Requirements For IPv6 in ICT Equipment

Jan Žorž
Sander Steffann

Document ID: ripe-501
Date: November 2010

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 computer technology (ICT) equipment and support. This document is intended to provide a Best Common Practice (BCP) template that can be used by governments or large enterprises when developing tender documents. It can also serve as an aid to those people or organisations interested in tendering for government or enterprise contracts.

Formulating requirements for IPv6 support can be done in several ways. In this document we look at three different options:

1. Option 1 is based loosely on the NIST/USGv6 profile developed by the US government:
   http://www.antd.nist.gov/usgv6/
   The go6 expert council and the Slovenian IPv6 working group have modified these documents to make them more universally applicable. The new draft includes a list of RFC specification standards which must be supported, divided into four categories of devices.
2. Option 2 is based on compliance with the “IPv6 Ready” program, as specified by the IPv6 Forum. This program is divided into two phases: Phase 1 includes testing and certification of the basic "core" protocols, while Phase 2 includes testing and certification of advanced IPv6 functionality.
3. Option 3 is a combination of the first two approaches.

Option 1

Requirements are divided in equipment and integrator support (output from go6 IPv6 WG).

The following is the draft text that we propose be included in public tenders for ICT equipment, specifying requirements for IPv6 capability and support:

All ICT hardware must support both the IPv4 and IPv6 protocols. Similar performance must be provided for both protocols. There should not be more than ...% difference in input, output and/or throughput data-flow performance, transmission and processing of packets between the two protocols.

(Notes for tender initiators: For high-end devices we recommend to state a maximum difference of 15%. For enterprise grade devices we recommend a maximum of 30%. For consumer grade devices we recommend a maximum of 40%.)

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

Requirements for support of standards

ICT hardware equipment can be roughly divided into four groups:

- Host: client or server
- Layer 2 switch
- Router or layer 3 switch
- Equipment to ensure network security (firewalls, IDS, IPS, ...)

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.

Please note that all RFC references are correct at the time of writing, but may be superseded by developments in the IETF. For all updates, please see: http://www.rfc-editor.org/

Hardware

Any hardware that does not comply to all of the mandatory standards is marked as inappropriate.

Requirements for "host" equipment

Mandatory support:

- IPv6 Basic specification [RFC2460]
- IPv6 Addressing Architecture basic [RFC4291]
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443]

- DHCPv6 client [RFC3315]
- SLAAC [RFC4862]
- Path MTU Discovery [RFC1981]
- Neighbour Discovery [RFC4861]
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
- IPsec-v2 [RFC2401, RFC2406, RFC2402]
- IKE version 2 (IKEv2) [RFC4306, RFC4718]
- 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]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]

Optional support:
- Revised ICMPv6 [RFC5095]
- Extended ICMP for multi-part messages [RFC4884]
- SEND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736]
- DS (Traffic class) [RFC2474, RFC3140]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- Cryptographically Generated Addresses [RFC3972]
- IPsec-v3 [RFC4301, RFC4303, RFC4302]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- Multicast Listener Discovery version 2 [RFC3810]
- Packetization Layer Path MTU Discovery [RFC4821]

Requirements for consumer grade "layer 2 switch" equipment
Mandatory support:
- MLDv2 snooping [RFC4541]

Optional support (management)
- IPv6 Basic specification [RFC2460]
- IPv6 Addressing Architecture basic [RFC4291]
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443]
- SLAAC [RFC4862]
- SNMP protocol [RFC3411]

- SNMP capabilities [RFC3412, RFC3413, RFC3414]

Requirements for enterprise/ISP core grade "layer 2 switch" equipment
Mandatory support:

- MLDv2 snooping [RFC4541]
- DHCPv6 snooping [RFC3315]
  DHCPv6 messages must be blocked between subscribers and the network so that false DHCPv6 servers cannot distribute addresses.
- Router Advertisement (RA) filtering [RFC4862, RFC5006]
  RA filtering must be used in the network to block unauthorised RA messages.
- Dynamic "IPv6 neighbour solicitation/advertisement" inspection [RFC4861]
  There must be an IPv6 neighbour solicitation/advertisement inspection, as in IPv4 "Dynamic ARP Inspection". The table with MAC-address and link-local and other assigned IPv6-addresses must be dynamically created by SLAAC or DHCPv6 messages.
- Neighbour Unreachability Detection [NUD, RFC4861] filtering
  There must be a NUD filtering function to ensure that false NUD messages cannot be sent.
- Duplicate Address Detection [DAD, RFC4429] snooping and filtering
  Only authorised addresses may be allowed as source IPv6 addresses in DAD messages from each port.

Optional support (management)

- IPv6 Basic specification [RFC2460]
- IPv6 Addressing Architecture basic [RFC4291]
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443]
- SLAAC [RFC4862]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- IPv6 Routing Header [RFC2460, Next Header value 43] snooping
- IPv6 Routing Header messages must not be allowed between subscriber ports and subscriber and uplink to prevent routing loops [See also RFC5095, Deprecation of Type 0 Routing Headers in IPv6]
- UPnP filtering
- UPnP messages must always be blocked between customer ports. There may be a possibility to filter different Ether types to allow only 0x86dd between subscriber ports. And most probably you must also permit 0×800 and 0×806 for IPv4.

Requirements for "router or layer 3 switch" equipment

Mandatory support:

- IPv6 Basic specification [RFC2460]
- IPv6 Addressing Architecture basic [RFC4291]
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443]
- SLAAC [RFC4862]
- MLDv2 snooping [RFC4541]
- Router-Alert option [RFC2711]
- Path MTU Discovery [RFC1981]
- Neighbour Discovery [RFC4861]
- Classless Inter-domain routing [RFC4632]
- If dynamic internal guidance 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]
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
- Using IPsec to Secure IPv6-in-IPv4 tunnels [RFC4891]
- Generic Packet Tunneling and IPv6 [RFC2473]
- If 6PE is requested, the equipment must comply with "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]
- Multicast Listener Discovery version 2 [RFC3810]
- If mobile IPv6 is requested, the equipment must comply with 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)" [RFC 4798]
- 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" [RFC 4659]
- 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)" [RFC 5120]

Optional support

- Revised ICMPv6 [RFC5095]
- DHCPv6 client / server [RFC3315]
- Extended ICMP for multi-part messages [RFC4884]
- SEND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736]
- DHCPv6 PD [RFC3633]
- Route Refresh for BGP Capabilities-4 [RFC2918]
- BGP Extended Communities Attribute [RFC4360]
- (QOS), Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Generic Routing Encapsulation [RFC2784]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- Cryptographically Generated Addresses [RFC3972]
- ProSafe-v3 [RFC4301, RFC4303, RFC4302]
- IPSec-v2 [RFC2401, RFC2406, RFC2402]
- IKE version 2 (IKEv2) [RFC4306, RFC4718]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- Mibsam SNMP for IP [RFC4293] Forwarding [RFC4292], IPsec [RFC4807] 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: http://tools.ietf.org/html/draft-kohno-ipv6-prefixlen-p2p-01
- Packetization Layer Path MTU Discovery [RFC4821]
- When IS-IS routing protocol is requested, the equipment should support "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC 5120] (this support is highly recommended)

Requirements for "network security" equipment

Equipment in this section is divided into three subgroups:

- Firewall (FW)
- Intrusion prevention device (IMS)
- 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 basic [RFC4291] (FW, IPS, APFW)
- Default Address Selection [RFC3484] (FW, IPS, APFW)
- ICMPv6 [RFC4443] (FW, IPS, APFW)
- SLAAC [RFC4862] (FW, IPS)
- Router-Alert option [RFC2711] (FW, IPS)
- Path MTU Discovery [RFC1981] (FW, IPS, APWF)
- Neighbour 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 guidance protocol (IGP), then the required RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308]. The contracting authority shall specify the required protocol. (FW, IPS, APFW)
- If the requested OSPF-v3, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- Support for QoS [RFC2474, RFC3140] (FW APFW)
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (FW)
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW)

Functionality and features that are supported over IPv4 should be comparable with the functionalities 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 synchronizing IPv4 sessions between all members of a cluster, then this must also be possible with IPv6 sessions.

Optional support

- Revised ICMPv6 [RFC5095]
- DHCPv6 client / server [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-v3 [RFC4301, RFC4303, RFC4302]
- OSPF-v3 [RFC5340]
- Authentication / Confidentiality for OSPF-v3 [RFC4552]
- Generic Packet Tunneling and IPv6 [RFC2473]
- IPsec-v2 [RFC2401, RFC2406, RFC2402]
- IKE version 2 (IKEv2) [RFC4306, RFC4718]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- DNS protocol extensions for incorporating IPv6 DNS resource records [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)
- Packetization Layer Path MTU Discovery [RFC4821]

Requirements for IPv6 support in software

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

Functional differences must not be significantly different between IPv4 and IPv6. The user should not experience any significant difference when software is communicating over IPv4 or IPv6.

Skill requirements of the systems integrator

Vendors and reseller 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. These certificates must indicate a general knowledge of the IPv6 protocol, IPv6 network planning and IPv6 security. 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 cancelled 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
Declaration of technical competence for planning, building and integrating ICT equipment in IPv4 and IPv6 networks and environments

Company: _____

Address: _____

declares, under criminal and material responsibility:

- That we have a sufficient number of people employed to perform offered services;
- That 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.

Place _____, date _____

Stamp and signature of systems integrator

Option 2

The tender initiator can require ICT equipment to be “Phase 1” or “Phase 2” certified under the “IPv6 Ready” program. Tests for both phases of certification can be done in five accredited laboratories around the world: TTA (Korea), BII (China), CHT-TL (Taiwan), IRISA (France) and UNH-IOL (US). These tests determine basic IPv6 protocols compliance (Phase 1, approximately 150 tests) and advanced IPv6 functionality (Phase 2, over 450 tests).

- About the IPv6 Ready program
- About Phase 1
- About Phase 2

Any other requirements for the system integrator remain the same as in the first option.

Proposed text for the tender initiator:

ICT equipment that supports and communicates over the IPv4 protocol must also support the IPv6 protocol and be able to communicate with other devices over IPv6. Basic IPv6 support must be verified and certified by the IPv6 Ready program with a “Phase 1” logo certificate. A “Phase 2” logo certificate will be awarded additional points (+10%) in the tender evaluation procedure.

Option 3

The third option is a mix of the two alternatives outlined above. The IPv6 Ready program does not cover all equipment that correctly supports IPv6, so declaring such equipment ineligible may not be desirable. This option suggests that the tender initiator specify that eligible equipment may be either Phase 1 or Phase 2 certified under the IPv6 Ready program, or be compliant with the appropriate RFCs listed in Option 1.

Proposed text for the tender initiator:

ICT equipment that supports and communicates over the IPv4 protocol must also support the IPv6 protocol and be able to communicate with other devices over IPv6.

Basic IPv6 support must be verified and certified by the IPv6 Ready program with a "Phase 1" logo certificate. A "Phase 2" logo certificate will be awarded additional points (+10%) in the tender evaluation procedure.

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 Option 1]

Acknowledgments

The authors would like to thank all involved in creation and modification 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 the go6 expert council for their enthusiastic governance of this document. We recognise the work done in the Slovenian IPv6 working group and thank them for their review and useful input, with special recognition 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 and Matsuzaki Yoshinobu, Ides Vanneuville, Olaf Maennel, Ole Troan, Teemu Savolainen and people from RIPE IPv6 WG (Joao Damas, S.P.Zeidler, Gert Döring and others) for their input, comments and review of the document. Last, but not least we would like to thank the RIPE NCC staff for correcting our grammar and wording in this document. And everybody else that contributed to this work.