ETSI TS 103 874-3 V1.1.1 (2024-10)

DECT-2020 New Radio (NR);
Application Profile Part 3;
IPv6 Profile

Reference
DTS/DECT-00415

Keywords
application profile, DECT-2020, IPv6

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Digital Enhanced Cordless Telecommunications (DECT).

The present document is an access profile using DECT-2020 New Radio (NR) technology.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

Internet protocol is the most common protocol for communicating between devices, hosts and back-end systems in modern network environments. Internet-of-Things (IoT) is the integration of various devices to the Internet, enabling data collection and device control in various systems.

DECT-2020, especially in mesh network topology, is well suited for IoT needs. Due to the specific features in DECT-2020 and in mesh networking more generally,the present document recommends features, operations and protocols how to best integrate the IPv6 technologies and protocols to operating over DECT-2020 radio network.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

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

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 103 636-1: "DECT-2020 New Radio (NR); Part 1: Overview; Release 2".

[2] ETSI TS 103 636-4: "DECT-2020 New Radio (NR); Part 4: MAC layer; Release 2".

[3] ETSI TS 103 636-5: "DECT-2020 New Radio (NR); Part 5: DLC and Convergence layers; Release 2".

[4] IETF RFC 8200: "Internet Protocol, Version 6 (IPv6) Specification".

[5] IETF RFC 4193: "Unique Local IPv6 Unicast Addresses".

[6] IETF RFC 7346: "IPv6 Multicast Address Scopes".

[7] IETF RFC 6282: "Compression Format for IPv6 Datagrams on IEEE 802.15.4".

[8] IETF RFC 4443: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification".

[9] IETF RFC 3810: "Multicast Listener Discovery Version 2 (MLDv2) for IPv6".

[10] IETF RFC 768: "User Datagram Protocol".

[11] IETF RFC 9293: "Transmission Control Protocol".

[12] IETF RFC 6347: "Datagram Transport Layer Security version 1.2".

[13] IETF RFC 9146: "Connection Identifier for DTLS 1.2".

[14] IETF RFC 5246: "The TLS Protocol version 1.2".

[15] IETF RFC 7251: "AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS".

[16] IETF RFC 4492: "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)".

[17] IETF RFC 3879: "Deprecating Site Local Addresses".

[18] IETF RFC 1035: "Domain Names - Implementation and Specification".

[19] IETF RFC 8766: "Discovery Proxy for Multicast DNS-Based Service Discovery".

[20] IETF RFC 6762: "Multicast DNS".

[21] IETF RFC 7925: "Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things".

[22] IETF RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[23] IETF RFC 7250: "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)".

[24] IETF RFC 4291: "IP Version 6 Addressing Architecture".

[25] IETF RFC 7136: "Significance of IPv6 Interface Identifiers".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IETF RFC 3022: "Traditional IP Network Address Translator (Traditional NAT)".

[i.2] IETF RFC 2764: "A Framework for IP Based Virtual Private Networks".

[i.3] OpenVPN Protocol.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms defined in ETSI TS 103 636-1 and the following apply:

Backend Router (BAR): connects DECT-2020 Border Routers to internet. It is possible that the Backend Router and Border Router are single device

Border Router (BR): connects the DECT-2020 radio network to internet or Backend Router

end-point: Internet host communicating with an RD in DECT-2020 network

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 636-1 [1] and the following apply:

BAR	Backend Router connecting to global Internet
BR	Border Routers connecting to DECT-2020 network

CDD	Configuration Data Distribution
DNS	Doman Name Service
DNS-SD	Doman Name Service - Service Discovery
DTLS	Datagram Transport Layer Security
EUI	Extended Unique Identifier
GUA	Global Unicast Address
ICMP	Internet Control Message Protocol
IID	Interface Identifier (device identifying part of IPv6 address)
IoT	Internet-of-Things
IPv6	Internet Protocol version 6
LAN	Local Area Network
mDNS	multicast DNS service discovery
MLD	Multicast Listener Discovery
MPL	Multicast for low-Power and Lossy networks
MTU	Maximum Transmission Unit
NAT	Network address translation
RFC	Request For Comments
RFU	Reserved for Future Use
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
ULA	Unique Local Address
VPN	Virtual Private Network

4 General

4.1 Introduction

4.1.1 General

Present specification defines how IPv6 [4] transmissions and addressing is done in the DECT-2020 New Radio (NR) [1].

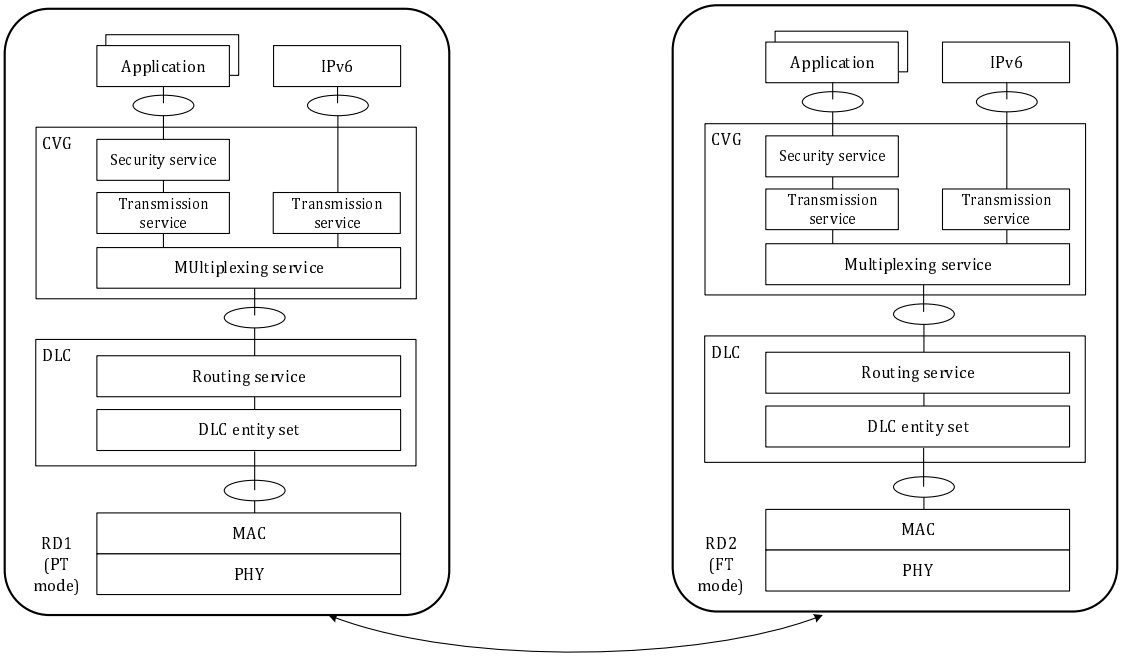

Figure 4.1-1: DECT-2020 Protocol Stack

As defined in [3] and shown in Figure 4.1-1, IPv6 is an optional application layer for DECT-2020 stack. The present document defines the IPv6 adaptation, or interworking, to enable RDs to connect to Internet or local network using IPv6 protocol family.

4.1.2 DECT-2020 addressing usage

IPv6 addressing is not used for the routing of messages inside the DECT-2020 network. It is expected that a border router, that connects the DECT-2020 radio network to Internet, can map the IPv6 addresses to device RD Long IDs used in routing on the DLC layer, and can then either perform route discovery as defined in DECT-2020 release 2 ETSI TS 103 636-1 [2] and ETSI TS 103 636-5 [3] or deliver the messages by flooding the network. DECT-2020 defines routing between RDs and BR in ETSI TS 103 636-5 [3].

4.1.3 No detailed DECT-2020 stack configuration

IPv6 Profile defines the IPv6 operation over DECT-2020. IPv6 is not a specific application but itself a generic communication protocol stack. It can run on top of various DECT-2020 stack configurations, for example over long latency massive mesh networks or over low latency star networks. Other application profiles define the DECT-2020 stack configurations for different kinds of DECT-2020 networks, detailing more specific configuration of the DECT-2020 protocol layers. IPv6 profile as generic protocol profile will not define a more detailed DECT-2020 network configuration. Application profiles can refer to this IPv6 profile if the application uses IPv6 and Internet protocols.

4.1.4 IPv6 DECT-2020 CVG endpoint

DECT-2020 convergence layer (CVG) [3] defines application, or endpoint, multiplexing for DECT-2020 networks. A CVG endpoint multiplexing identifier has been defined for IPv6 in https://portal.etsi.org/PNNS/Protocol-Specification-Allocation/DECT-2020-NR-Endpoint-Multiplexing-Addresses.

Separate endpoints have been defined for both normal IPv6 [4] and IPv6 header compressed packets as defined in IETF RFC 6282 [7].

4.1.5 Configuration data distribution

IPv6 profile address autoconfiguration and optimizations rely on Configuration Data Distribution (CDD) [3].

4.2 Services expected of DECT-2020 CVG and DLC layer

IPv6 profile expects following services from DECT-2020 stack [2] and [3]:

- Transmission and reception of CVG PDUs;
- Support 1280-byte IPv6 Packets in CVG payload;
- Reliable transmissions;
- DECT-2020 DLC routing of transmissions to destination devices using the DECT Long RD ID;
- Long RD ID addressing information for received DECT-2020 PDUs given to IPv6 profile implementation;
- Indication of status of the CVG PDU transmissions;
- Indication of the Sink change and the Long RD ID of the Sink;
- Configuration Data Distribution.

IPv6 profile operation is for data transmission only, the establishment or discovery of a DECT-2020 network is not using the services and protocols of the IPv6 stack. Network creation (advertisement and discovery) and operation is defined by DECT-2020 features defined in the DECT-2020 standards [1], [2] and [3].

4.3 Order of transmission

The transmission order is Big endian and left to right:

- A list of octets is transmitted 1st octet first.
- For each octet, bits are numbered 0 to 7 according to transmission order. Bit 0 is transmitted first (ascending transmission order).
- This order is the same as defined for CVG layer.

5 IPv6 protocol adaptation definition

5.1 General

IPv6 adaptation for DECT-2020 is defined to ensure the fluent operation of IPv6 and related Internet protocols over the varying link capacities encountered in the DECT-2020 networks. Especially in a DECT-2020 mesh network the link capacity can vary greatly as an IPv6 packet is transmitted hop-by-hop to the destination RD. The impacts of this link variation are mitigated with IPv6 header compression.

Common definition also ensures the interoperability of devices in a mesh network.

5.2 IPv6 addressing architecture

The DECT-2020 mesh is a mesh-under routing network, so the link-local IPv6 addresses are not scoped to the next DECT-2020 radio hop but extend over all the radio links in a DECT-2020 network as shown in Figure 5.2-1.

Network always has a Border Router, with one or more Sinks. Network may have multiple Border Routers under a Backend Router (BAR). In the present document it is assumed that in a multiple Sinks and multiple Border Routers configuration all the DECT-2020 routing trees from the Sink share the same Network ID [2]. BAR and BR are logical functions that may be implemented in the same device. When there is a local network with multiple BRs, the BAR is usually a separate device, as shown in Figure 5.2-1.

DECT-2020 network is identified by a Network ID. Network ID also largely identifies the application and device type that form the network. The same DECT-2020 network, as identified by the Network ID, may be found in multiple, separate geographical locations. Thus, the same DECT-2020 network may be reachable via multiple different IPv6 addresses of the Backend Routers.

IPv6 address consists of a network address part, called a prefix, and a device interface ID (IID) [4]. Global Internet network address is defined for the backend router or border routers by the Internet service provider.

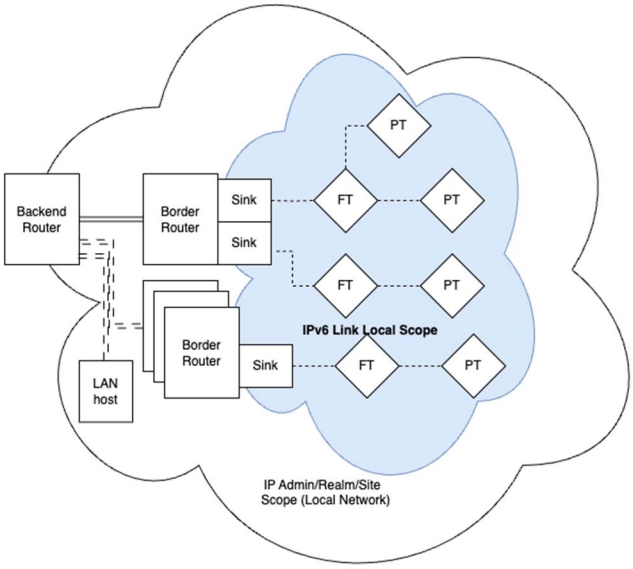

Figure 5.2-1: Network addressing architecture

Figure 5.2-1 shows the different scopes of IPv6 addresses with regards to DECT-2020 network and the multiple Sinks and BRs configurations.

The DECT-2020 devices shall support multiple IPv6 addresses for their DECT-2020 interface. These include Global Unique Address (GUA) [4], Unique Local Address (ULA) [5] and link local unicast IPv6 addresses [4] and possibly multicast addresses in different scopes [6].

IPv6 unicast address scopes are mapped as [4] and [5]:

- Unique Local Address (prefix "fc00::/7", ULA) scope is configured by the administrators, it can include even back-end services connected with a VPN technology through Backend Router
- Link Local Address (prefix "fe80::") scope is the DECT-2020 devices in same Network ID reachable possibly by multiple Border Routers, including the Sink devices and the BRs

IPv6 multicast scopes are mapped as [6]:

- IPv6 Realm and Admin Scopes ("ff03", "ff04" or "ff05") are configured by the administrators, and can include, in addition to the DECT-2020 devices and their Sinks and BRs, the LAN hosts reachable by the BAR and possible VPN reachable back-end services
- IPv6 Link-Local Scope ("ff02") is the DECT-2020 devices in same Network ID reachable possibly by multiple Border Routers, including the Sink devices and the BRs

NOTE: The present document uses the Admin scope name for both multicast scopes of "ff04" and "ff05::" which in [5] and [6] is defined for site local scope. However, site local scope is deprecated [17] for unicast, and the term is avoided for its ambiguity for multicast as well.

Border Routers shall be prepared to forward realm-local and admin-local multicast, and route GUA and ULA scoped unicast in and out of the DECT-2020 network as defined in local IPv6 routing configuration.

Backend Router connecting the DECT-2020 network to internet may provide NAT service or VPN tunnelling services [i.1], [i.2] and [i.3]. Due to the common UDP transport use and often infrequent communications by the devices in mesh networks, the NAT mapping time-outs for UDP can be problematic. A common solution is to provide a Virtual Private Network tunnel from the Backend Router to the backend servers. VPN tunnelling also enables all services and devices to use ULA addresses protecting them from general Internet access attempts.

5.3 IPv6 link maximum transmission unit

IPv6 requires link MTU to be at least 1 280 bytes [4]. RDs shall support link MTU of at least 1 280 bytes as CVG payload. The DECT-2020 CVG and DLC layers [3] shall fragment and reassemble packets forwarded over DECT-2020 network.

5.4 IPv6 prefix configuration

5.4.1 IPv6 address allocation options to routers

The addressing scope and Internet side address configuration mechanism how a BAR or BR receives an internet address is not defined in the present specification. Internet protocols provide multiple locally configurable options for address allocation.

The BAR can receive a DECT-2020 network prefix explicitly with prefix delegation, or the BAR can receive implicit DECT-2020 prefix as an IPv6 router advertisement. The BAR might not even have IPv6 upwards connectivity, instead relying on a local IPv6 unique addressing (ULA) and doing NAT to internet or using a VPN tunnel to backend services. It is left for the network administrators to define the approach to use in their installations.

5.4.2 Prefix advertisement for DECT-2020 RDs

Devices shall create unique IPv6 addresses based on shared Prefix as published by the Sink and with the IID part consisting of DECT-2020 Sink Long RD ID and the device's own Long RD ID [2].

RDs shall support Configuration Data Distribution (CDD) [3] as defined in Annex A. The CDD may be used to advertise GUA or ULA prefixes. An RD shall accept the prefix or prefixes regardless of the scope.

The 64-bit IID part of device's IPv6 address shall consist of the 32-bit DECT-2020 Sink device Long RD ID and the device's own 32-bit Long RD ID. The Sink Long RD ID in the IID enables memory efficient routing for systems that have multiple Sink devices under one Border Router.

Link local address shall be formed by the device automatically, regardless of if a GUA or ULA prefix is configured. The address shall have the standard link local scope [4] and IID part consisting of the Sink Long RD ID and Device Long RD ID.

NOTE: The Long RD ID usage differs from EUI-64 based stateless address autoconfiguration for IPv6 as the unique/local bit is not utilized as defined in IETF RFC 4291 [24]. This is not considered problematic as IPv6 has defined usage for random and semantically opaque identifiers [25] indicating that the unique/local bit is not necessary anymore.

5.5 Replaced IPv6 procedures

Due to the specific nature of the DECT-2020 network and its services, following IPv6 procedures [4] are not needed for network and communication operation:

- Duplicate address detection
- Neighbour advertisement or solicitation
- Router advertisement or solicitation

Addressing inside the DECT-2020 network is based on unique Long RD IDs [2], so duplicate IPv6 addressing detection should not be used.

The DECT-2020 FT and PT devices have their DECT-2020 neighbour information from associations and beacon advertisements [2], so IPv6 Neighbour advertisement and solicitation should not be used.

IPv6 packets in the DECT-2020 network are routed using the DECT-2020 protocols [1] and [3], so IPv6 routing advertisement or solicitation inside the DECT-2020 network should not be used.

Due to the large link-local scope in DECT-2020 network, the propagation of the ICMP multicasts for duplicate addressing detection, neighbour advertisements and solicitation and for router advertisement and solicitation should be limited by DECT-2020 hop counts if the mechanisms are used.

5.6 IPv6 header compression

IPv6 header can be considerable overhead for small link-layer packets. As the link capacity over a weak radio link can be limited, the devices may support header compression as defined in IETF RFC 6282 [7]. Devices shall always support uncompressed IPv6.

The BR may be configured to use IPv6 header compression. Header compression support by the BR is indicated in CDD data in Annex A. If any prefix or address is flagged to be used in header compression, i.e. if Context Usage is '1', header compression is supported and may be used by RDs.

If header compression is supported, the DECT-2020 RDs shall support IPv6 Header Compression (LOWPAN_IPHC) and IPv6 Extension Header Compression (LOWPAN_NHC) and context identifiers as defined in IETF RFC 6282 [7] and extended below, and shall support context identifiers distribution in CDD configuration as defined in Annex A.

Due to the IEEE 802.15.4 technology and link-local address scope assumptions in IETF RFC 6282 [7], the source and destination address stateless compressions in the RFC are ineffective for DECT-2020 environment. The IID deriving defined in RFC 6282 [7], chapter 3.2.2 is extended here so that the DECT-2020 Long RD IDs are used in forming the elided IID.

CDD may be used to distribute the shared context identifiers used in RFC 6282 [7], chapter 3.1.2 for eliding different IPv6 prefixes and whole addresses. If the context information is configured, the RDs may elide the IPv6 source and/or destination addresses according to addressing modes 1 and 3 as defined in IETF RFC 6282 [7]. In case of addressing mode 1 the context identification is the prefix scope and the remaining IID of the address is sent in packet. In case of fully elided addresses in addressing mode 3 there are 2 options:

1) Context defines the prefix and IID is derived from the Sink Long RD ID and RD Long RD ID in the encapsulating DECT-2020 header.

2) Context defines the full IPv6 address of the internet host.

If header compression is supported, RD devices shall support 16 contexts, that at maximum are full IPv6 address in length.

NOTE: Option 2 of addressing mode 3 allows eliding the IPv6 address of the end-points outside the DECT-2020 network, for example management servers. Care needs be taken in this approach, as load balancing solutions or cloud service scaling solutions may rely on RDs using multiple different IPv6 addresses for the service. The service end-point's IPv6 address may also change during the lifetime of the service.

5.7 Multicast IPv6

Multicast routing from backend system into DECT-2020 network and vice versa shall be performed by the BR if configured in IPv6 routing table. RD devices may support IPv6 multicast.

It is expected that the IPv6 multicast is static in nature where a BR is configured to forward known IPv6 multicasts and RD devices are pre-configured to listen for these known multicast addresses. It is expected that much of the traffic is targeted for all nodes. RDs do not need to be aware of multicast memberships of other RD devices for routing of the IPv6 multicast. If IPv6 multicast is supported, IPv6 multicast shall be done as defined in clause 6.3.

All multicast addresses may be compressed as defined in clause 5.6.

If IPv6 multicast is supported, RDs should listen on these multicast addresses

IPv6	ff02::1	All nodes on the link scope network (FT and PT devices)
IPv6	ff05::1	All nodes on the Admin scope network (FT and PT devices)

If IPv6 multicast is supported, BR shall listen on these multicast addresses

IPv6	ff02::2	All routers on the link scope network
IPv6	ff02::16	MLDv2 control in Link-local scope
IPv6	ff05::16	MLDv2 control in Admin scope

If IPv6 multicast is supported, BR/Sink IPv6 should listen on these multicast addresses
IPv6 ff05::fb Multicast DNS in Admin scope
IPv6 ff05::2 All routers on the Admin scope network

5.8 Internet Control Message Protocol (ICMPv6)

The RDs should support ICMPv6 [9] error messages when received as responses for RD initiated transmissions.

NOTE 1: RDs in FT mode can not generate destination unreachable-errors or time exceeded-errors as they only forward the transmissions on DECT-2020 level, not as IPv6 routing forwarding.

The RDs should understand Echo request and Echo response generation [8].

NOTE 2: Ping command (ICMPv6 Echo request and response) are sometimes used as continuous network operation test and measurement. Ping should be used conservatively in DECT-2020 networks.

If IPv6 multicast is supported, the RDs may support MLDv2 protocol [9]. The RDs shall not generate MLDv2 reports for pre-configured multicast addresses. The BR should use a very long MLD query interval.

5.9 Transport protocols

5.9.1 General

The RDs shall support UDP [10].

The RDs may support transmission and reception of UDP header compression as defined in IETF RFC 6282 [7].

NOTE: Due to the unreliable nature of UDP, application layer acknowledgements and re-transmissions should be used. Due to the variation on DECT-2020 networks' latency behaviour the protocol's time-out values need to be carefully designed.

The RDs may support TCP [11].

5.9.2 Transport layer security

DTLS over UDP should be supported. If supported, the RDs shall support DTLS version 1.2 [12]. To optimize DTLS operation for RD whose IPv6 address may changes in mesh network self-configuration or node mobility, the DTLS connection ID [13] should be supported by Devices and backend DTLS connection end-points.

If TCP is supported, the RDs should support TLS [14].

If DTLS or TLS is supported, the end-points should implement raw public keys profile as defined in IETF RFC 7925 [21] and IETF RFC 7250 [23]. The end-points may implement certificates profile as specified in IETF RFC 7925 [21], IETF RFC 6347 [12], IETF RFC 5246 [14], IETF RFC 7251 [15] and IETF RFC 4492 [16]. The end point may support pre-shared key profiles, as defined in IETF RFC 7925 [21] and IETF RFC 4279 [22].

5.10 DNS and DNS based service discovery

DNS may be supported [18]. DNS service's IPv6 address may be configured using CDD as defined in the Annex A.

BR or BAR may act as DNS based service discovery proxy [19] for local services. If DNS service discovery is supported, BR or BAR should support unicast DNS-SD and BRs should support multicast mDNS [20].

RDs supporting DNS-SD should support service discovery proxy configuration as defined in Annex A.

6 Procedures

6.1 Unicast procedures

6.1.1 RD originating unicast transmission procedure

When transmitting a unicast IPv6 packet, IPv6 adaptation layer in an RD shall:

- if the destination IPv6 address prefix is the link-local prefix:
  - set the EP address of the CVG layer to value indicating plain IPv6;
  - set the CVG layer payload to contain the IPv6 packet;
  - set the DLC destination address to be the Long RD ID indicated in the lowest 32 bits of the destination IPv6 address IID;
  - instruct the CVG layer to transmit the message using packet routing between RDs, clause 5.2.8.4 of ETSI TS 103 636-5 [3];
- else:
  - if compressed IPv6 if supported by BR:
    - set the EP address of the CVG layer to value compressed IPv6;
    - compress the IPv6 header;
  - else:
    - set the EP address of the CVG layer to value indicating plain IPv6;
  - set the CVG layer payload to contain the IPv6 packet;
  - set the DLC destination address be the backend address;
  - instruct the CVG layer to transmit the message using packet routing to backend (uplink) procedure, clause 5.2.8.2 of ETSI TS 103 636-5 [3].

6.1.2 BR originated unicast transmission procedure

When transmitting a unicast IPv6 packet to DECT-2020 network, IPv6 adaptation layer in a BR or Sink shall:

- if the destination IPv6 address prefix is the link-local prefix or if the destination IPv6 address prefix is one of the subnet prefixes configured to the BR:
  - set the EP address of the CVG layer to value indicating plain IPv6 or compressed IPv6;
  - set the CVG layer payload to contain the IPv6 packet;
  - set the DLC destination address to be the Long RD ID indicated in the lowest 32 bits of the destination IPv6 address IID;
  - instruct the CVG layer to transmit the packet using routing from backend (downlink) procedure, clause 5.2.8.3 of ETSI TS 103 636-5 [3];
- else:
  - discard the IPv6 packet.

6.1.3 Unicast error situations

For source routing and cached routing, the BR may generate ICMPv6 error message destination unreachable based on the DLC Route Error IE it receives, clause 5.3.3.6 of ETSI TS 103 636-5 [3].

6.2 Multicast procedures

6.2.1 RD multicast listener registration procedure

When interested in listening to a IPv6 multicast address, and MLDv2 usage is enabled, an RD shall generate an Unsolicited Report for the multicast address listened to as defined in IETF RFC 768 [10]. MLDv2 report transmission should be repeated a few times, with moderate length random delays between transmissions (0 to 2 seconds). The RD shall send this report using link-local multicast as defined in IETF RFC 768 [10] and in clause 6.2.2.

An RD that has sent an MLD report should respond to MLD queries.

6.2.2 RD originated multicast transmission procedure

When transmitting an IPv6 multicast packet, IPv6 adaptation layer in an RD shall:

- if the destination IPv6 address scope is larger than link-local scope:
  - if compressed IPv6 if supported by BR:
    - set the EP address of the CVG layer to value compressed IPv6;
    - compress the IPv6 header;
- else:
  - set the EP address of the CVG layer to value indicating plain IPv6;
  - set the CVG layer payload to contain the IPv6 packet;
  - set the DLC destination address to be the backend address;
  - instruct the CVG layer to transmit the packet using packet routing to backend (uplink) procedure as defined in ETSI TS 103 636-5 [3], clause 5.2.8.2;
- else:
  - set the EP address of the CVG layer to value indicating plain IPv6;
  - set the CVG layer payload to contain the IPv6 packet;
  - set the DLC destination address to be the broadcast address;
  - instruct the CVG layer to transmit the message using packet routing between RDs as defined in ETSI TS 103 636-5 [3], clause 5.2.8.4.

6.2.3 BR originated multicast transmission procedure

When transmitting an IPv6 multicast packet to DECT-2020 network, IPv6 adaptation layer in a BR shall:

- if there are IPv6 multicast listeners registered for this multicast address:
  - set the EP address of the CVG layer to value indicating plain IPv6 or compressed IPv6;
  - set the CVG layer payload to contain the IPv6 packet;
  - set the DECT-2020 destination address of the routing layer to be the broadcast address;

  - instruct the CVG layer to transmit the message using packet routing from backend (downlink) procedure as defined in ETSI TS 103 636-5 [3], clause 5.2.8.3;

- else:

  - discard the IPv6 packet.

6.3 Limiting IPv6 multicast forwarding in DECT-2020 Network

Considering the DECT-2020 Network as single link places specific considerations for having multiple BRs forwarding multicast to the network.

If majority of devices are interested in the multicast(s), the IPv6 multicast forwarding should be configured manually in the BRs and MLDv2 operation should be configured off in the RDs.

RD should limit MLDv2 report sending. The report transmission initial startup delay should be multiplied by the Route Cost [2]. This suppresses unnecessary reports as RDs closer to Sink will send the report first. RD that receives the multicast of interest without generating a report should suppress generation of solicitated reports.

MLDv2 report indicating interest on a multicast reception is sent as link-local multicast by an RD, using the RD-to-RD communications, and can thus be received by multiple BRs in the DECT-2020 network. The decision in a BR to forward multicast should consider the source IPv6 address for the report. If the Sink IDs of the BR are different than in the MLDv2 report source IP's IID part, the packet may be dropped as coming from different routing tree. Accepting it and starting to forward multicast would lead to multiple BRs forwarding the multicast to the network. Depending on if the devices move in the network and if majority of devices are interested in the multicasts, it may be the best choice to forward the traffic from multiple BRs. BR forwarded multicast stays in the routing tree unlike RD originated multicast.

6.4 Mobility between DECT-2020 Sinks

Since the IPv6 address contains the Sink Long RD ID, whenever an RD moves from under one Sink to another Sink its IPv6 address changes. Mobility under same Sink does not change the IPv6 address.

An RD moving under a different Sink shall read the CDD information advertised and follow the operations as defined in CDD [3]. Sink address is expressed in Route Info IE in parent beacon [2].

An RD shall renegotiate or refresh the back-end connection or inform the back-end server when its IPv6 address changes.

6.5 Border Router or Sink restart

If the downlink routing into the DECT-2020 network is based on selective source routing, any restart or reset of the BR may result in the loss of the routing information. Sink shall be the responsible device to distribute Configuration Data Distribution [3], and in restart situation operate as defined in CDD [3].

An RD shall read again the CDD information when detecting a changed Application Sequence Number as defined in CDD [3].

An RD should indicate to IP-stack and application layers when IPv6 address has changed, so applications can renegotiate or refresh their server connections using the new IPv6 address.

Annex A (normative): Configuration data distribution definition for IPv6 profile

The Configuration Data Distribution [3] uses EPs to differentiate Data Items, allowing multiple information elements within a Data Item. The information elements for the IPv6 profile are normatively defined below. The IPv6 profile data both for plain IPv6 and header compression format, is identified with the CVG Endpoint value of 0x8003 as defined in https://portal.etsi.org/PNNS/Protocol-Specification-Allocation/DECT-2020-NR-Endpoint-Multiplexing-Addresses.

Below defined information elements are mandatory to support for parsing. Element content may support feature that is optional to support, but the general structure of the element shall be supported at minimum so that the content is ignored but next element can be found.

A.1 CDD Information Element: IPv6 Control Element

Mandatory. Element length 1 byte.

Table A.1-1: IPv6 Control Element definition

Field Name	# of bits	Explanation
Element type	2	Identifies control element, Value 0x0.
Element Version	2	Identifies elements version, Value 0x0.
RFU	3	RFU, Value 0x0.
Re-register	1	Re-Register on Application Sequence Number Change. Value '1' indicates that RD shall refresh IPv6 connections and sessions when the Application Sequence number has changed. Value '0' indicates no refresh is needed.

A.2 CDD Information Element: IPv6 Address Element

Optional. Element Length 9 or 18 bytes.
Element header + prefix 8-bytes or Element Header + address 16 bytes + service ID 1 byte.

Table A.2-2: Address Element definition

Field Name	# of bits	Explanation
Element type	2	Identifies IPv6 Address element, Value 0x1
Element Version	2	Identifies element version, Value 0x0
RFU	2	Reserved for future use. Shall be '0'
Prefix Type	1	Value '0' indicates 64-bit prefix for IPv6 address autoconfiguration Value '1' indicates full 128-bit IPv6 address, with service ID
Context Usage	1	Value '0' indicates address element is not used in header compression Value '1' indicates Border Router supports address element in header compression. Context ID is included
Context ID	4	Identifier for header compression. Shall be '0' if address element is not used in header compression
Service ID	4	Defined when prefix type is '1' Value '0x1' indicates the address is DNS server Value '0x2' indicates the address is application server Value '0x3' indicates the address is device management server Value '0x4' indicates network time server Value '0x5' indicates DNS-SD proxy address Values '0x6 - 0xf' RFU Defined as 0x0 when prefix type is '0'
Address information	64 or 128	As defined by Prefix type

Annex B (informative): Change history

Date	Version	Information about changes
January 2024	0.0.2	TO-BE-DELETED-FOR-PUBLICATION Edited after discussions on DECT WG meetings and telcos, draft made available
April 2024	0.0.3	TO-BE-DELETED-FOR-PUBLICATION TLV encoding defined, defined multicast procedures for simple multicast as broadcast, advanced multicast operation
June 2024	0.0.4	TO-BE-DELETED-FOR-PUBLICATION TLV replaced with CDD data, procedures clarified
September 2024	0.0.5	TO-BE-DELETED-FOR-PUBLICATION Final draft. Removed prefix-based multicast provisioning, Matter usage of it is based on FabricID that is provisioned to device as part of the Matter operational certificate

History

Document history		
V1.1.1	October 2024	Publication