Requirements For IPv6 in ICT Equipment

Authors:

- Merike Käo, <merike@doubleshotsecurity.com>
- Jan Žorž, <jan@go6.si>
- Sander Steffann, <sander@steffann.nl>
- Tim Chown <tim.chown@jisc.ac.uk>
- Tim Winters <tim@qacafe.com>

Working Groups:

- IPv6 Working Group
- Best Current Operational Practices Task Force (Proposed Charter)

Document ID: ripe-772

Updates: ripe-554

Date: December 2021

Table of contents:

1 Introduction

To ensure the smooth and cost-efficient uptake of IPv6 across their networks, it is important that large commercial, public sector or research and education enterprises specify requirements for IPv6 functionality and compatibility when drafting tenders for Information and Communication Technology (ICT) equipment and support.

This document is intended to provide a Best Current Practice (BCP) to support organisations in such tender processes, but does not specify any standards or policy itself. It is an update to ripe-554, which is the second version of the "Requirements for IPv6 in ICT Equipment" guidance.

It offers guidance on what specifications to ask for and it is intended to be used as a **template** that can be used by governments, universities, large enterprises or any other organisation when specifying IPv6 support in their tenders or equipment requirements. It can also serve as an aid to those people or organisations interested in tendering for government or enterprise contracts.

Be aware that the standards listed here have their origin in various bodies, principally the IETF, which operate independently of the RIPE community, and that any of these standards might be changed or become replaced with a newer version. While this document has been approved by the RIPE membership, principally via the IPv6 WG, as of the date of publication, its contents will age as new RFCs or related documents are issued.

You may also need to adjust the recommendations to your specific local needs; again, this document is purely a template, and the suggested Mandatory and Optional elements may need to be tuned for your specific use case(s).

Some parts of this section are loosely based on the NIST/USGv6 profile developed by the US government:

https://www.nist.gov/programs-projects/usgv6-program

for which there is a newer version at:

https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.500-267Ar1.pdf

The authors have modified the content of these documents to make them more universally applicable. This option includes a list of RFC specification standards, which must be supported, divided into seven categories of devices. Note that this document removes the 'mobile device' category, instead including such devices as hosts.

This document also follows the IPv6 Node requirements document, RFC8504 (which updated RFC6434). This RFC contains general IETF guidance and consensus on what parts of IPv6 need to be implemented by different devices, and its contents are generally reflected in this document.

1.1 General information on how to use this document

This document does not dictate specific technologies to be used, rather it assumes a network design/solution has been produced, and that design, and the components it uses, needs to be mapped to the procurement document.

An IPv6 Ready Logo certificate can be required for hosts, routers, and CPE Routers. While the Logo certification was devised around 20 years ago, it is kept current with IPv6 standard updates and is a globally accepted program for vendors to promote their equipment and to assert that their equipment fulfills basic IPv6 requirements. The IPv6 Ready Logo latest updates require that devices be tested in IPv6-only environments and have IPv6 enabled by default. The tender initiator shall also provide the list of required mandatory and optional RFCs in order not to exclude vendors that did not yet put their equipment under IPv6 Ready Logo testing certifications. This way public tenders can't be accused of preferring any type or vendor of equipment.

For more information about the IPv6 Ready Logo program see: http://www.ipv6ready.org/

When we specify the list of required RFCs, we must list all mandatory requirements, except the entries that start with, "If [functionality] is requested…" These entries are mandatory only if the tender initiator requires certain functionality. Similarly, if features listed as Optional are required for the tender initiator's specific use case(s), then those requirements should be made Mandatory. Please note that the tender initiator should decide what functionality is required, not the equipment vendor; this document is simply a template.

1.2 How to specify requirements

As stated above, the IPv6 Ready Logo program does not cover all equipment that correctly supports IPv6; so declaring such equipment ineligible may not be desirable. This document recommends that the tender initiator specify that eligible equipment be either certified under the IPv6 Ready program or be compliant with the appropriate RFCs listed in the section below.

Important note for tender initiator:
The IPv6 Ready Logo certification covers basic IPv6 requirements and some advanced features, but not all of them. If you require any advanced feature that is not covered by the IPv6 Ready Logo certification, please request a list of RFCs that covers those specific needs in addition to IPv6 Logo Certification. In the lists below RFCs that are covered in the IPv6 Ready Logo certification are marked with *.

2 Proposed generic text for the tender initiator

In every tender, the following text shall be included:

All ICT hardware and software that is a subject of this tender must support the IPv6 protocol, and MUST operate in an IPv6-only environment. For example, where SNMP is used, it must be able to operate over IPv6 transport.

If IPv4 is supported, similar performance and capabilities must be provided for both protocols in input, output and/or throughput data-flow performance, transmission and processing of packets. The difference must not be noticeable to users.

IPv6 support can be verified and certified by the IPv6 Ready Logo certificate.

Equipment that has not been put through the IPv6 Ready testing procedures must comply appropriately with the Mandatory and Optional RFCs listed below:

[insert appropriate list of selected mandatory and optional RFCs from below lists]

3 Categories of devices in scope for this document

Requirements are divided in hardware equipment and integrator support.

All requirements placed on IPv4 traffic capabilities like latency, bandwidth and throughput, or for monitoring and accounting, should also be required for IPv6 traffic.

3.1 Definitions and descriptions of different categories of devices

The following definitions will be used for classifying the varying hardware equipment. While some hardware may have overlapping functionality (i.e. a layer-2 switch can act as a layer-3 router or a router may have some firewall capabilities), it is expected that for any overlapping functionality, the requirements for each specific device be combined.

Note that the mobile device category included in ripe-554 has been removed. Such devices now fall under the host category, such that they are considered only from their connectivity to the local infrastructure (via WiFi), and thus the 3GPP-related requirements are out of scope of this document.

Host: A host is a network participant that sends and receives packets but does not forward them on behalf of others. This includes mobile devices attaching to local network infrastructure.

Host devices in an enterprise may be multihomed, mobile devices being one example, and devices with a network and management interface being another. The IETF has worked for many years on approaches to multihoming for IPv6. Specific [RFC4191] requirements are included in this document.

Switch, or 'Layer-2 Switch': A switch or 'layer-2 switch' is a device that is primarily used for forwarding Ethernet frames, based on their attributes. Exchanging Ethernet information with other Ethernet switches is usually part of its function. This category is further split below into consumer grade (typically for home use) and enterprise/ISP grade.

WiFi access points are technically not pure layer-2 devices, but they should (possibly in cooperation with a wireless controller) perform the same functionality as a layer-2 switch as far as IPv6 features are concerned. Thus the text from this section may also be used for WiFi access points.

Router or 'Layer-3 Switch': A router or 'layer-3 switch' is a device that is primarily used for forwarding IP packets based on their attributes. Exchanging routing information with other routers is usually part of its function.

Network Security Equipment: Network security equipment is devices whose primary function is to permit, deny and/or monitor traffic between interfaces in order to detect or prevent potential malicious activity. These interfaces can also include VPNs (SSL or IPsec). Network Security Equipment is often also a layer-2 switch or a router/layer-3 switch.

Customer Premise Equipment (CPE): A CPE device is a small office or residential router that is used to connect home users and/or small offices in a myriad of configurations. Although a CPE is usually a router, the requirements are different from an Enterprise/ISP router/layer-3 switch. CPEs often need to support IPv6 transition mechanisms; this document will focus primarily on transition methods for IPv6-only networks.

Load Balancer is a networking device that distributes workload across multiple computers, servers or other resources, to achieve optimal or planned resource utilisation, maximise throughput, minimise response time, and avoid overload.

The following references are of relevance to this BCP document. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this BCP document are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

3.2 Things that are out of scope of this document

In the interests of reaching consensus to publish an update to ripe-554 as efficiently as possible, the authors minimised the addition of new types of devices. These may be added in a future update, or as a separate update.

As stated above, mobile devices are considered in this document only in regards to their connectivity to the enterprise infrastructure (typically by WiFi) and in this respect are considered to be hosts.

Note that VMs and containers are out of scope for this document; these functions may be provided on systems procured as hosts via this guidance, but are not “ICT equipment” in themselves.

While [RFC8504] includes a section on YANG for network management, further YANG requirements are not included in this document.

Certain new routing functions that have emerged recently have also not been added at this point, one example being SRv6 [RFC8986].

4 Lists of required RFC standards for different categories of hardware

ICT hardware equipment is divided in this document into seven functional groups:

- Host: client (including mobile device) or server
- Consumer grade layer-2 switch
- Enterprise/ISP grade layer-2 switch
- Router or layer-3 switch
- Network security equipment (firewalls, IDS, IPS,...)
- CPE equipment
- Load Balancer

We have divided the following requirements into two types, Mandatory and Optional. Equipment must meet the Mandatory standards requirements list. Support for the Optional requirements may earn the tender applicant additional points, if so specified by the tender initiator.

Any hardware that does not comply with **all** of the Mandatory standards should be marked as inappropriate by the tender evaluator.

The standards that are part of the IPv6 Ready Logo test procedures, typically performed by accredited labs, are marked with an asterisk *.

4.1 Requirements for "host" equipment

Mandatory support:

- IPv6 Basic specification [RFC8200/STD 86] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection for IPv6 [RFC6724]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443/STD89] *
- If support for DHCPv6 is required, the device must support
    - Stateful DHCPv6 client [RFC8415] *
    - Stateless DHCPv6 client [RFC8415] *

    - DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC3646]*
    - A Method for Generating Semantically Opaque Interface Identifiers (IIDs) with the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC7943]
- SLAAC [RFC4862] *
- Path MTU Discovery [RFC8201/STD87] *
- Neighbor Discovery [RFC4861] [RFC6980] *
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596/STD88]
- DNS message extension mechanism [RFC6891/STD75]
- DNS message size requirements [RFC3226]
- Transmission of IPv6 Packets over Ethernet Networks [RFC2464]
- Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery [RFC6980]
- Updates to the IPv6 Multicast Addressing Architecture [RFC7371]
- A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC7217],
- IPv6 Router Advertisement Options for DNS Configuration [RFC8106]
- Multicast Listener Discovery version 2 [RFC3810] *
- Default Router Preferences and More-Specific Routes: Type A and B host roles [RFC4191]
- If support for tunneling and dual stack is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
- IPv6 Flow Label Specification [RFC6437]

Optional support:

- Extended ICMP for multi-part messages [RFC4884]
- Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6 [RFC8981]
- DS (Traffic class) [RFC2474, RFC3140]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296/STD79, RFC7619, RFC8221, RFC8247] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- Packetisation Layer Path MTU Discovery [RFC4821] [RFC8899]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes: Type C host role [RFC4191]
- IPv6 Router Advertisement Flags Option [RFC5175]
- The Addition of Explicit Congestion Notification (ECN) to IP [RFC3168]
- First-Hop Router Selection by Hosts in a Multi-Prefix Network [RFC8028].
- Distributing Address Selection Policy Using DHCPv6 [RFC7078]
- For improved IPv6 address privacy, support should be considered for “Security and Privacy Considerations for IPv6 Address Generation Mechanisms” [RFC7721] and “Recommendation on Stable IPv6 Interface Identifiers” [RFC8064]
- “MIPv6” [RFC6275, RFC5555] and “Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture” [RFC4877]
- Discovering PREF64 in Router Advertisements [RFC8781]

4.2 Requirements for consumer grade "layer-2 switch" equipment

Optional support (management):

- MLDv2 snooping [RFC4541]
- IPv6 Basic specification [RFC8200/STD86] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection for IPv6 [RFC6724]
- ICMPv6 [RFC4443/STD89] *
- SLAAC [RFC4862] *
- Neighbor Discovery [RFC4861] [RFC6980] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- Transmission of IPv6 Packets over Ethernet Networks [RFC2464]

4.3 Requirements for enterprise/ISP grade "layer-2 switch" equipment

Mandatory support (forwarding plane):

- Transmission of IPv6 Packets over Ethernet Networks [RFC2464]
- MLDv2 snooping [RFC4541]
- Router Advertisement (RA) Guard [RFC6105] and [RFC7113]
- DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers [RFC 7610]
- Dynamic "IPv6 Neighbor solicitation/advertisement" inspection [RFC4861]
- Neighbor Unreachability Detection [NUD, RFC4861] filtering
- Duplicate Address Detection [DAD, RFC4429] snooping and filtering
- If support for DHCPv6 is required, the device must support
    - Lightweight DHCPv6 Relay Agent [RFC6221]
    - DHCPv6 Relay Agent Remote-ID Option [RFC4649]
    - DHCPv6 Relay Agent Subscriber-ID Option [RFC4580]
    - DHCPv6 Client Link-Layer Address Option [RFC6939]

Mandatory support (management; the device must function as an IPv6 host for management):

- IPv6 Basic specification [RFC8200/STD86] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection for IPv6 [RFC6724]
- ICMPv6 [RFC4443/STD89] *
- SLAAC [RFC4862] *
- If support for SNMP is required:
    - SNMP protocol [RFC3411]
    - SNMP capabilities [RFC3412, RFC3413, RFC3414]
    - SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- IPv6 Routing Header [RFC8200, Next Header value 43] filtering *

Optional support:

- Source Address Validation Improvement (SAVI) Solution for DHCP [RFC7513]

4.4 Requirements for "router or layer-3 switch" equipment

Mandatory support:

- IPv6 Basic specification [RFC8200/STD86] *
- Transmission of IPv6 Packets over Ethernet Networks [RFC2464]
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection for IPv6 [RFC6724]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- If support for DHCPv6 is required, the device must support
    - DHCPv6 client/server/relay [RFC8415] *
    - DHCPv6 Relay Agent Remote-ID Option [RFC4649]
    - DHCPv6 Relay Agent Subscriber-ID Option [RFC4580]
    - DHCPv6 Client Link-Layer Address Option [RFC6939]
- ICMPv6 [RFC4443/STD89] *
- SLAAC [RFC4862] *
- IPv6 Router Advertisement Options for DNS Configuration [RFC8106] *
- MLDv2 snooping [RFC4541]
- Multicast Listener Discovery version 2 [RFC3810] *
- Updates to the IPv6 Multicast Addressing Architecture [RFC7371]
- Path MTU Discovery [RFC8201/STD87] *
- Neighbor Discovery [RFC4861] [RFC6980]*
- 127-bit IPv6 Prefixes on Inter-Router Links [RFC6164]
- IPv6 Prefix Length Recommendations for Forwarding [RFC 7608]*
- If support for SNMP is required:
    - SNMP protocol [RFC3411]
    - SNMP capabilities [RFC3412, RFC3413, RFC3414]
    - SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- If a dynamic interior gateway protocol (IGP) is requested, then RIPng [RFC2080], OSPFv3 [RFC5340] [RFC5613] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
- If OSPFv3 is requested, the equipment must comply with "Authentication/Confidentiality for OSPFv3" [RFC4552] or “Supporting Authentication Trailer for OSPFv3” [RFC7166].
- If OSPFv3 and SNMP are requested, the device must support "Management Information Base for OSPFv3" [RFC5643]
- If BGP4 protocol is requested, the equipment must comply with [RFC4271], [RFC1772], [RFC4760], [RFC1997], [RFC3392], [RFC2545], [RFC5492], [RFC6268], [RFC6608], [RFC6793], [RFC7606], [RFC7607], [RFC7705] and [RFC8212]
- If VRRP protocol is requested the equipment must comply with [RFC5798]
- If PIM-SM protocol is requested the equipment must comply with [RFC 7761/STD83] and [RFC5059]

- Support for QoS [RFC2474, RFC3140]
- If support for tunneling and dual stack is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
- If support for tunneling and dual stack is required, the device must support Generic Packet Tunneling and IPv6 [RFC2473]
- If 6PE is requested, the equipment must support "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]
- If mobile IPv6 is requested, the equipment must support MIPv6 [RFC3775, RFC5555] and "Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture" [RFC4877]
- If MPLS functionality (for example, BGP-free core, MPLS TE, MPLS FRR) is requested, the PE-routers and route reflectors must support "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]
- If MPLS Traffic Engineering is used in combination with IS-IS routing protocol, the equipment must support "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120].
- If layer-3 VPN functionality is requested, the PE-routers and route reflectors must support "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN" [RFC4659].
- IPv6 Flow Label Specification [RFC6437]

Optional support:

- Extended ICMP for multi-part messages [RFC4884]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC8415] *
- DHCPv6 Prefix Delegation [RFC8415] *
- DHCPv6 Bulk Leasequery [RFC5460]
- DHCPv6 Active Leasequery [RFC7653]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- (QOS) Active Queue Management support [RFC7567]
- Generic Routing Encapsulation [RFC2784]
- IPsec/IKEv2 (Control Plane) [RFC4301, RFC4303, RFC7268, RFC8221, RFC 8247] *
- IPsec/IKEv2 VPN (Data Plane) [RFC4301, RFC4303], RFC7269, RFC8221] *
- Using IPsec to Secure IPv6-in-IPv4 tunnels [RFC4891]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596/STD88]
- DNS message extension mechanism [RFC6891/STD75]
- DNS message size Requirements [RFC3226]
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]
- Discovering PREF64 in Router Advertisements [RFC8781]

4.5 Requirements for "network security equipment”

Equipment in this section is divided into three subgroups:

- Firewall (FW)
- Intrusion prevention device (IPS)
- Application firewall (APFW)

For every mandatory standard the applicable subgroups are specified in parentheses at the end of the line.

Mandatory support:

- IPv6 Basic specification [RFC8200/STD86] (FW, IPS, APFW) *
- IPv6 Addressing Architecture [RFC4291] (FW, IPS, APFW)
- Default Address Selection for IPv6 [RFC6724] (FW, IPS, APFW)
- ICMPv6 [RFC4443/STD89] (FW, IPS, APFW) *
- Transmission of IPv6 Packets over Ethernet Networks [RFC2464]
- SLAAC [RFC4862] (FW, IPS) *
- If support for SNMP is required:
    - SNMP protocol [RFC3411]
    - SNMP capabilities [RFC3412, RFC3413, RFC3414]
    - SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- IPv6 Router Advertisement Options for DNS Configuration [RFC8106] (FW)
- Inspecting IPv6-in-IPv4 protocol-41 traffic, which is specified in: Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (IPS)
- Path MTU Discovery [RFC8201/STD87] (FW, IPS, APFW) *
- Neighbor Discovery [RFC4861] (FW, IPS, APFW) *
- If the request is for the BGP4 protocol, the equipment must comply with RFC4271, RFC1772, RFC4760 and RFC2545 (FW, IPS, APFW)
- If the request is for a dynamic internal gateway protocol (IGP), then the required RIPng [RFC2080], OSPFv3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol. (FW, IPS, APFW)
- If OSPFv3 is requested, the equipment must comply with "Authentication/Confidentiality for OSPFv3" [RFC4552] or “Supporting Authentication Trailer for OSPFv3” [RFC7166] (FW, IPS, APFW)
- If OSPFv3 and SNMP are requested, the device must support "Management Information Base for OSPFv3" [RFC5643]
- Support for QoS [RFC2474, RFC3140] (FW, APFW)
- If tunneling is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (FW)

A Network Security Device is often placed where a layer-2 switch or a router/layer-3 switch would otherwise be placed. Depending on this placement those requirements should be included.

Functionality and features that are supported over IPv4 should be comparable with the functionality supported over IPv6. For example, if an intrusion prevention system is capable of operating over IPv4 in layer-2 and layer-3 mode, then it should also offer this functionality over IPv6. Or if a firewall is running in a cluster capable of synchronising IPv4 sessions between all members of a cluster, then this must also be possible with IPv6 sessions.

Optional support:

- DHCPv6 client/server/relay [RFC8415] *
- Stateless DHCPv6 [RFC8415] *
- DHCPv6 Prefix Delegation [RFC8415] *
- Extended ICMP for Multipart Messages [RFC4884]
- SLAAC Privacy Extensions [RFC4941]
- BGP Communities Attribute [RFC1997]
- BGP Capabilities Advertisement WITH-4 [RFC3392]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296/STD79] *
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW)
- OSPFv3 [RFC5340]
- Authentication/Confidentiality for OSPFv3 [RFC4552]
- Generic Packet Tunneling and IPv6 [RFC2473]
- DNS extensions to support IPv6 [RFC3596]
- DNS message extension mechanism [RFC6891]
- DNS message size requirements [RFC3226]
- Using IPSec to Secure IPv6-in-IPv4 Tunnels [RFC4891]
- Multicast Listener Discovery version 2 [RFC3810] *
- MLDv2 snooping [RFC4541] (when in L2 or passthrough mode) *
- Packetisation Layer Path MTU Discovery [RFC4821] and [RFC8899]
- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5739]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]
- Transmission and Processing of IPv6 Extension Headers [RFC 7045]

4.6 Requirements for CPE equipment

Mandatory support:

- Basic Requirements for IPv6 Customer Edge Routers [RFC7084] *
- Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service [RFC6092]
- If support for specific IPv4 transition mechanisms is required, the device must support the relevant requirements, as can be taken from Requirements for IPv6 Customer Edge Routers to

Support IPv4-as-a-Service [RFC8585] and Discovering PREF64 in Router Advertisements [RFC8781]

- If support for SNMP is required:
    - SNMP protocol [RFC3411]
    - SNMP capabilities [RFC3412, RFC3413, RFC3414]
    - SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]

Optional support:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296, RFC7619, RFC8221, RFC8247] *
- "MIPv6" [RFC6275, RFC5555] and "Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture" [RFC4877]
- Extended ICMP for multi-part messages [RFC4884]
- SLAAC Privacy Extensions [RFC4941]
- Transmission of IPv6 Packets over Ethernet Networks [RFC2464]
- (QOS) DS (Traffic class) [RFC2474, RFC3140]
- (QOS) Active Queue Management support [RFC7567]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821] and [RFC8899]
- Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service [RFC8585]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

4.7 Requirements for Load balancers

A load balancer distributes incoming requests and/or connections from clients to multiple servers. Load balancers will have to support several combinations of IPv4 and IPv6 connections:

- Load balancing IPv6 clients to IPv6 servers (6-to-6) **must** be supported
- Load balancing IPv6 clients to IPv4 servers (6-to-4) **must** be supported
- Load balancing IPv4 clients to IPv4 servers (4-to-4) **should** be supported
- Load balancing IPv4 clients to IPv6 servers (4-to-6) **should** be supported
- Load balancing a single external/virtual IPv4 address to a mixed set of IPv4 and IPv6 servers **should** be supported
- Load balancing a single external/virtual IPv6 address to a mixed set of IPv4 and IPv6 servers **should** be supported

Mandatory support:

- IPv6 Basic specification [RFC8200/STD86] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC6274]
- Transmission of IPv6 Packets over Ethernet Networks [RFC2464]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443/STD89] *
- Path MTU Discovery [RFC8201/STD87] *

- Neighbor Discovery [RFC4861] *
- IPv6 Router Advertisement Options for DNS Configuration [RFC8106]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596/STD88]
- DNS message extension mechanism [RFC6891]
- DNS message size requirements [RFC3226]
- If layer-7 load balancing (application level/reverse proxy, defined as ‘surrogate’ in section 2.2 of RFC3040) is requested, the equipment must support "Forwarded HTTP Extension [RFC7239]" for both IPv4 and IPv6 client addresses
- If layer-7 load balancing (application level/reverse proxy, defined as ‘surrogate’ in section 2.2 of RFC3040) is requested, the equipment must support "Transport Layer Security (TLS) Protocol Version 1.3 [RFC8446]"
- If support for IPsec is required, the device must support IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296/STD79] * and Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5685]
- If support for BGP4 is required, the equipment must comply with RFC4271, RFC1772, RFC4760 and RFC2545
- If support for a dynamic internal gateway protocol (IGP) is required, RIPng [RFC2080], OSPFv3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
- If OSPFv3 is requested, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552]

Optional support:

- Extended ICMP for multi-part messages [RFC4884]
- DS (Traffic class) [RFC2474, RFC3140]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]
- NAT64/DNS64 [RFC6146, RFC6147]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

5 Requirements for IPv6 support in software

All software must support IPv6 and be able to communicate over IPv6-only and dual-stack networks. If software includes network parameters in its local or remote server settings, it must support configuration of IPv6 parameters. The user should not experience any noticeable difference when software is communicating over IPv4 or IPv6, unless this is providing explicit benefit to the user.

Software developer/vendor must at a minimum do the following things to guarantee this:

- It is strongly recommended not to use any address literals in software code, as described in “Default Address Selection for Internet Protocol version 6” [RFC6724]
- Every place in the software where IP addresses are handled (such as in user interfaces, configuration parsing or where data is processed) all valid IPv6 address notations as specified in "IP Version 6 Addressing Architecture [RFC4291]" must be supported
- Every place where IPv6 addresses are shown or output the notation as specified in "A Recommendation for IPv6 Address Text Representation [RFC5952]" should be followed
- Resolving hostnames in DNS must support IPv6 (AAAA) answers
- Connecting to other systems and receiving connections from other systems must support IPv6 connections using the appropriate system mechanisms (e.g. networking sockets)
- When setting up a connection the software should follow Default Address Selection for Internet Protocol Version 6 [RFC6724] or Happy Eyeballs Version 2: Better Connectivity Using Concurrency [RFC8305]
- These requirements should also be checked in any library or tools used by the software

This list is not exhaustive and only covers the basic requirements.

The white paper "IP-version dependency in application software - Preparing source code for IPv6"[1] from the Netherlands IPv6 Foundation can be used to get developers started.

6 IPsec: Mandatory vs Optional

In the original IPv6 Node Requirements (RFC4294) IPsec was listed as a 'MUST' implement to be standards compliant. The updated Node Requirements RFC (RFC6434) published in 2011 changed IPsec to a 'SHOULD' implement. Reasons for the change were stated in that RFC.

The RIPE IPv6 Working Group has extensively discussed whether to make IPsec support mandatory or optional. When finalising ripe-554, the most vocal constituents showed support for moving IPsec to the optional sections, which is what is also reflected in this updated document.

While the consensus of the community was to make IPsec optional in most cases, the IETF confirmed in 2019 in the latest version of the IPv6 Node Requirements standard (RFC8504) that IPsec 'SHOULD' be implemented (not ‘MUST’). In the IETF context, a ‘SHOULD’ means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

Organisations that use IPsec or expect to use it in the future should include the following in the mandatory section when initiating the tender:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC8221, RFC7296 RFC7619 and RFC 8247] *

[1] https://www.stipv6.nl/wp-content/uploads/2013/09/ip-aspects-software-stipv6-white-paper-v12.pdf

The current set of mandatory-to-implement algorithms for the IPsec Architecture are defined in Cryptographic Algorithm Implementation Requirements for ESP and AH [RFC8221]. IPv6 nodes implementing the IPsec Architecture MUST conform to the requirements in [RFC8221].

The current set of mandatory-to-implement algorithms for IKEv2 are defined in Cryptographic Algorithm Implementation Requirements for ESP and AH [RFC8247]. IPv6 nodes implementing IKEv2 MUST conform to the requirements in [RFC8247] and/or any future updates or replacements to [RFC8247].

While the Authentication Header specified in RFC4302 was supposed to be the way to provide for integrity and non-repudiation, because it could not traverse NATs, it became common practice for ESP null to be used. As stated in Section 13.1 of RFC8504, which is taken from RFC4301, IPv6 nodes implementing the IPsec Architecture 'MUST' implement ESP (RFC4303) and 'MAY' implement AH (RFC4302).

7 Skill requirements of the systems integrator

Vendors and resellers that offer system integration services must have at least three employees who have valid certificates of competency from the equipment manufacturers for the equipment that is sold as part of the tender. Additionally these employees must have general knowledge of the IPv6 protocol, IPv6 network planning and IPv6 security (eg. as indicated by certification for these skills also). If it becomes obvious during the equipment installation and integration that the integrator's knowledge, competence and experience is not sufficient to successfully install and configure the equipment to establish normal IPv4 and IPv6 communication with the network, the agreement shall be canceled and become null and void.

The definition of proper integration, timing and degree of disruption of the network during the assembly shall be a matter of agreement between the client and systems integrator.

It is also recommended that a systems integrator and its employees have a broad knowledge of IPv6 and generic IPv6 certificates other than those specifically offered by the equipment manufacturers. These certificates can be obtained from independent education providers. Such knowledge may be awarded extra points in the tender process.

All bidders in the tender process must sign the following form, which indicates that the company and its employees have passed technical training for design, construction and integration of ICT equipment in IPv4 and IPv6 networks.

7.1 Declaration of IPv6 competence

Tender initiators should require technical IPv6 competence declaration from the equipment supplier or integrator. IPv6 knowledge and experience is required to assure proper installation and integration of equipment in the IPv6 ICT environment.

Declaration should say that the equipment supplier or system integrator declares under criminal and material responsibility:

- That they have a sufficient number of people employed to perform the offered services;
- That those employees are professionally trained for their work - design, construction and integration of ICT equipment in both IPv4 and IPv6 networks and environments;
- That the quality of offered services meets the requirements laid out in the tender documents, and that these requirements apply to both IPv4 and IPv6.

Note that declarations like this can vary depending on local legislation. Therefore translators and tender initiators should get legal advice on the exact wording for these requirements.

8 Acknowledgments

The very first (Slovenian) version of this document was created in the Go6 Expert council and the Slovenian IPv6 working group back in 2009.

The original authors would like to thank all involved in the creation and modification of the first version of this document (ripe-501, year 2009). First of all, we would like to thank Janez Sterle, Urban Kunc, Matjaz Straus, Simeon Lisec, Davor Sostaric and Matjaz Lenassi from go6 expert council for their enthusiastic governance of this document. We recognise the work done in the Slovenian IPv6 working group for their review and useful input, special recognition goes to Ivan Pepelnjak, Andrej Kobal and Ragnar Us for their efforts and work done on the document. Thanks also to the Co-chairs of RIPE IPv6 Working Group, David Kessens, Shane Kerr and Marco Hogewoning, for their support and encouragement. We would also like to thank Patrik Fältström, Torbjörn Eklöv, Randy Bush, Matsuzaki Yoshinobu, Ides Vanneuville, Olaf Maennel, Ole Trøan, Teemu Savolainen and people from RIPE IPv6 WG (Joao Damas, S.P.Zeidler, Gert Doering and others) for their input, comments and review of the document. Last, but not least we would like to thank Chris Buckridge from RIPE-NCC for correcting our grammar and wording in this document. And everybody else that contributed to this work.

The authors of the previous version of the document (ripe-554, year 2012) would like to thank the RIPE IPv6 WG and its chairs for all support and encouragement to develop a followup version of the document. Special thanks goes to Ole Trøan, editor of RFC6204 for his help in the CPE section and also suggesting other changes across the document. Thanks to Marco Hogewoning, Ivan Pepelnjak and S.P. Zeidler for great input in ideas how to make document structure and content better, Timothy Winters and Erica Johnson (both IPv6 Ready Logo committee, UNH) for help with marking RFCs they test and constructive suggestions. Thanks also to Yannis Nikolopoulos and Frits Nolet. Special thanks goes to Jouni Korhonen, Jari Arkko, Eric Vyncke, David Freedman, Tero Kivinen and Michael Richardson for some very useful comments and suggestions that made this document much better.

The authors of the current version of the document would like to thank members of the RIPE IPv6

Working Group and its chairs, and especially Jens Link, Martin Schröder, Fernando Gont, Enno Rey, Dave Taht, Azalea Fernandez, Yannis Nikolopoulos and Eric Vyncke for their comments.

Suggestions for improvement of current document and comments can be sent to the RIPE IPv6 WG or RIPE BCOP TF mailing lists.
https://www.ripe.net/mailman/listinfo/ipv6-wg/
https://www.ripe.net/mailman/listinfo/bcop