Requirements For IPv6 in ICT Equipment

Proposal authors:

- ***Merike Käo, <merike@doubleshotsecurity.com>***
- ***Jan Žorž, <jan@go6.si>***
- ***Sander Steffann, <sander@steffann.nl>***

Table of content:

Introduction

To ensure the smooth and cost-efficient uptake of IPv6 across their networks, it is important that governments and large enterprises specify requirements for IPv6 compatibility when seeking tenders for Information and Communication Technology (ICT) equipment and support. This document is intended to provide a Best Current Practice (BCP) and does not specify any standards or policy itself.

It can serve as a template that can be used by governments, large enterprises and all other organisations when seeking IPv6 support in their tenders or equipment requirements and offer guidance on what specifications to ask for. 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, which operate independent of the RIPE community, and that any of these standards might be changed or become replaced with a newer version. You may also need to adjust the recommendations to your specific local needs.

Some parts of this section are loosely based on the NIST/USGv6 profile developed by the US government:[1]
http://www.antd.nist.gov/usgv6/
The authors have modified these documents to make them more universally applicable. This option includes a list of RFC specification standards, which must be supported, divided into eight categories of devices.

This document also follows IPv6 Node requirements document, RFC6434. This RFC is the general IETF guidance on what parts of IPv6 need to be implemented by different devices.

General information on how to use this document

An IPv6 Ready Logo certificate can be required for any device. This is the easiest way for vendors providing the equipment to prove that it fulfills basic IPv6 requirements. 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.

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. Please note that the tender initiator should decide what functionality is required, not the equipment vendor.

Certain features that are in the 'optional' section in this document might be important for your specific case and/or organisation. In such cases the tender initiator should move the requirement to the 'required' section in their tender request.

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.

About the IPv6 Ready Logo program: http://www.ipv6ready.org/

Also note that there exists the BOUNDv6 project whose goal is to create a permanent multi-vendor network environment connecting approved laboratories

[1] The USGv6 specifications are currently undergoing an updated revision which is

where the community can test IPv6 enabled applications and devices in meaningful test scenarios. Tender initiators are encouraged to have a look and also use the results of this project.

About BOUNDv6: http://www.boundv6.org/

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 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 *.

Proposed generic text for the tender initiator

In every tender, following text shall be included:

All ICT hardware as subject of this tender must support both the IPv4 and IPv6 protocols. Similar performance must be provided for both protocols in input, output and/or throughput data-flow performance, transmission and processing of packets.

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

Any software that communicates via the IP protocol must support both protocol versions (IPv4 and IPv6). The difference must not be noticeable to users.

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

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

Lists of mandatory and optional RFC/3GPP technical specifications support for various hardware and software

Requirements are divided in hardware equipment and integrator support.

It should be assumed that all IPv4 traffic would migrate to IPv6. All requirements placed on IPv4 traffic capabilities like latency, bandwidth and throughput should also be required for IPv6 traffic.

IPsec: Mandatory or Optional

In the original IPv6 Node Requirements (RFC 4294) IPsec was listed as a 'MUST' implement to be standards compliant. The updated RFC (RFC 6434) changed

IPsec to a 'SHOULD' implement. Reasons for the change are stated in this new RFC.

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

While the consensus of the community was to make IPsec optional in most cases, the IETF have now stated that IPsec 'SHOULD' be implemented in the latest version of the IPv6 Node Requirements standard (RFC 6434). 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, RFC4302, RFC5996] *

Definitions and descriptions of different type 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.

Host: A host is a network participant that sends and receives packets but does not forward them on behalf of others.

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.

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.

Mobile Device: In the context of this document a mobile device is a node that connects to a 3GPP defined system using some 3GPP specified access technology (such as 2G, 3G, or LTE). For situations where the network logic is being provided solely by a dedicated device A connected to another device B, the specification will refer to device A and not to device B. If the protocol logic is distributed (e.g. a computer with an external Ethernet interface that performs TCP checksum offloading), the aggregate system is being referred to.

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.

Lists of required RFC/3GPP standards for different type of hardware

ICT hardware equipment is divided into seven functional groups:

- Host: client or server
- Layer 2 switch
- Router or layer 3 switch
- Network security equipment (firewalls, IDS, IPS,...)
- CPE
- Mobile Device
- Load Balancer

We have divided the following requirements into two categories, “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 *.

Requirements for "host" equipment

Mandatory support:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- DHCPv6 client [RFC3315] *
- SLAAC [RFC4862] *
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- 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 mobile IPv6 is required, the device must support “MIPv6” [RFC3775, RFC5555] and “Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture” [RFC4877]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Revised ICMPv6 [RFC5095] *

Optional support:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- 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]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

Requirements for consumer grade "layer 2 switch" equipment

Optional support (management)

- MLDv2 snooping [RFC4541]

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]

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

Mandatory support:

- MLDv2 snooping [RFC4541]
- DHCPv6 filtering [RFC3315]
- Router Advertisement (RA) filtering [RFC4862]
- Dynamic "IPv6 Neighbor solicitation/advertisement" inspection [RFC4861]
- Neighbor Unreachability Detection [NUD, RFC4861] filtering
- Duplicate Address Detection [DAD, RFC4429] snooping and filtering.[2]

Optional support (management)

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- IPv6 Routing Header [RFC2460, Next Header value 43] filtering *
- Revised ICMPv6 [RFC5095] *
- UPnP filtering

Requirements for "router or layer-3 switch" equipment

Mandatory support:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]

[2] The IETF Source Address Validation Improvements (SAVI) working group is currently working on RFCs that specify a framework for source address validation. Once these RFCs are published, the NUD and DAD filtering references can be changed accordingly.

- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- MLDv2 snooping [RFC4541]
- Multicast Listener Discovery version 2 [RFC3810] *
- Router-Alert option [RFC2711]
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- Revised ICMPv6 [RFC5095] *
- If a dynamic interior gateway protocol (IGP) is requested, then RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
- If OSPF-v3 is requested, the equipment must comply with "Authentication/Confidentiality for OSPF-v3" [RFC4552]
- If BGP4 protocol is requested, the equipment must comply with RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 and RFC2545
- 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 the IS-IS routing protocol is requested the equipment must support "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120]
- 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 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]
- 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]

Optional support

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- DHCPv6 client / server / relay [RFC3315] *
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]

- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- Route Refresh for BGP-4 Capabilities [RFC2918]
- BGP Extended Communities Attribute [RFC4360]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Generic Routing Encapsulation [RFC2784]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Using IPsec to Secure IPv6-in-IPv4 tunnels [RFC4891]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size Requirements [RFC3226]
- 127-bit IPv6 Prefixes on Inter-Router Links [RFC6164]
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

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 [RFC2460] (FW, IPS, APFW) *
- IPv6 Addressing Architecture [RFC4291] (FW, IPS, APFW)
- Default Address Selection [RFC3484] (FW, IPS, APFW)
- ICMPv6 [RFC4443] (FW, IPS, APFW) *
- SLAAC [RFC4862] (FW, IPS) *
- Revised ICMPv6 [RFC5095] *
- Inspecting IPv6-in-IPv4 protocol-41 traffic, which is specified in: Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (IPS)
- Router-Alert option [RFC2711] (FW, IPS)
- Path MTU Discovery [RFC1981] (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], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol. (FW, IPS, APFW)
- If OSPF-v3 is requested, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- Support for QoS [RFC2474, RFC3140] (FW, APFW)
- If tunneling is reqired, 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

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- DHCPv6 client / server / relay [RFC3315] *
- Extended ICMP for Multipart Messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- 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]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW)
- OSPF-v3 [RFC5340]
- Authentication / Confidentiality for OSPF-v3 [RFC4552]
- Generic Packet Tunneling and IPv6 [RFC2473]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]

- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- DNS extensions to support IPv6 [RFC3596]
- DNS message extension mechanism [RFC2671]
- 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]
- 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]

Requirements for CPE equipment

Mandatory support:

- RFC6204 (Basic Requirements for IPv6 Customer Edge Routers) *

Optional support:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- If support for mobile IPv6 is required, the device needs to comply to “MIPv6” [RFC3775, RFC5555] and “Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture” [RFC4877]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- 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]
- IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) [RFC5969]
- Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion [RFC6333] If support this then also must support Dynamic Host Configuration protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite [RFC6334]
- The A+P Approach to the IPv4 Address Shortage [RFC6346]
- 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]

Requirements for Mobile Devices

Mandatory support:

- IPv6 basic specification [RFC2460] *
- Neighbor Discovery for IPv6 [RFC4861] *
- IPv6 Stateless Address Autoconfiguration [RFC4862] *
- IPv6 Addressing Architecture [RFC4291] *
- ICMPv6 [RFC4443] *
- IPv6 over PPP [RFC2472]
- Multicast Listener Discovery version 2 [RFC3810] *
- IPv6 Router Alert Option [RFC2711]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]

Optional support:

- Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [RFC4941]
- Path MTU Discovery for IPv6 [RFC1981] *
- Generic Packet Tunneling for IPv6 [RFC2473]
- DHCPv6 [RFC3315] *
- Stateless DHCPv6 [RFC3736]
- DHCPv6 option for SIP servers [RFC3319]
- IPv6 Prefix Options for DHCPv6 [RFC3633]
- Prefix Exclude Option for DHCPv6-based Prefix Delegation [draft-ietf-dhc-pd-exclude]
- Default Address Selection [RFC3484]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- IKEv2 Mobility and Multihoming Protocol MOBIKE [RFC 4555]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

References:

- 3GPP
    - Internetworking Between Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) [3GPP TS 29.061]
    - GPRS Service Description [3GPP TS 23.060]
    - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access [3GPP TS 23.401]
    - Signalling flows for IP multimedia Call control based on SIP and SDP [3GPP TS 24.228]
    - IP multimedia call control protocol based on SIP and SDP [3GPP TS 24.229]
    - IP Based Multimedia Framework [3GPP TS 22.941]
    - Architectural Requirements [3GPP TS 23.221]

    - Packet domain; Mobile Stations (MS) Supporting Packet Switching Service [3GPP TS 27.060]
    - IPv6 migration guidelines [3GPP TR 23.975]
- IETF
    - IPv6 for Some Second and Third Generation Cellular Hosts [RFC3316]
    - Recommendations for IPv6 in 3GPP Standards [RFC3314]
    - IPv6 in 3rd Generation Partnership Project (3GPP) [RFC6459]

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

If a load balancer provides layer-7 (application level / reverse proxy, defined as ‘surrogate’ in section 2.2 of RFC3040) load balancing then support for the X-forwarded-for (or equivalent) header in HTTP **must** be provided in order to make the source IP address of the client visible to the servers.

Mandatory support:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Revised ICMPv6 [RFC5095] *

Optional support:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]

- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- 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]
- If support for IPsec is required, the device must support IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] * 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, the RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
- If OSPF-v3 is requested, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- IPv6 Host-to-Router Load Sharing [RFC4311] (FW)
- Default Router Preferences and More-Specific Routes [RFC4191] (FW)

Requirements for IPv6 support in software

All software must support IPv4 and IPv6 and be able to communicate over IPv4-only, IPv6-only and dual-stack networks. If software includes network parameters in its local or remote server settings, it should also support configuration of IPv6 parameters.

All features that are offered over IPv4 must also be available over IPv6. 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.

It is strongly recommended not to use any address literals in software code, as described in “Default Address Selection for Internet Protocol version 6” [RFC3484].

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 additionally 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.

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 IPv6 in the 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 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 advise on the exact wording for these requirements.

Acknowledgments

First version of this document was done in the Go6 Expert council and the Slovenian IPv6 working group.

The authors would like to thank all involved in creation and modification of previous version of this document. 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 this current document would like to thank RIPE IPv6 WG and it's chairs for all support end 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.

Suggestions for improvement of current document and comments can be sent to <ripe501team@go6.si> or to RIPE IPv6 Working Group mailinglist.