piece contains data up to, but not including the data pointed to by the Urgent Pointer, and the Urgent field is set to 65,535 to indicate that the Urgent Pointer is beyond the end of this packet. The second piece can then be sent with the Urgent field set normally.

RQ_000_8821 TCP Jumbograms
RFC2675 5.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a TCP packet in which the URG bit field is to be set to one (1), an IPv6 node MUST set the Urgent Pointer to 65,535 if the offset in octets between the TCP Sequence Number field and the urgent Pointer field if that offset is greater than 65,535 and greater than or equal to the length of TCP data.
Specification Text:
When a TCP packet is to be sent with an Urgent Pointer (i.e., the URG bit set), first calculate the offset from the Sequence Number to the Urgent Pointer. If the offset is less than 65,535, fill in the Urgent field and continue with the normal TCP processing. **If the offset is greater than 65,535, and the offset is greater than or equal to the length of the TCP data, fill in the Urgent Pointer with 65,535 and continue with the normal TCP processing.** Otherwise, the TCP packet must be split into two pieces. The first piece contains data up to, but not including the data pointed to by the Urgent Pointer, and the Urgent field is set to 65,535 to indicate that the Urgent Pointer is beyond the end of this packet. The second piece can then be sent with the Urgent field set normally.

RQ_000_8822 TCP Jumbograms
RFC2675 5.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing a TCP packet in which the URG bit field is to be set to one (1), an IPv6 node MUST split the TCP packet into two parts, as follows, to be sent in separate packets if the offset in octets between the TCP Sequence Number field and the urgent Pointer field if that offset is greater than 65,535 and less than the length of TCP data:

Packet	Urgent Pointer contents	TCP Data included
1	65,535	Data up to, but not including the data pointer to by the Urgent Pointer field
2	End of the packet	Remaining data

Specification Text:
When a TCP packet is to be sent with an Urgent Pointer (i.e., the URG bit set), first calculate the offset from the Sequence Number to the Urgent Pointer. If the offset is less than 65,535, fill in the Urgent field and continue with the normal TCP processing. If the offset is greater than 65,535, and the offset is greater than or equal to the length of the TCP data, fill in the Urgent Pointer with 65,535 and continue with the normal TCP processing. **Otherwise, the TCP packet must be split into two pieces. The first piece contains data up to, but not including the data pointed to by the Urgent Pointer, and the Urgent field is set to 65,535 to indicate that the Urgent Pointer is beyond the end of this packet. The second piece can then be sent with the Urgent field set normally.**

RQ_000_8823 Jumbograms
RFC2675 5.2 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives a TCP packet in which the Urgent bit field is set to one (1) and the Urgent Pointer field contains the decimal value 65,535.
Requirement:
The IPv6 node MUST process the packet using an offset equal to the length of the TCP data instead of the value received in the Urgent Pointer field.
Specification Text:
For TCP input processing, when a TCP packet is received with the URG bit set and an Urgent field of 65,535, the Urgent Pointer is calculated using an offset equal to the length of the TCP data, rather than the offset in the Urgent field.

4.11 Requirements extracted from RFC 3513

RQ_000_1600 Interface Identifiers
RFC3513 2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
If an IPv6 node ascribes an identifier to an interface or set of interfaces, that identifier MUST be 128 bits (16 octets) in length.
Specification Text:
IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces (where "interface" is as defined in section 2 of RFC2460). There are three types of addresses:

Unicast: An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

Anycast: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance).

```
Multicast:  An identifier for a set of interfaces (typically belonging
            to different nodes).  A packet sent to a multicast address
            is delivered to all interfaces identified by that address.
```

RQ_000_1611 Address Architecture
RFC3513 2.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST make it possible for IPv6 addresses of any type to be assigned to interfaces.
Specification Text:
IPv6 addresses of all types are assigned to interfaces, not nodes. An IPv6 unicast address refers to a single interface. Since each interface belongs to a single node, any of that node's interfaces' unicast addresses may be used as an identifier for the node.

RQ_000_1613 Link-local Address
RFC3513 2.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST make it possible for at least one link-local unicast address to be assigned to each of its interfaces.
Specification Text:
All interfaces are required to have at least one link-local unicast address (see section 2.8 for additional required addresses). A single interface may also have multiple IPv6 addresses of any type (unicast, anycast, and multicast) or scope. Unicast addresses with scope greater than link-scope are not needed for interfaces that are not used as the origin or destination of any IPv6 packets to or from non-neighbors. This is sometimes convenient for point-to-point interfaces. There is one exception to this addressing model:

```
   A unicast address or a set of unicast addresses may be assigned to
   multiple physical interfaces if the implementation treats the
   multiple physical interfaces as one interface when presenting it
   to the internet layer.  This is useful for load-sharing over
   multiple physical interfaces.
```

Currently IPv6 continues the IPv4 model that a subnet prefix is associated with one link. Multiple subnet prefixes may be assigned to the same link.

RQ_000_1614 Address Architecture
RFC3513 2.1 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MAY make it possible for multiple IPv6 addresses of any type (unicast, anycast, and multicast) or any scope to be assigned to each of its interfaces.
Specification Text:
All interfaces are required to have at least one link-local unicast address (see section 2.8 for additional required addresses). **A single interface may also have multiple IPv6 addresses of any type (unicast, anycast, and multicast) or scope.** Unicast addresses with scope greater than link-scope are not needed for interfaces that are not used as the origin or destination of any IPv6 packets to or from non-neighbors. This is sometimes convenient for point-to-point interfaces. There is one exception to this addressing model:

```
   A unicast address or a set of unicast addresses may be assigned to
   multiple physical interfaces if the implementation treats the
   multiple physical interfaces as one interface when presenting it
   to the internet layer.  This is useful for load-sharing over
   multiple physical interfaces.
```

Currently IPv6 continues the IPv4 model that a subnet prefix is associated with one link. Multiple subnet prefixes may be assigned to the same link.

RQ_000_1617 Unicast Address
RFC3513 2.1 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MAY make it possible for a unicast address or set of addresses to be assigned to multiple physical interfaces.
Specification Text:
All interfaces are required to have at least one link-local unicast address (see section 2.8 for additional required addresses). A single interface may also have multiple IPv6 addresses of any type (unicast, anycast, and multicast) or scope. Unicast addresses with scope greater than link-scope are not needed for interfaces that are not used as the origin or destination of any IPv6 packets to or from non-neighbors. This is sometimes convenient for point-to-point interfaces. **There is one exception to this addressing model:**

A unicast address or a set of unicast addresses may be assigned to multiple physical interfaces if the implementation treats the multiple physical interfaces as one interface when presenting it to the internet layer. This is useful for load-sharing over multiple physical interfaces.

Currently IPv6 continues the IPv4 model that a subnet prefix is associated with one link. Multiple subnet prefixes may be assigned to the same link.

RQ_000_1618 Address Architecture
RFC3513 2.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT permit a single subnet prefix to be associated with more than one link.
Specification Text:
All interfaces are required to have at least one link-local unicast address (see section 2.8 for additional required addresses). A single interface may also have multiple IPv6 addresses of any type (unicast, anycast, and multicast) or scope. Unicast addresses with scope greater than link-scope are not needed for interfaces that are not used as the origin or destination of any IPv6 packets to or from non-neighbors. This is sometimes convenient for point-to-point interfaces. There is one exception to this addressing model:

A unicast address or a set of unicast addresses may be assigned to multiple physical interfaces if the implementation treats the multiple physical interfaces as one interface when presenting it to the internet layer. This is useful for load-sharing over multiple physical interfaces.

Currently IPv6 continues the IPv4 model that **a subnet prefix is associated with one link**. Multiple subnet prefixes may be assigned to the same link.

RQ_000_1619 Address Architecture
RFC3513 2.1 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IpV6 node MAY make it possible multiple subnet prefixes to be assigned to a single link.
Specification Text:
All interfaces are required to have at least one link-local unicast address (see section 2.8 for additional required addresses). A single interface may also have multiple IPv6 addresses of any type (unicast, anycast, and multicast) or scope. Unicast addresses with scope greater than link-scope are not needed for interfaces that are not used as the origin or destination of any IPv6 packets to or from non-neighbors. This is sometimes convenient for point-to-point interfaces. There is one exception to this addressing model:

A unicast address or a set of unicast addresses may be assigned to multiple physical interfaces if the implementation treats the multiple physical interfaces as one interface when presenting it to the internet layer. This is useful for load-sharing over multiple physical interfaces.

Currently IPv6 continues the IPv4 model that a subnet prefix is associated with one link. **Multiple subnet prefixes may be assigned to the same link**.

RQ_000_1629 Unspecified Address
RFC3513 2.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing an Unspecified IPv6 address, an IPv6 node MUST set each of the 128 address bits to zero (Hexadecimal 0000:0000:0000:0000:0000:0000:0000:0000).
Specification Text:
The type of an IPv6 address is identified by the high-order bits of the address, as follows:

Address type	Binary prefix	IPv6 notation	Section
Unspecified	**00...0 (128 bits)**	**::/128**	**2.5.2**
Loopback	00...1 (128 bits)	::1/128	2.5.3
Multicast	11111111	FF00::/8	2.7
Link-local unicast	1111111010	FE80::/10	2.5.6
Site-local unicast	1111111011	FEC0::/10	2.5.6
Global unicast	(everything else)		

Anycast addresses are taken from the unicast address spaces (of any scope) and are not syntactically distinguishable from unicast addresses.

RQ_000_1630 Loopback Address
RFC3513 2.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing an IPv6 Loopback address, an IPv6 node MUST set the high-order 127 address bits to zero and the lowest order bit to 1 (Hexadecimal 0000:0000:0000:0000:0000:0000:0000:0001).
Specification Text:
The type of an IPv6 address is identified by the high-order bits of the address, as follows:

Address type	Binary prefix	IPv6 notation	Section
Unspecified	00...0 (128 bits)	::/128	2.5.2
Loopback	**00...1 (128 bits)**	**::1/128**	**2.5.3**
Multicast	11111111	FF00::/8	2.7
Link-local unicast	1111111010	FE80::/10	2.5.6
Site-local unicast	1111111011	FEC0::/10	2.5.6
Global unicast	(everything else)		

Anycast addresses are taken from the unicast address spaces (of any scope) and are not syntactically distinguishable from unicast addresses.

RQ_000_1631 Multicast Address
RFC3513 2.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing an IPv6 multicast address, an IPv6 node MUST set the high-order 8 address bits to the binary value 11111111 (Hexadecimal FF)
Specification Text:
The type of an IPv6 address is identified by the high-order bits of the address, as follows:

Address type	Binary prefix	IPv6 notation	Section
Unspecified	00...0 (128 bits)	::/128	2.5.2
Loopback	00...1 (128 bits)	::1/128	2.5.3
Multicast	**11111111**	**FF00::/8**	**2.7**
Link-local unicast	1111111010	FE80::/10	2.5.6
Site-local unicast	1111111011	FEC0::/10	2.5.6
Global unicast	(everything else)		

Anycast addresses are taken from the unicast address spaces (of any scope) and are not syntactically distinguishable from unicast addresses.

RQ_000_1632 Unicast Address
RFC3513 2.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
When constructing an IPv6 link-local unicast address, an IPv6 node MUST set the high-order 10 address bits to the binary value 1111111010 (Hexadecimal FE8)
Specification Text:
The type of an IPv6 address is identified by the high-order bits of the address, as follows:

Address type	**Binary prefix**	**IPv6 notation**	**Section**
Unspecified	00...0 (128 bits)	::/128	2.5.2
Loopback	00...1 (128 bits)	::1/128	2.5.3
Multicast	11111111	FF00::/8	2.7
Link-local unicast	**1111111010**	**FE80::/10**	**2.5.6**
Site-local unicast	1111111011	FEC0::/10	2.5.6
Global unicast	(everything else)		

Anycast addresses are taken from the unicast address spaces (of any scope) and are not syntactically distinguishable from unicast addresses.

RQ_000_1633 Unicast Address
RFC3513 2.4 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet containing an address that is not the Unspecified address, the Loopback address, a link-local unicast address or a multicast address
Requirement:
The IPv6 node MUST treat the received address as a global unicast address
Specification Text:
The type of an IPv6 address is identified by the high-order bits of the address, as follows:

Address type	**Binary prefix**	**IPv6 notation**	**Section**
Unspecified	00...0 (128 bits)	::/128	2.5.2
Loopback	00...1 (128 bits)	::1/128	2.5.3
Multicast	11111111	FF00::/8	2.7
Link-local unicast	1111111010	FE80::/10	2.5.6
Site-local unicast	1111111011	FEC0::/10	2.5.6
Global unicast	**(everything else)**		

Anycast addresses are taken from the unicast address spaces (of any scope) and are not syntactically distinguishable from unicast addresses.

RQ_000_1634 Anycast Address
RFC3513 2.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST construct an Anycast address from the available unicast address space using the same syntactical form as unicast addresses.

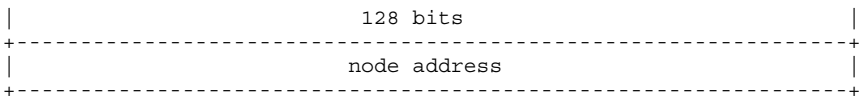
Specification Text:
The type of an IPv6 address is identified by the high-order bits of the address, as follows:

Address type	Binary prefix	IPv6 notation	Section
Unspecified	00...0 (128 bits)	::/128	2.5.2
Loopback	00...1 (128 bits)	::1/128	2.5.3
Multicast	11111111	FF00::/8	2.7
Link-local unicast	1111111010	FE80::/10	2.5.6
Site-local unicast	1111111011	FEC0::/10	2.5.6
Global unicast	(everything else)		

Anycast addresses are taken from the unicast address spaces (of any scope) and are not syntactically distinguishable from unicast addresses.

RQ_000_1638 Unicast Address
RFC3513 2.5 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
An IPv6 node SHOULD NOT impose any specific internal structure on a unicast address associated with any of its interfaces.
Specification Text:
IPv6 nodes may have considerable or little knowledge of the internal structure of the IPv6 address, depending on the role the node plays (for instance, host versus router). **At a minimum, a node may consider that unicast addresses (including its own) have no internal structure**:



RQ_000_1642 Interface Identifiers
RFC3513 2.5.1 MANDATORY
Applies to: Host, Router
Context:

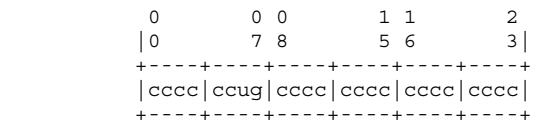
Requirement:
An IPv6 node MUST NOT permit interface identifiers (low order bits of an IPv6 unicast address) to be duplicated within a subnet prefix (high order bits of an IPv6 unicast address).
Specification Text:
Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link. **They are required to be unique within a subnet prefix**. It is recommended that the same interface identifier not be assigned to different nodes on a link. They may also be unique over a broader scope. In some cases an interface's identifier will be derived directly from that interface's link-layer address. The same interface identifier may be used on multiple interfaces on a single node, as long as they are attached to different subnets.

RQ_000_1646 Interface Identifiers
RFC3513 2.5.1 OPTIONAL
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MAY make it possible for an interface identifier (low order bits of IPv6 unicast address) to be used on multiple interfaces if these interfaces all belong to different subnets.
Specification Text:
Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link. They are required to be unique within a subnet prefix. It is recommended that the same interface identifier not be assigned to different nodes on a link. They may also be unique over a broader scope. In some cases an interface's identifier will be derived directly from that interface's link-layer address. **The same interface identifier may be used on multiple interfaces on a single node, as long as they are attached to different subnets**.

RQ_000_1648 Modified EUI64 Interface Identifiers
RFC3513 2.5.1, 2.5.4 -5 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node constructs an IPv6 unicast address with a prefix other than binary 000
Requirement:
The IPv6 node MUST construct the interface identifier that is 64 bits long and in Modified EUI-64 format.
Specification Text:
For all unicast addresses, except those that start with binary value 000, Interface IDs are required to be 64 bits long and to be constructed in Modified EUI-64 format.

RQ_000_1653 With Built-in Device Identifiers
RFC3513 2.5.1 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node derives a Modified EUI-64 interface identifier from an IEEE EUI-64 identifier
Requirement:
The IPv6 node MUST invert the state of bit 6 in the first octet (u bit) of the IEEE EUI-64 identifier.
Specification Text:
Modified EUI-64 format interface identifiers are formed by inverting the "u" bit (universal/local bit in IEEE EUI-64 terminology) when forming the interface identifier from IEEE EUI-64 identifiers. In the resulting Modified EUI-64 format the "u" bit is set to one (1) to indicate global scope, and it is set to zero (0) to indicate local scope. The first three octets in binary of an IEEE EUI-64 identifier are as follows:



written in Internet standard bit-order , where "u" is the universal/local bit, "g" is the individual/group bit, and "c" are the bits of the company_id.

RQ_000_1655 Unspecified Address
RFC3513 2.5.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT permit the address 0:0:0:0:0:0:0:0 (Unspecified address) to be assigned to any interface.
Specification Text:
The address 0:0:0:0:0:0:0:0 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address. One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address.

RQ_000_1658 Unspecified Address
RFC3513 2.5.2 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT set the Destination Address field in any outgoing IPv6 packet to 0:0:0:0:0:0:0:0 (Unspecified address)
Specification Text:
The unspecified address must not be used as the destination address of IPv6 packets or in IPv6 Routing Headers. An IPv6 packet with a source address of unspecified must never be forwarded by an IPv6 router.

RQ_000_1659 Unspecified Address
RFC3513 2.5.2 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT set an Address field in the Routing Header of any outgoing IPv6 packet to 0:0:0:0:0:0:0:0 (Unspecified address)
Specification Text:
The unspecified address must not be used as the destination address of IPv6 packets or **in IPv6 Routing Headers**. An IPv6 packet with a source address of unspecified must never be forwarded by an IPv6 router.

RQ_000_1660 Unspecified Address
RFC3513 2.5.2 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet in which the Source address field is set to 0:0:0:0:0:0:0:1 (Unspecified address)
Requirement:
The IPv6 router MUST NOT forward the IPv6 packet.
Specification Text:
The unspecified address must not be used as the destination address of IPv6 packets or in IPv6 Routing Headers. **An IPv6 packet with a source address of unspecified must never be forwarded by an IPv6 router**.

RQ_000_1662 Loopback Address
RFC3513 2.5.3 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT permit the address 0:0:0:0:0:0:0:1 (Loopback address) to be assigned to any interface.
Specification Text:
The unicast address 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to send an IPv6 packet to itself. **It may never be assigned to any physical interface**. It is treated as having link-local scope, and may be thought of as the link-local unicast address of a virtual interface (typically called "the loopback interface") to an imaginary link that goes nowhere.

RQ_000_1664 Loopback Address
RFC3513 2.5.3 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT set the IPv6 address value 0:0:0:0:0:0:0:1 (Loopback address) in the source address field of any IPv6 packets that are sent outside of the node.
Specification Text:
The unicast address 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to send an IPv6 packet to itself. It may never be assigned to any physical interface. It is treated as having link-local scope, and may be thought of as the link-local unicast address of a virtual interface (typically called "the loopback interface") to an imaginary link that goes nowhere.

The loopback address must not be used as the source address in IPv6 packets that are sent outside of a single node. An IPv6 packet with a destination address of loopback must never be sent outside of a single node and must never be forwarded by an IPv6 router. A packet received on an interface with destination address of loopback must be dropped.

RQ_000_1665 Loopback Address
RFC3513 2.5.3 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT set the IPv6 address value 0:0:0:0:0:0:0:1 (Loopback address) in the destination address field of any IPv6 packets that are sent outside of the node.
Specification Text:
The unicast address 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to send an IPv6 packet to itself. It may never be assigned to any physical interface. It is treated as having link-local scope, and may be thought of as the link-local unicast address of a virtual interface (typically called "the loopback interface") to an imaginary link that goes nowhere.

The loopback address must not be used as the source address in IPv6 packets that are sent outside of a single node. **An IPv6 packet with a destination address of loopback must never be sent outside of a single node** and must never be forwarded by an IPv6 router. A packet received on an interface with destination address of loopback must be dropped.

RQ_000_1666 Loopback Address
RFC3513 2.5.3 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet in which the destination address field is set to the address value 0:0:0:0:0:0:0:1 (Loopback address)
Requirement:
The router MUST NOT forward the IPv6 packet.
Specification Text:
The unicast address 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to send an IPv6 packet to itself. It may never be assigned to any physical interface. It is treated as having link-local scope, and may be thought of as the link-local unicast address of a virtual interface (typically called "the loopback interface") to an imaginary link that goes nowhere.

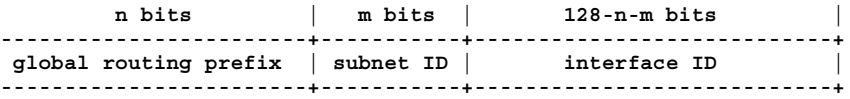
The loopback address must not be used as the source address in IPv6 packets that are sent outside of a single node. **An IPv6 packet with a destination address of loopback** must never be sent outside of a single node and **must never be forwarded by an IPv6 router**. A packet received on an interface with destination address of loopback must be dropped.

RQ_000_1667 Loopback Address
RFC3513 2.5.3 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet in which the destination address field is set to the address value 0:0:0:0:0:0:0:1 (Loopback address)
Requirement:
The IPv6 node MUST drop the IPv6 packet.
Specification Text:
The unicast address 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to send an IPv6 packet to itself. It may never be assigned to any physical interface. It is treated as having link-local scope, and may be thought of as the link-local unicast address of a virtual interface (typically called "the loopback interface") to an imaginary link that goes nowhere.

The loopback address must not be used as the source address in IPv6 packets that are sent outside of a single node. An IPv6 packet with a destination address of loopback must never be sent outside of a single node and must never be forwarded by an IPv6 router. **A packet received on an interface with destination address of loopback must be dropped.**

RQ_000_1668 Unicast Address
RFC3513 2.5.4 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST make it possible for a global unicast address comprising a global routing prefix in its high-order bits, a subnet identifier in its mid-order bits and an interface identifier in its low-order bits to be assigned to an interface
Specification Text:
The general format for IPv6 global unicast addresses is as follows:



where the global routing prefix is a (typically hierarchically- structured) value assigned to a site (a cluster of subnets/links), the subnet ID is an identifier of a link within the site, and the interface ID is as defined in section 2.5.1.

All global unicast addresses other than those that start with binary 000 have a 64-bit interface ID field (i.e., n + m = 64), formatted as described in section 2.5.1. Global unicast addresses that start with binary 000 have no such constraint on the size or structure of the interface ID field.

Examples of global unicast addresses that start with binary 000 are the IPv6 address with embedded IPv4 addresses described in section 2.5.5 and the IPv6 address containing encoded NSAP addresses specified in RFC 18888. An example of global addresses starting with a binary value other than 000 (and therefore having a 64-bit interface ID field) can be found in RFC 2374.

RQ_000_1670 Mapping of IPv4 Addresses
RFC3513 2.5.5 OPTIONAL
Applies to: Router, Host
Context:
An IPv6 node constructs an IPv6 packet which is to be routed over an IPv4 routing infrastructure.
Requirement:
The IPv6 node MAY set the IPv4 address into the low-order 32 bits of the address field with the high order 96 bits set to all-zeros (0).
Specification Text:
The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that use this technique are assigned special IPv6 unicast addresses that carry a global IPv4 address in the low-order 32 bits. This type of address is termed an "IPv4- compatible IPv6 address" and has the format:

```
|               80 bits               | 16 |      32 bits        |
+-------------------------------------+----+---------------------+
|0000.............................0000|0000|    IPv4 address     |
+-------------------------------------+----+---------------------+
```

Note: The IPv4 address used in the "IPv4-compatible IPv6 address" must be a globally-unique IPv4 unicast address.

A second type of IPv6 address which holds an embedded IPv4 address is also defined. This address type is used to represent the addresses of IPv4 nodes as IPv6 addresses. This type of address is termed an "IPv4-mapped IPv6 address" and has the format:

```
|               80 bits               | 16 |      32 bits        |
+-------------------------------------+----+---------------------+
|0000.............................0000|FFFF|    IPv4 address     |
+-------------------------------------+----+---------------------+
```

RQ_000_1673 Mapping of IPv4 Addresses
RFC3513 2.5.5 RECOMMENDED
Applies to: Host, Router
Context:
An IPv6 node constructs an IPv6 packet which is to be routed over an IPv4 routing infrastructure.
Requirement:
The IPv6 node SHOULD set the IPv4 address into the low-order 32 bits of the address field with the next 16 bits set to all ones (hex FFFF) and the high order 80 bits set to all-zeros (0).
Specification Text:
The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that use this technique are assigned special IPv6 unicast addresses that carry a global IPv4 address in the low-order 32 bits. This type of address is termed an "IPv4- compatible IPv6 address" and has the format:

```
|               80 bits               | 16 |      32 bits        |
+-------------------------------------+----+---------------------+
|0000.............................0000|0000|    IPv4 address     |
+-------------------------------------+----+---------------------+
```

Note: The IPv4 address used in the "IPv4-compatible IPv6 address" must be a globally-unique IPv4 unicast address.

A second type of IPv6 address which holds an embedded IPv4 address is also defined. This address type is used to represent the addresses of IPv4 nodes as IPv6 addresses. This type of address is termed an "IPv4-mapped IPv6 address" and has the format:

```
|               80 bits               | 16 |      32 bits        |
+-------------------------------------+----+---------------------+
|0000.............................0000|FFFF|    IPv4 address     |
+-------------------------------------+----+---------------------+
```

RQ_000_1675 Link-local Address
RFC3513 2.5.6 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST interpret any address in the following format as link-Local:

Address Bits	Contents
0 to 63	interface identifier
64 to 117	all zeros
118 to 127	1111111010

Specification Text:
There are two types of local-use unicast addresses defined. These are Link-Local and Site-Local. The Link-Local is for use on a single link and the Site-Local is for use in a single site. **Link-Local addresses have the following format:**

10 bits	**54 bits**	**64 bits**
1111111010	**0**	**interface ID**

Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present.

Routers must not forward any packets with link-local source or destination addresses to other links.

RQ_000_1676 Link-local Address
RFC3513 2.5.6 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet in which the source address field is set to a Link-Local address
Requirement:
The IPv6 router MUST NOT forward the packet to other links.
Specification Text:
There are two types of local-use unicast addresses defined. These are Link-Local and Site-Local. The Link-Local is for use on a single link and the Site-Local is for use in a single site. Link-Local addresses have the following format:

10 bits	54 bits	64 bits
1111111010	0	interface ID

Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present.

Routers must not forward any packets with link-local source or destination addresses to other links.

RQ_000_1677 Link-local Address
RFC3513 2.5.6 MANDATORY
Applies to: Router
Context:
An IPv6 router receives an IPv6 packet in which the source address field is set to a Link-Local address
Requirement:
The IPv6 router MUST NOT forward the packet to other links.
Specification Text:
There are two types of local-use unicast addresses defined. These are Link-Local and Site-Local. The Link-Local is for use on a single link and the Site-Local is for use in a single site. Link-Local addresses have the following format:

```
|   10     |
|  bits    |         54 bits         |          64 bits           |
+----------+-------------------------+----------------------------+
|1111111010|           0             |       interface ID         |
+----------+-------------------------+----------------------------+
```

Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present.

Routers must not forward any packets with link-local source or destination addresses to other links.

RQ_000_1678 Anycast Address
RFC3513 2.6 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST make it possible for any of its unicast addresses to be explicitly configured as an anycast address.
Specification Text:
Anycast addresses are allocated from the unicast address space, using any of the defined unicast address formats. Thus, anycast addresses are syntactically indistinguishable from unicast addresses. **When a unicast address is assigned to more than one interface, thus turning it into an anycast address, the nodes to which the address is assigned must be explicitly configured to know that it is an anycast address**.

RQ_000_1687 Anycast Address
RFC3513 2.6.1 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node needs to send a packet to any one of the routers attached to a specific subnet
Requirement:
The IPv6 node constructs the packet with the Destination field set to an address constructed with the appropriate subnet prefix set into the high-order bits and all zeros set into the remaining low-order bits.
Specification Text:
The Subnet-Router anycast address is predefined. Its format is as follows:

```
|                        n bits                 |   128-n bits   |
+-----------------------------------------------+----------------+
|                  subnet prefix                | 00000000000000 |
+-----------------------------------------------+----------------+
```

The "subnet prefix" in an anycast address is the prefix which identifies a specific link. This anycast address is syntactically the same as a unicast address for an interface on the link with the interface identifier set to zero.

Packets sent to the Subnet-Router anycast address will be delivered to one router on the subnet. All routers are required to support the Subnet-Router anycast addresses for the subnets to which they have interfaces.

The subnet-router anycast address is intended to be used for applications where a node needs to communicate with any one of the set of routers.

RQ_000_1688 Anycast Address
RFC3513 2.6.1 MANDATORY
Applies to: Router
Context:
An IPv6 router receives a packet in which the high-order bits of the Destination Address field are set to the subnet prefix of one of subnets to which the router has an interface and the remaining low-order bits are set to all zeros.
Requirement:
The IPv6 router MUST treat this packet as one sent to a Subnet-Router Anycast address.
Specification Text:
The Subnet-Router anycast address is predefined. Its format is as follows:

n bits	**128-n bits**
subnet prefix	**00000000000000**

The "subnet prefix" in an anycast address is the prefix which identifies a specific link. This anycast address is syntactically the same as a unicast address for an interface on the link with the interface identifier set to zero.

Packets sent to the Subnet-Router anycast address will be delivered to one router on the subnet. All routers are required to support the Subnet-Router anycast addresses for the subnets to which they have interfaces.

The subnet-router anycast address is intended to be used for applications where a node needs to communicate with any one of the set of routers.

RQ_000_1689 Multicast Address
RFC3513 2.7 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST make it possible for any of its interfaces to be assigned to any number of multicast groups.
Specification Text:
An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. Multicast addresses have the following format:

8	4	4	112 bits
11111111	flgs	scop	group ID

binary 11111111 at the start of the address identifies the address as being a multicast address.

flgs is a set of 4 flags:

0	0	0	T

The high-order 3 flags are reserved, and must be initialized to 0.

T = 0 indicates a permanently-assigned ("well-known") multicast address, assigned by the Internet Assigned Number Authority (IANA).

T = 1 indicates a non-permanently-assigned ("transient") multicast address.

scop is a 4-bit multicast scope value used to limit the scope of the multicast group. The values are:

0 reserved
1 interface-local scope
2 link-local scope
3 reserved
4 admin-local scope
5 site-local scope
6 (unassigned)
7 (unassigned)
8 organization-local scope

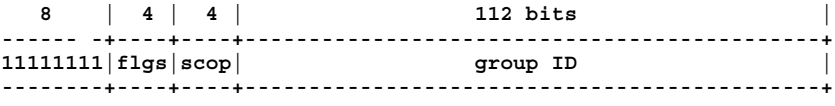
```
   9  (unassigned)
   A  (unassigned)
   B  (unassigned)
   C  (unassigned)
   D  (unassigned)
   E  global scope
   F  reserved

   interface-local scope spans only a single interface on a node, and is useful only
   for loopback transmission of multicast.

   link-local and site-local multicast scopes span the same topological regions as the
   corresponding unicast scopes.

   admin-local scope is the smallest scope that must be administratively configured,
   i.e., not automatically derived from physical connectivity or other,
   non- multicast-related configuration.

   organization-local scope is intended to span multiple sites belonging to a single
   organization.

   scopes labeled "(unassigned)" are available for administrators to define additional
   multicast regions.

group ID identifies the multicast group, either permanent or transient, within the
given scope.
```

RQ_000_1690 Multicast Address
RFC3513 2.7 MANDATORY
Applies to: Host, Router
Context:

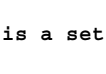
Requirement:
An IPv6 node MUST construct an IPv6 multicast address in the following format:

Bit position	Value
121 - 128	FF hex
118 - 120	0 (zero)
117	T flag
113 - 116	scop field
001 - 112	multicast group ID

Specification Text:
An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. **Multicast addresses have the following format:**



binary 11111111 at the start of the address identifies the address as being a multicast address.



flgs is a set of 4 flags:

The high-order 3 flags are reserved, and must be initialized to 0.

T = 0 indicates a permanently-assigned ("well-known") multicast address, assigned by the Internet Assigned Number Authority (IANA).

T = 1 indicates a non-permanently-assigned ("transient") multicast address.

scop is a 4-bit multicast scope value used to limit the scope of the multicast group. The values are:

```
   0  reserved
   1  interface-local scope
   2  link-local scope
   3  reserved
   4  admin-local scope
```

```
   5  site-local scope
   6  (unassigned)
   7  (unassigned)
   8  organization-local scope
   9  (unassigned)
   A  (unassigned)
   B  (unassigned)
   C  (unassigned)
   D  (unassigned)
   E  global scope
   F  reserved

   interface-local scope spans only a single interface on a node, and is useful only
   for loopback transmission of multicast.

   link-local and site-local multicast scopes span the same topological regions as the
   corresponding unicast scopes.

   admin-local scope is the smallest scope that must be administratively configured,
   i.e., not automatically derived from physical connectivity or other,
   non- multicast-related configuration.

   organization-local scope is intended to span multiple sites belonging to a single
   organization.

   scopes labeled "(unassigned)" are available for administrators to define additional
   multicast regions.
```

group ID identifies the multicast group, either permanent or transient, within the given scope.

RQ_000_1691 Multicast Address

RFC3513 2.7 MANDATORY

Applies to: Router, Host

Context:

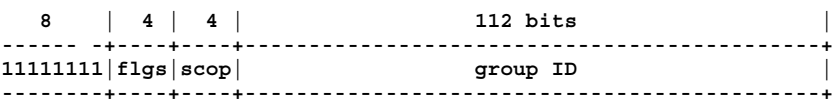
An IPv6 node constructs a transient multicast address (i.e., one that has not been preassigned by IANA)

Requirement:

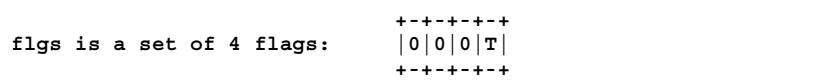
The IPv6 node MUST set the T flag (bit 117) in the multicast address to one (1)

Specification Text:

An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. **Multicast addresses have the following format:**



binary 11111111 at the start of the address identifies the address as being a multicast address.



The high-order 3 flags are reserved, and must be initialized to 0.

T = 0 indicates a permanently-assigned ("well-known") multicast address, assigned by the Internet Assigned Number Authority (IANA).

T = 1 indicates a non-permanently-assigned ("transient") multicast address.

```
scop is a 4-bit multicast scope value used to limit the scope of the multicast group.
The values are:

   0  reserved
   1  interface-local scope
   2  link-local scope
   3  reserved
   4  admin-local scope
   5  site-local scope
   6  (unassigned)
```

```
   7  (unassigned)
   8  organization-local scope
   9  (unassigned)
   A  (unassigned)
   B  (unassigned)
   C  (unassigned)
   D  (unassigned)
   E  global scope
   F  reserved

   interface-local scope spans only a single interface on a node, and is useful only
   for loopback transmission of multicast.

   link-local and site-local multicast scopes span the same topological regions as the
   corresponding unicast scopes.

   admin-local scope is the smallest scope that must be administratively configured,
   i.e., not automatically derived from physical connectivity or other,
   non- multicast-related configuration.

   organization-local scope is intended to span multiple sites belonging to a single
   organization.

   scopes labeled "(unassigned)" are available for administrators to define additional
   multicast regions.

group ID identifies the multicast group, either permanent or transient, within the
given scope.
```

RQ_000_1692 Multicast Address

RFC3513 2.7 MANDATORY

Applies to: Router, Host

Context:

An IPv6 node constructs a transient IPv6 multicast address whose scope is limited to a single interface on the node (i.e., for the purpose of loopback transmission of multicast)

Requirement:

The IPv6 node MUST set the scop field (bits 113 to 116) in the multicast address to the value one (1)

Specification Text:

An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. **Multicast addresses have the following format:**

```
  binary 11111111 at the start of the address identifies the
  address as being a multicast address.

                                +-+-+-+-+
  flgs is a set of 4 flags:     |0|0|0|T|
                                +-+-+-+-+

     The high-order 3 flags are reserved, and must be initialized to 0.

        T = 0 indicates a permanently-assigned ("well-known") multicast address,
        assigned
        by the Internet Assigned Number Authority (IANA).

        T = 1 indicates a non-permanently-assigned ("transient") multicast address.
```

scop is a 4-bit multicast scope value used to limit the scope of the multicast group. The values are:

```
   0  reserved
   1  interface-local scope
   2  link-local scope
   3  reserved
   4  admin-local scope
   5  site-local scope
   6  (unassigned)
   7  (unassigned)
```

8 organization-local scope
9 (unassigned)
A (unassigned)
B (unassigned)
C (unassigned)
D (unassigned)
E global scope
F reserved

interface-local scope spans only a single interface on a node, and is useful only for loopback transmission of multicast.

link-local and site-local multicast scopes span the same topological regions as the corresponding unicast scopes.

admin-local scope is the smallest scope that must be administratively configured, i.e., not automatically derived from physical connectivity or other, non- multicast-related configuration.

organization-local scope is intended to span multiple sites belonging to a single organization.

scopes labeled "(unassigned)" are available for administrators to define additional multicast regions.

group ID identifies the multicast group, either permanent or transient, within the given scope.

RQ_000_1693 Multicast Address

RFC3513 2.7 MANDATORY

Applies to: Router, Host

Context:

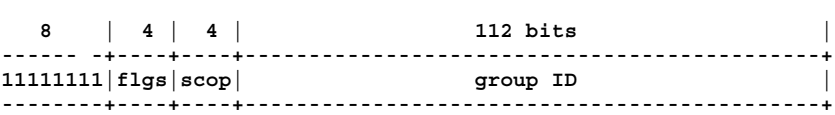
An IPv6 node constructs a transient IPv6 multicast address whose scope is limited to link-local

Requirement:

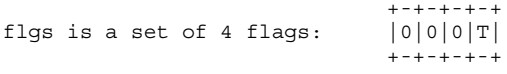
The IPv6 node MUST set the scop field (bits 113 to 116) in the multicast address to the value 2

Specification Text:

An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. **Multicast addresses have the following format:**



binary 11111111 at the start of the address identifies the address as being a multicast address.



The high-order 3 flags are reserved, and must be initialized to 0.

T = 0 indicates a permanently-assigned ("well-known") multicast address, assigned by the Internet Assigned Number Authority (IANA).

T = 1 indicates a non-permanently-assigned ("transient") multicast address.

scop is a 4-bit multicast scope value used to limit the scope of the multicast group. The values are:

0 reserved
1 interface-local scope
2 link-local scope
3 reserved
4 admin-local scope
5 site-local scope
6 (unassigned)
7 (unassigned)
8 organization-local scope

9 (unassigned)
A (unassigned)
B (unassigned)
C (unassigned)
D (unassigned)
E global scope
F reserved

interface-local scope spans only a single interface on a node, and is useful only for loopback transmission of multicast.

link-local and site-local multicast scopes span the same topological regions as the corresponding unicast scopes.

admin-local scope is the smallest scope that must be administratively configured, i.e., not automatically derived from physical connectivity or other, non- multicast-related configuration.

organization-local scope is intended to span multiple sites belonging to a single organization.

scopes labeled "(unassigned)" are available for administrators to define additional multicast regions.

group ID identifies the multicast group, either permanent or transient, within the given scope.

RQ_000_1694 Multicast Address

RFC3513 2.7 MANDATORY

Applies to: Router, Host

Context:

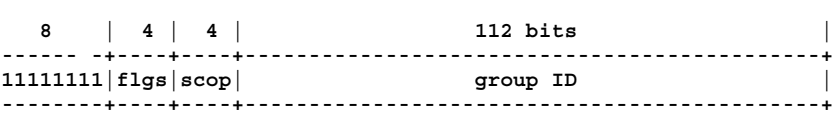
An IPv6 node constructs a transient IPv6 multicast address whose scope is limited to admin-local

Requirement:

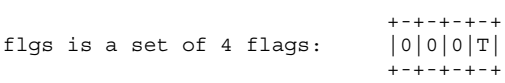
The IPv6 node MUST set the scop field (bits 113 to 116) in the multicast address to the value 4

Specification Text:

An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. **Multicast addresses have the following format:**



binary 11111111 at the start of the address identifies the address as being a multicast address.



The high-order 3 flags are reserved, and must be initialized to 0.

T = 0 indicates a permanently-assigned ("well-known") multicast address, assigned by the Internet Assigned Number Authority (IANA).

T = 1 indicates a non-permanently-assigned ("transient") multicast address.

scop is a 4-bit multicast scope value used to limit the scope of the multicast group. The values are:

0 reserved
1 interface-local scope
2 link-local scope
3 reserved
4 admin-local scope
5 site-local scope
6 (unassigned)
7 (unassigned)

```
   8  organization-local scope
   9  (unassigned)
   A  (unassigned)
   B  (unassigned)
   C  (unassigned)
   D  (unassigned)
   E  global scope
   F  reserved

   interface-local scope spans only a single interface on a node, and is useful only
   for loopback transmission of multicast.

   link-local and site-local multicast scopes span the same topological regions as the
   corresponding unicast scopes.

   admin-local scope is the smallest scope that must be administratively configured,
   i.e., not automatically derived from physical connectivity or other,
   non- multicast-related configuration.


   organization-local scope is intended to span multiple sites belonging to a single
   organization.

   scopes labeled "(unassigned)" are available for administrators to define additional
   multicast regions.

group ID identifies the multicast group, either permanent or transient, within the
given scope.
```

RQ_000_1695 Multicast Address

RFC3513 2.7 MANDATORY

Applies to: Router, Host

Context:

An IPv6 node constructs a transient IPv6 multicast address whose scope is limited to a single administrative site

Requirement:

The IPv6 node MUST set the scop field (bits 113 to 116) in the multicast address to the value 5

Specification Text:

An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. Multicast addresses have the following format:

```
|   8    |  4 |  4 |                  112 bits                   |
+------ -+----+----+---------------------------------------------+
|11111111|flgs|scop|                  group ID                   |
+--------+----+----+---------------------------------------------+
```

```
binary 11111111 at the start of the address identifies the
address as being a multicast address.

                               +-+-+-+-+
flgs is a set of 4 flags:      |0|0|0|T|
                               +-+-+-+-+

   The high-order 3 flags are reserved, and must be initialized to 0.

      T = 0 indicates a permanently-assigned ("well-known") multicast address,
      assigned
      by the Internet Assigned Number Authority (IANA).

      T = 1 indicates a non-permanently-assigned ("transient") multicast address.

scop is a 4-bit multicast scope value used to limit the scope of the multicast group.
The values are:

   0  reserved
   1  interface-local scope
   2  link-local scope
   3  reserved
   4  admin-local scope
   5  site-local scope
   6  (unassigned)
   7  (unassigned)
   8  organization-local scope
```

```
   9  (unassigned)
   A  (unassigned)
   B  (unassigned)
   C  (unassigned)
   D  (unassigned)
   E  global scope
   F  reserved

   interface-local scope spans only a single interface on a node, and is useful only
   for loopback transmission of multicast.

   link-local and site-local multicast scopes span the same topological regions as the
   corresponding unicast scopes.


   admin-local scope is the smallest scope that must be administratively configured,
   i.e., not automatically derived from physical connectivity or other,
   non- multicast-related configuration.


   organization-local scope is intended to span multiple sites belonging to a single
   organization.

   scopes labeled "(unassigned)" are available for administrators to define additional
   multicast regions.

group ID identifies the multicast group, either permanent or transient, within the
given scope.
```

RQ_000_1696 Multicast Address

RFC3513 2.7 MANDATORY

Applies to: Router, Host

Context:

An IPv6 node constructs a transient IPv6 multicast address whose scope is limited to multiple administrative sites

Requirement:

The IPv6 node MUST set the scop field (bits 113 to 116) in the multicast address to the value 8

Specification Text:

An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. Multicast addresses have the following format:

```
|   8    |  4 |  4 |                  112 bits                   |
+------ -+----+----+---------------------------------------------+
|11111111|flgs|scop|                  group ID                   |
+--------+----+----+---------------------------------------------+
```

```
  binary 11111111 at the start of the address identifies the
  address as being a multicast address.

                                +-+-+-+-+
  flgs is a set of 4 flags:     |0|0|0|T|
                                +-+-+-+-+

     The high-order 3 flags are reserved, and must be initialized to 0.

        T = 0 indicates a permanently-assigned ("well-known") multicast address,
        assigned
        by the Internet Assigned Number Authority (IANA).

        T = 1 indicates a non-permanently-assigned ("transient") multicast address.

  scop is a 4-bit multicast scope value used to limit the scope of the multicast group.
  The values are:

     0  reserved
     1  interface-local scope
     2  link-local scope
     3  reserved
     4  admin-local scope
     5  site-local scope
     6  (unassigned)
     7  (unassigned)
     8  organization-local scope
```

```
9  (unassigned)
A  (unassigned)
B  (unassigned)
C  (unassigned)
D  (unassigned)
E  global scope
F  reserved

interface-local scope spans only a single interface on a node, and is useful only
for loopback transmission of multicast.

link-local and site-local multicast scopes span the same topological regions as the
corresponding unicast scopes.


admin-local scope is the smallest scope that must be administratively configured,
i.e., not automatically derived from physical connectivity or other,
non- multicast-related configuration.


organization-local scope is intended to span multiple sites belonging to a single
organization.

scopes labeled "(unassigned)" are available for administrators to define additional
multicast regions.

group ID identifies the multicast group, either permanent or transient, within the
given scope.
```

RQ_000_1697 Multicast Address

RFC3513 2.7 MANDATORY

Applies to: Host, Router

Context:

An IPv6 node constructs a transient IPv6 multicast address whose scope is unlimited

Requirement:

The IPv6 node MUST set the scop field (bits 113 to 116) in the multicast address to the hexadecimal value E

Specification Text:

An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. Multicast addresses have the following format:

```
|   8    |  4 |  4 |                  112 bits                   |
+------ -+----+----+---------------------------------------------+
|11111111|flgs|scop|                  group ID                   |
+--------+----+----+---------------------------------------------+
```

```
binary 11111111 at the start of the address identifies the
address as being a multicast address.

                                +-+-+-+-+
flgs is a set of 4 flags:       |0|0|0|T|
                                +-+-+-+-+

   The high-order 3 flags are reserved, and must be initialized to 0.

      T = 0 indicates a permanently-assigned ("well-known") multicast address,
      assigned
      by the Internet Assigned Number Authority (IANA).

      T = 1 indicates a non-permanently-assigned ("transient") multicast address.
```

scop is a 4-bit multicast scope value used to limit the scope of the multicast group. The values are:

```
0  reserved
1  interface-local scope
2  link-local scope
3  reserved
4  admin-local scope
5  site-local scope
6  (unassigned)
7  (unassigned)
8  organization-local scope
```

9 (unassigned)
A (unassigned)
B (unassigned)
C (unassigned)
D (unassigned)
E global scope
F reserved

interface-local scope spans only a single interface on a node, and is useful only for loopback transmission of multicast.

link-local and site-local multicast scopes span the same topological regions as the corresponding unicast scopes.

admin-local scope is the smallest scope that must be administratively configured, i.e., not automatically derived from physical connectivity or other, non- multicast-related configuration.

organization-local scope is intended to span multiple sites belonging to a single organization.

scopes labeled "(unassigned)" are available for administrators to define additional multicast regions.

group ID identifies the multicast group, either permanent or transient, within the given scope.

RQ_000_1698 Multicast Address

RFC3513 2.7 OPTIONAL

Applies to: Host, Router

Context:

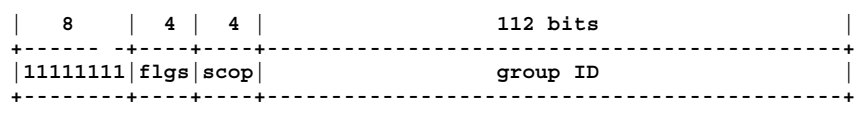
An IPv6 node constructs a transient IPv6 multicast address whose scope is administration-specific (i.e., not interface-local, link-local, site-local, organization-local or global)

Requirement:

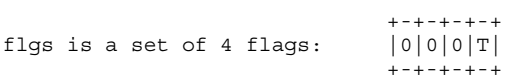
The IPv6 node MAY set the scop field (bits 113 to 116) in the multicast address to any of the hexadecimal values 6, 7, 9, A, B, C or D.

Specification Text:

An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. Multicast addresses have the following format:



binary 11111111 at the start of the address identifies the address as being a multicast address.



The high-order 3 flags are reserved, and must be initialized to 0.

T = 0 indicates a permanently-assigned ("well-known") multicast address, assigned by the Internet Assigned Number Authority (IANA).

T = 1 indicates a non-permanently-assigned ("transient") multicast address.

scop is a 4-bit multicast scope value used to limit the scope of the multicast group. The values are:

0 reserved
1 interface-local scope
2 link-local scope
3 reserved
4 admin-local scope
5 site-local scope
6 (unassigned)

7 (unassigned)
8 organization-local scope
9 (unassigned)
A (unassigned)
B (unassigned)
C (unassigned)
D (unassigned)
E global scope
F reserved

interface-local scope spans only a single interface on a node, and is useful only for loopback transmission of multicast.

link-local and site-local multicast scopes span the same topological regions as the corresponding unicast scopes.

admin-local scope is the smallest scope that must be administratively configured, i.e., not automatically derived from physical connectivity or other, non- multicast-related configuration.

organization-local scope is intended to span multiple sites belonging to a single organization.

scopes labeled "(unassigned)" are available for administrators to define additional multicast regions.

group ID identifies the multicast group, either permanent or transient, within the given scope.

RQ_000_1707 Multicast Address Behavior
RFC3513 2.7 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT set the value in the source address field of an outgoing IPv6 packet to a multicast address.
Specification Text:
Multicast addresses must not be used as source addresses in IPv6 packets or appear in any Routing header.

RQ_000_1708 Multicast Address Behavior
RFC3513 2.7 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT set the value of any of the address fields in the Routing Header of an IPv6 packet to a multicast address.
Specification Text:
Multicast addresses must not be used as source addresses in IPv6 packets or appear in any Routing header.

RQ_000_1709 Multicast Address Behavior
RFC3513 2.7 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 router MUST NOT forward any multicast packet beyond the scope indicated by the scop field in the destination multicast address.
Specification Text:
Routers must not forward any multicast packets beyond of the scope indicated by the scop field in the destination multicast address.

RQ_000_1710 Multicast Address Behavior
RFC3513 2.7 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT send an IPv6 packet in which the destination address field contains a multicast address with its scop field set to the value zero (0).
Specification Text:
Nodes must not originate a packet to a multicast address whose scop field contains the reserved value 0; if such a packet is received, it must be silently dropped. Nodes should not originate a packet to a multicast address whose scop field contains the reserved value F; if such a packet is sent or received, it must be treated the same as packets destined to a global (scop E) multicast address.

RQ_000_1711 Multicast Address Behavior
RFC3513 2.7 MANDATORY
Applies to: Router, Host
Context:
An IPv6 node receives an IPv6 packet in which the destination address field contains a multicast address with its scop field set to the value zero (0).
Requirement:
The IPv6 node MUST silently drop the multicast packet.
Specification Text:
Nodes must not originate a packet to a multicast address whose scop field contains the reserved value 0; **if such a packet is received, it must be silently dropped.** Nodes should not originate a packet to a multicast address whose scop field contains the reserved value F; if such a packet is sent or received, it must be treated the same as packets destined to a global (scop E) multicast address.

RQ_000_1712 Multicast Address Behavior
RFC3513 2.7 RECOMMENDED
Applies to: Host, Router
Context:

Requirement:
An IPv6 node SHOULD NOT send an IPv6 packet in which the destination address field contains a multicast address with its scop field set to the hexadecimal value F.
Specification Text:
Nodes must not originate a packet to a multicast address whose scop field contains the reserved value 0; if such a packet is received, it must be silently dropped. **Nodes should not originate a packet to a multicast address whose scop field contains the reserved value F;** if such a packet is sent or received, it must be treated the same as packets destined to a global (scop E) multicast address.

RQ_000_1713 Multicast Address Behavior
RFC3513 2.7 MANDATORY
Applies to: Host, Router
Context:
An IPv6 node receives an IPv6 packet in which the destination address field contains a multicast address with its scop field set to the hexadecimal value F.
Requirement:
The IPv6 node MUST process the packet in the same way as a packet destined to a global (scop E) multicast address.
Specification Text:
Nodes must not originate a packet to a multicast address whose scop field contains the reserved value 0; if such a packet is received, it must be silently dropped. Nodes should not originate a packet to a multicast address whose scop field contains the reserved value F; **if such a packet is sent or received, it must be treated the same as packets destined to a global (scop E) multicast address.**

RQ_000_1714 Multicast Address
RFC3513 2.7.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST NOT construct a multicast IPv6 address containing a Group ID set to the values 0:0:0:0:0:0:1, 0:0:0:0:0:0:2, 0:0:0:0:0:0:5 or 0:0:0:0:1:FF00:0000 to 0:0:0:0:1:FFFF:FFFF with the T flag set to zero (0) unless the address is an All Nodes multicast address, an All Routers multicast address or a Solicited-node multicast address.

Specification Text:
The following well-known multicast addresses are pre-defined. **The group ID's defined in this section are defined for explicit scope values.**

Use of these group IDs for any other scope values, with the T flag equal to 0, is not allowed.

RQ_000_1715 Multicast Address
RFC3513 2.7.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
An IPv6 node MUST NOT assign the following addresses to any multicast group:

FF00:0:0:0:0:0:0:0	FF06:0:0:0:0:0:0:0	FF0C:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0	FF07:0:0:0:0:0:0:0	FF0D:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0	FF08:0:0:0:0:0:0:0	FF0E:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0	FF09:0:0:0:0:0:0:0	FF0F:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0	FF0A:0:0:0:0:0:0:0	
FF05:0:0:0:0:0:0:0	FF0B:0:0:0:0:0:0:0	

Specification Text:
The following well-known multicast addresses are pre-defined. The group ID's defined in this section are defined for explicit scope values.

Use of these group IDs for any other scope values, with the T flag equal to 0, is not allowed.

Reserved Multicast Addresses: FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

The above multicast addresses are reserved and shall never be assigned to any multicast group.

All Nodes Addresses: FF01:0:0:0:0:0:0:1
FF02:0:0:0:0:0:0:1

The above multicast addresses identify the group of all IPv6 nodes, within scope 1 (interface-local) or 2 (link-local).

All Routers Addresses: FF01:0:0:0:0:0:0:2
FF02:0:0:0:0:0:0:2
FF05:0:0:0:0:0:0:2

The above multicast addresses identify the group of all IPv6 routers, within scope 1 (interface-local), 2 (link-local), or 5 (site-local).

Solicited-Node Address: FF02:0:0:0:0:1:FFXX:XXXX

Solicited-node multicast address are computed as a function of a node's unicast and anycast addresses. A solicited-node multicast address is formed by taking the low-order 24 bits of an address (unicast or anycast) and appending those bits to the prefix FF02:0:0:0:0:1:FF00::/104 resulting in a multicast address in the range

FF02:0:0:0:0:1:FF00:0000

to

FF02:0:0:0:0:1:FFFF:FFFF

RQ_000_1716 All Nodes Multicast Addresses
RFC3513 2.7.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
In order to send a multicast IPv6 packet to all its associated interface-local nodes, an IPv6 node MUST set the destination address field in the packet to the address value FF01:0:0:0:0:0:0:1.
Specification Text:
All Nodes Addresses: FF01:0:0:0:0:0:0:1
FF02:0:0:0:0:0:0:1

The above multicast addresses identify the group of all IPv6 nodes, within scope 1 (interface-local) or 2 (link-local).

RQ_000_1717 All Nodes Multicast Addresses
RFC3513 2.7.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
In order to send a multicast IPv6 packet to all its associated link-local nodes, an IPv6 node MUST set the destination address field in the packet to the address value FF02:0:0:0:0:0:0:1.
Specification Text:
All Nodes Addresses: FF01:0:0:0:0:0:0:1
FF02:0:0:0:0:0:0:1

The above multicast addresses identify the group of all IPv6 nodes, within scope 1 (interface-local) or **2 (link-local).**

RQ_000_1718 Router Multicast Addresses
RFC3513 2.7.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
In order to send a multicast IPv6 packet to all its associated interface-local routers, an IPv6 node MUST set the destination address field in the packet to the address value FF01:0:0:0:0:0:0:2.
Specification Text:
All Routers Addresses: FF01:0:0:0:0:0:0:2
FF02:0:0:0:0:0:0:2
FF05:0:0:0:0:0:0:0

The above multicast addresses identify the group of all IPv6 routers, within scope 1 (interface-local), 2 (link-local), or 5 (site-local).

RQ_000_1719 Router Multicast Addresses
RFC3513 2.7.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
In order to send a multicast IPv6 packet to all its associated link-local routers, an IPv6 node MUST set the destination address field in the packet to the address value FF02:0:0:0:0:0:0:2.
Specification Text:
All Routers Addresses: FF01:0:0:0:0:0:0:2
FF02:0:0:0:0:0:0:2
FF05:0:0:0:0:0:0:0

The above multicast addresses identify the group of all IPv6 routers, within scope 1 (interface-local), **2 (link-local)**, or 5 (site-local).

RQ_000_1720 Router Multicast Addresses
RFC3513 2.7.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
In order to send a multicast IPv6 packet to all its associated site-local routers, an IPv6 node MUST set the destination address field in the packet to the address value FF05:0:0:0:0:0:0:2.
Specification Text:
All Routers Addresses: FF01:0:0:0:0:0:0:2
FF02:0:0:0:0:0:0:2
FF05:0:0:0:0:0:0:2

The above multicast addresses identify the group of all IPv6 routers, within scope 1 (interface-local), 2 (link-local), or **5 (site-local)**.

RQ_000_1721 Solicited-Node Multicast Addresses
RFC3513 2.7.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
In order to send a solicited-node multicast IPv6 packet to all its associated link-local unicast addresses, an IPv6 node MUST set the high-order 104 bits of the destination address field in the packet to the address value FF0:0:0:0:0:1:FF00::/104 and the low-order 24 bits to the low-order 24 bits of the Unicast address being solicited.
Specification Text:
Solicited-Node Address: FF02:0:0:0:0:1:FFXX:XXXX

Solicited-node multicast address are computed as a function of a node's unicast and anycast addresses. A solicited-node multicast address is formed by taking the low-order 24 bits of an address (unicast or anycast) and appending those bits to the prefix FF02:0:0:0:0:1:FF00::/104 resulting in a multicast address in the range

FF02:0:0:0:0:1:FF00:0000

to

FF02:0:0:0:0:1:FFFF:FFFF.

RQ_000_1722 Solicited-Node Multicast Addresses
RFC3513 2.7.1 MANDATORY
Applies to: Router, Host
Context:

Requirement:
In order to send a solicited-node multicast IPv6 packet to all its associated link-local anycast addresses, an IPv6 node MUST set the high-order 104 bits of the destination address field in the packet to the address value FF0:0:0:0:0:1:FF00::/104 and the low-order 24 bits to the low-order 24 bits of the anycast address being solicited.

Specification Text:
Solicited-Node Address: FF02:0:0:0:0:1:FFXX:XXXX

Solicited-node multicast address are computed as a function of a node's unicast and anycast addresses. A solicited-node multicast address is formed by taking the low-order 24 bits of an address (unicast or anycast) and appending those bits to the prefix FF02:0:0:0:0:1:FF00::/104 resulting in a multicast address in the range

FF02:0:0:0:0:1:FF00:0000

to

FF02:0:0:0:0:1:FFFF:FFFF.

RQ_000_1725 Solicited-Node Multicast Addresses
RFC3513 2.7.1 MANDATORY
Applies to: Host, Router
Context:

Requirement:
An IPv6 node MUST join (on the appropriate interface) the solicited-node multicast address associated with each of its assigned unicast and anycast addresses.
Specification Text:
A node is required to compute and join (on the appropriate interface) the associated Solicited-Node multicast addresses for every unicast and anycast address it is assigned.

RQ_000_1726 Address Architecture
RFC3513 2.8 MANDATORY
Applies to: Host
Context:

Requirement:
An IPv6 host MUST recognize the following addresses as identifying itself:

(1) Its required Link-Local Address for each interface.
(2) Any additional Unicast and Anycast Addresses that have been configured for the node's interfaces (manually or automatically).
(3) The loopback address.
(4) The All-Nodes Multicast Addresses defined in RFC3515.
(5) The Solicited-Node Multicast Address for each of its unicast and anycast addresses.
(6) Multicast Addresses of all other groups to which the node belongs.

Specification Text:
A host is required to recognize the following addresses as identifying itself:

*** Its required Link-Local Address for each interface.**
*** Any additional Unicast and Anycast Addresses that have been configured for the node's interfaces (manually or automatically).**
*** The loopback address.**
*** The All-Nodes Multicast Addresses defined in section 2.7.1.**
*** The Solicited-Node Multicast Address for each of its unicast and anycast addresses.**
*** Multicast Addresses of all other groups to which the node belongs.**

RQ_000_1727 Address Architecture
RFC3513 2.8 MANDATORY
Applies to: Router
Context:

Requirement:
An IPv6 host MUST recognize the following addresses as identifying itself:

(1) Its required Link-Local Address for each interface.
(2) Any additional Unicast and Anycast Addresses that have been configured for the node's interfaces (manually or automatically).
(3) The loopback address.
(4) The All-Nodes Multicast Addresses defined in RFC3515.
(5) The Solicited-Node Multicast Address for each of its unicast and anycast addresses.
(6) Multicast Addresses of all other groups to which the node belongs.

(7) The Subnet-Router Anycast Addresses for all interfaces for which
it is configured to act as a router.
(8) All other Anycast Addresses with which the router has been configured.
(9) The All-Routers Multicast Addresses defined in section 2.7.1.

Specification Text:

A router is required to recognize all addresses that a host is required to recognize, plus the following addresses as identifying itself:

*** The Subnet-Router Anycast Addresses for all interfaces for which it is configured to act as a router.**
*** All other Anycast Addresses with which the router has been configured.**
*** The All-Routers Multicast Addresses defined in section 2.7.1.**

RQ_000_9051 Loopback Address

RFC3513 2.5.3 MANDATORY

Applies to: Router, Host

Context:

Requirement:

An IPv6 node MUST NOT make it possible for the Loopback address (unicast address 0:0:0:0:0:0:0:1) to be assigned to any physical interface.

Specification Text:

The unicast address 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to send an IPv6 packet to itself. It may never be assigned to any physical interface.

Annex A (informative): Duplicated requirements

Within the IPv6 Core Requirements Catalogue, a number of the extracted requirements duplicate other requirements taken from elsewhere in the set of core IPv6 specifications. Table A.1 summarizes these duplications.

Table A.1: IPv6 Core duplicate requirements

Duplicate Requirements	
Parent Requirement	**Child Requirements**
RQ_000_1004	RQ_000_1004
	RQ_000_1049
RQ_000_1244	RQ_000_1244
	RQ_000_9026
RQ_000_1272	RQ_000_1272
	RQ_000_1232
RQ_000_1287	RQ_000_1285
	RQ_000_1287
RQ_000_1449	RQ_000_1003
	RQ_000_1449
RQ_000_1802	RQ_000_1802
	RQ_000_1098
RQ_000_1818	RQ_000_1808
	RQ_000_1818
RQ_000_1822	RQ_000_1822
	RQ_000_1103
RQ_000_7003	RQ_000_7003
	RQ_000_7030
RQ_000_7034	RQ_000_7001
	RQ_000_7034
RQ_000_8124	RQ_000_8124
	RQ_000_8110
RQ_000_8136	RQ_000_8136
	RQ_000_8299
RQ_000_8141	RQ_000_8118
	RQ_000_8141
	RQ_000_8301
RQ_000_8147	RQ_000_8147
	RQ_000_8114
RQ_000_8159	RQ_000_8159
	RQ_000_8115
RQ_000_8167	RQ_000_8167
	RQ_000_8409
RQ_000_8183	RQ_000_8183
	RQ_000_8526
RQ_000_8188	RQ_000_8188
	RQ_000_8549
RQ_000_8211	RQ_000_8211
	RQ_000_8290
RQ_000_8241	RQ_000_8241
	RQ_000_8134
RQ_000_8250	RQ_000_8250
	RQ_000_8196
RQ_000_8251	RQ_000_8251
	RQ_000_8145
RQ_000_8349	RQ_000_8140
	RQ_000_8287
	RQ_000_8349
RQ_000_8394	RQ_000_8394
	RQ_000_8193
RQ_000_8395	RQ_000_8395
	RQ_000_8153

Duplicate Requirements	
Parent Requirement	**Child Requirements**
RQ_000_8396	RQ_000_8396
	RQ_000_8158
RQ_000_8397	RQ_000_8397
	RQ_000_8203
RQ_000_8398	RQ_000_8398
	RQ_000_8213
RQ_000_8399	RQ_000_8399
	RQ_000_8219
RQ_000_8400	RQ_000_8400
	RQ_000_8226
RQ_000_8408	RQ_000_8408
	RQ_000_8194
RQ_000_8410	RQ_000_8410
	RQ_000_8181
RQ_000_8411	RQ_000_8411
	RQ_000_8206
RQ_000_8412	RQ_000_8412
	RQ_000_8214
RQ_000_8413	RQ_000_8413
	RQ_000_8220
RQ_000_8414	RQ_000_8414
	RQ_000_8225
RQ_000_8469	RQ_000_8469
	RQ_000_8521
RQ_000_8488	RQ_000_8488
	RQ_000_8174
RQ_000_8538	RQ_000_8538
	RQ_000_8197
RQ_000_8539	RQ_000_8539
	RQ_000_8187
RQ_000_8541	RQ_000_8541
	RQ_000_8207
RQ_000_8543	RQ_000_8543
	RQ_000_8228
RQ_000_8546	RQ_000_8546
	RQ_000_8117
	RQ_000_8182
RQ_000_8574	RQ_000_8574
	RQ_000_8307
RQ_000_8591	RQ_000_8591
	RQ_000_8468
	RQ_000_8596

Annex B (informative): Bibliography

ETSI TS 102 351: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); IPv6 Testing: Methodology and Framework".

History

Document history		
V1.1.1	April 2006	Publication
V2.1.1	February 2008	Publication