TECHNICAL CODE

INTERNET PROTOCOL VERSION 6 (IPv6) - COMPLIANT EQUIPMENT (FIRST REVISION)

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network functionality, network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.skmm.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Malaysian Communications & Multimedia Commission (MCMC)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Page

Committee representation

Internet Protocol version 6 Working Group (IPv6 WG) under the Malaysian Technical Standards Forum Bhd (MTSFB), which developed this Technical Code, consists of representatives from the following organisations:

American Malaysian Chamber of Commerce

Apple Inc

Cisco Systems Malaysia

Digi Telecommunications Sdn Bhd

Hewlett Packard Enterprise

My6 Initiative Berhad

Panasonic AVC Networks

Persatuan Industri Komputer dan Multimedia Malaysia

SIRIM Berhad

Sony EMCS (M) Sdn Bhd

Telekom Malaysia Berhad

webe digital sdn bhd

Foreword

This technical code for Internet Protocol version 6 (IPv6) - Compliant Equipment (First Revision) ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standard Forum Bhd (MTSFB) via its Internet Protocol version 6 Working Group (IPv6 WG).

This Technical Code was developed for the purpose of certifying communications equipment under the Communications and Multimedia (Technical Standards) Regulations 2000.

Major modifications in this revision are as follows:

a) deletion of normative references that are not applicable;

b) refined the category of equipment as non-exhaustive examples of equipment which are subjected to this Technical Code;

c) updated on current RFCs;

d) addition of 5-core compliance requirements for the categories of equipment as minimum specifications for compliance purposes; and

e) incorporation of IPv6 Forum's IPv6 Ready Test plans such as UNH-IOL Test Specification Core Protocol v4.0.7 for IPv6 compliance requirement.

This Technical Code cancels and replaces the MCMC MTSFB TC T013:2016, *Specifications for Internet Protocol version 6 (IPv6) Compliant Equipment.*

This Technical Code shall continue to be valid and effective until reviewed or cancelled.

INTERNET PROTOCOL VERSION 6 (IPv6) - COMPLIANT EQUIPMENT (FIRST REVISION)

1. Scope

This Technical Code defines the core technical functions, the category of equipment and compliance requirement for Internet Protocol version 6 (IPv6). This document aims to assist various stakeholders from government and non-government bodies, agencies, organisations as well as from the industry in ensuring that any products with internet functionality to be used in Malaysia meets the minimum capabilities to support an IPv6 ecosystem.

This would be in line with the national aspiration to accelerate the adoption of IPv6 services in Malaysia and to allow consumers access to application or services using IPv6.

2. Normative references

The following normative references are indispensable for the application of this technical code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative reference (including any amendments) applies.

IPv6 Ready, *Test Specification Core Protocols*

NIST SP500-267, *A Profile for IPv6 in the U.S. Government*

IETF, *Request for Comments (RFC)* (as listed in Annex A)

3. Terms and definitions

For the purpose of this Technical Code, the following terms and definitions apply.

3.1 Closed Circuit Television (CCTV)

Closed Circuit Television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

3.2 Internet Protocol Television Set Top Box (IPTV STB)

Internet Protocol Television Set Top Box (IPTV STB) is an information appliance device that provides Internet Protocol (IP) network service from the service provider. IPTV STB is sold or leased directly by the service provider.

3.3 Network Element (NE)

Network Element (NE) is to provide network connectivity, control IP protocols, packet routing and forwarding from source/origin to a specific destination.

3.4 Network Service Element (NSE)

The primary functions of Network Service Element (NSE) are to permit, deny and/or monitor traffic between interfaces in order to detect or prevent potential malicious activity.

3.5 Terminal/Host

Terminal/Host is devices or elements, which are, network participant that sends and receives packets but does not forward them on behalf of others. The primary purpose is to support application protocols that are the source and/or destination of IP layer communication.

3.6 White box switch

A white box switch is a network switch that is assembled from standardised commodity parts. A white box switch may come pre-loaded with minimal software or it may be sold as a bare metal device.

4. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

See Annex B.

5. Equipment categories

This Technical Code defines the technical requirements for equipment to be IPv6 compliant with the following functions:

a) Terminal/Host;

b) NE; and

c) NSE.

The equipment to be qualified shall have its primary purpose or dependent on IP connectivity to serve its purpose.

In the event the equipment has multiple primary functions, the technical requirements in Annex C shall be fulfilled to comply with this technical code. For certification purposes, an equipment shall be declared based on its highest function whereby the Annex D applies. For example, if an equipment has a host and NSE as primary functions, then NSE shall be its primary function.

An example (non-exhaustive) of equipment or elements which are subject to this Technical Code are as defined in Table 1.

Table 1. Example of equipment

Category	Equipment
Terminals/ Host	a) Any other user terminals, User Equipment (UE) requiring IP connectivity b) Internet of Things (IoT) devices that required IP connectivity c) CCTV d) IP Camera e) IPTV STB f) Layer 2 switch and WiFi Access Point (AP)

Table 1. Example of equipment *(continued)*

Category	Equipment
NE	a) Layer 3 switch/router b) Load Balancer (LB) c) Internet Protocol Public Automatic Branch Exchange (IP PABX) d) Residential Gateway (RG) e) Broadband Remote Access Server (BRAS) f) Radio Access Network (NodeB, eNodeB) g) Mobility Management Entity (MME) h) Serving GPRS Support Node (SGSN) i) Gateway GPRS Support Node (GGSN) j) Serving Gateway (S-GW) k) Packet Data Network Gateway (P-GW)
NSE	a) Firewall (FW) b) Application Firewall (APFW) c) Intrusion Protection System (IPS) d) Intrusion Detection System (IDS)

NOTES:

1. Equipment may apply for multiple categories.
2. Equipment may function as Terminal/Host, NE and/or NSE.
3. Equipment/white box/servers and Personal Computer (PC) which have Operation System (OS) that are supplied by a 3rd party and has the potential for IP connectivity as one of its primary function shall comply for certification.
4. For products that are sharing the same OS, testing on 1 representative model is acceptable, per product type.
5. IPv6 is also mandated for cellular products (under Terminal/Host). However, 3rd Generation Partnership Project (3GPP) standards will take precedence over IPv6 Forum IPv6 Ready Test Specifications Core Protocol document for cellular interfaces.

6. Segments

Segments refer to classes or categories in which IPv6 compliant equipment may be deployed wherever applicable. For any given function of an IPv6 compliant equipment, the model of equipment to cater for each segment may be different as each segment has specific needs and specifications. Thus, it is important to be able to determine, for any IPv6 compliant equipment; its intended segment of deployment prior to deliberating on the specifications listed in this document.

3 segments are described as follows:

a) Consumer

The consumer is referring to the retail end users as follows:

i) fixed (wired or wireless broadband); and

ii) mobile cellular (3G/4G/5G).

b) Enterprise

i) enterprise; and

ii) government agencies.

c) Service providers

i) telcos and celcos;

ii) network service provider; and

iii) internet service provider.

7. Functional requirements

IPv6 functional requirements are categorised as Table 2 below.

Table 2. IPv6 functional requirements

No	IPv6 Functional	Description
1	IPv6 basic capabilities	Fundamental operation and configuration of the IP layer
2	Addressing	Technical requirement for IPv6 address architecture and Cryptographically Generated Addresses (CGAs)
3	Transition mechanisms	Technical requirement to adopt IPv6 in existing Internet Protocol version 4 (IPv4) infrastructure
4	Link specific	Technical requirement for different link layer technologies
5	Routing protocols	Technical requirement for interior and exterior gateway protocol
6	Multicasting	Technical requirement for generalised multicast and configure options for Single Source Multicast (SSM) capabilities
7	Network management	Technical requirement for Simple Network Management Protocol (SNMP) and its Management Information Bases (MIBs)
8	Application requirement	Technical requirement for network services such as: a) Domain Name System (DNS); b) Dynamic Host Configuration Protocol (DHCP); and c) Socket Application Programming Interface (API).
9	Mobility	Technical requirement for Mobile IP (MIP) and configure options for Network Mobility (NEMO)
10	Quality of service	Technical requirement for Differentiated Service (DS) mechanisms in the router
11	IP Security	Technical requirement for IP Security (IPSec) and its key management protocol

Table 2. IPv6 functional requirements *(continued)*

No	IPv6 Functional	Description
12	Network protection device	Technical requirement: a) FW b) APFW; c) IDS; d) IPS; and e) Session Border Controller (SBC).

The details of its functions are shown in Table C.1 in Annex C.

8. IPv6 compliance requirement

Annex D describes the 5-core compliance requirement across the 3 categories of equipment in all segments outlined in Clause 6. There are 2 levels of compliance requirement; which are as follows:

a) M is a mandatory test case where the industry shall comply; and

b) O is an optional test case where the industry shall comply if the option is implemented.

These requirements are the minimum specifications for compliance purposes. The core compliance requirement for equipment in enterprise and service providers segments are the same thus have been combined for simplicity.

9. Sample test report

As IPv6 standards are still evolving, exceptions may be granted and/or test cases may be updated or invalidated based on the development of global standards. The latest version of the Test Specification Document from IPv6 Forum shall be accepted.

Refer to IPv6 Forum's IPv6 Ready Test plans such as UNH-IOL Test Specification Core Protocols v4.0.7 or higher for the detailed testing steps. The device shall comply with and pass all the mandatory IPv6 tests as specified in Annex D.

A sample of test report format is shown in Annex E as an indication to interested stakeholders on information that should be presented for certification.

Annex A
(Normative)

Normative reference

Table A.1. Request for Comments (RFC) list

RFC Number	Title
RFC 1195	Use of Open System Interconnection (OSI) Intermediate System to Intermediate System (IS-IS) for routing in Transmission Control Protocol (TCP)/IP and dual environments
RFC 1772	Application of the Border Gateway Protocol (BGP) in the Internet
RFC 2404	The use of HMAC-SHA-1-96 within Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 2410	The NULL encryption algorithm and its use with IPsec
RFC 2451	The ESP Cipher Block Chaining (CBC) Mode Cipher Algorithms
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks
RFC 2467	Transmission of IPv6 Packets over Fibre Distributed Data Interface (FDDI) Networks
RFC 2473	Generic packet tunnelling in IPv6 specification
RFC 2474	Definition of the DS field in the IPv4 and IPv6 headers
RFC 2475	An architecture for DS
RFC 2491	IPv6 over Non-Broadcast Multiple Access (NBMA) networks
RFC 2507	IP header compression
RFC 2508	Compressing IP/User Datagram Protocol (UDP)/Real-Time Transport Protocol (RTP) Headers for low-speed serial links
RFC 2526	Reserved IPv6 subnet anycast addresses
RFC 2545	Use of Border Gateway Protocol version 4 (BGP-4) multiprotocol extensions for IPv6 inter-domain routing
RFC 2597	Assured forwarding Per Hop Behaviour (PHB) group
RFC 2675	IPv6 Jumbograms
RFC 2710	Multicast Listener Discovery (MLD) for IPv6
RFC 2711	IPv6 router alert option
RFC 2784	Generic Routing Encapsulation (GRE)
RFC 2983	DS and tunnels
RFC 3056	Connection of IPv6 domains via IPv4 clouds
RFC 3086	Definition of DS PHB and rules for their specification
RFC 3095	RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP and uncompressed
RFC 3140	PHB Identification Codes
RFC 3146	Transmission of IPv6 packets over IEEE 1394 networks
RFC 3168	The addition of Explicit Congestion Notification (ECN) to IP

Table A.1. Request for Comment (RFC) list *(continued)*

RFC Number	Title
RFC 3173	IP Payload Compression Protocol (IPComp)
RFC 3226	Domain Name System Security Extensions (DNSSEC) and IPv6 A6 aware server/resolver message size requirements
RFC 3241	ROHC over Point-to-Point Protocol (PPP)
RFC 3246	An Expedite Forwarding (EF) PHB
RFC 3247	Supplemental information for the new definition of the EF PHB
RFC 3260	New terminology and clarifications for Diffserv
RFC 3289	Management information base for the DS architecture
RFC 3306	Unicast-Prefix-based IPv6 multicast addresses
RFC 3307	Allocation guidelines for IPv6 multicast addresses
RFC 3315	DHCP for IPv6
RFC 3411	An architecture for describing SNMP management frameworks
RFC 3412	Message processing and dispatching for the SNMP
RFC 3413	SNMP Applications
RFC 3414	User-based Security Model (USM) for the Simple Network Management Protocol version 3 (SNMPv3)
RFC 3493	Basic socket interface extensions for IPv6
RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3542	Advanced sockets API for IPv6
RFC 3566	The AES-XCBC-MAC-96 algorithm and its use with IPsec
RFC 3572	IPv6 over Multiple Access Protocol Over SONET/SDH (MAPOS)
RFC 3590	Source address selection for the MLD Protocol
RFC 3596	DNS extensions to support IPv6
RFC 3602	The AES-CBC cipher algorithm and its use with IPsec
RFC 3633	IPv6 prefix options for DHCP version 6 (DHCPv6)
RFC 3678	Socket interface extensions for multicast source filters
RFC 3686	Using Advanced Encryption Standard (AES) counter mode with IPSec ESP
RFC 3736	Stateless DHCP service for IPv6
RFC 3810	Multicast Listener Discovery version 2 (MLDv2) for IPv6
RFC 3843	ROHC: A compression profile for IP
RFC 3879	Deprecating site local addresses
RFC 3948	UDP encapsulation of IPSec ESP packets
RFC 3956	Embedding the Rendezvous Point (RP) address in an IPv6 multicast address
RFC 3963	NEMO basic support protocol
RFC 3971	SEcure Neighbour Discovery (SEND)
RFC 3972	CGA

Table A.1. Request for Comment (RFC) list *(continued)*

RFC Number	Title
RFC 3986	Uniform Resource Identifier (URI): Generic syntax
RFC 4007	IPv6 scoped address architecture
RFC 4022	Management information base for the TCP
RFC 4038	Application aspects of IPv6 transition
RFC 4087	IP tunnel MIB
RFC 4106	The use of Galois/Counter Mode (GCM) in IPSec ESP
RFC 4113	Management information base for the UDP
RFC 4191	Default router preferences and more-specific routes
RFC 4193	Unique local IPv6 unicast addresses
RFC 4213	Basic transition mechanisms for IPv6 hosts and routers
RFC 4271	A BGP-4
RFC 4283	Mobile node identifier option for Mobile IPv6 (MIPv6)
RFC 4291	IPv6 addressing architecture
RFC 4292	IP forwarding table MIB
RFC 4293	USM for the SNMPv3
RFC 4295	MIPv6 MIB
RFC 4301	Security architecture for the IP
RFC 4302	IP AH
RFC 4303	IP ESP
RFC 4308	Cryptographic suites for IPSec
RFC 4309	Using AES Cipher Block Chaining-Message Authentication Code (CCM) Mode with IPSec ESP
RFC 4338	Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) packets over fibre channel
RFC 4361	Node-specific client identifiers for Dynamic Host Configuration Protocol version 4 (DHCPv4)
RFC 4362	ROHC: A link-layer assisted profile for IP/UDP/RTP
RFC 4380	Teredo: Tunnelling IPv6 over UDP through Network Address Translations (NATs)
RFC 4434	The AES-XCBC-PRF-128 algorithm for the IKE
RFC 4443	Internet Control Message Protocol for IPv6 (ICMPv6) specification
RFC 4489	A method for generating link-scoped IPv6 multicast addresses
RFC 4543	The use of Galois Message Authentication Code (GMAC) in IPSec ESP and AH
RFC 4552	Authentication/Confidentiality for Open Shortest Path First version 3 (OSPFv3)
RFC 4581	CGA extension field format
RFC 4584	Extension to sockets API for MIPv6
RFC 4594	Configuration guidelines for DiffServ service classes

Table A.1. Request for Comment (RFC) list *(continued)*

RFC Number	Title
RFC 4604	Using Internet Group Management Protocol version 3 (IGMPv3) and MLDv2 for source-specific multicast
RFC 4607	Source-specific multicast for IP
RFC 4609	Protocol Independent Multicast - Sparse Mode (PIM-SM) multicast routing security issues and enhancements
RFC 4659	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 4760	Multiprotocol extensions for BGP-4
RFC 4798	Connecting IPv6 islands over IPv4 Multi-Protocol Label Switching (MPLS) using IPv6 Provider Edge (6PE) Routers
RFC 4807	IPSec security policy database configuration MIB
RFC 4809	Requirements for an IPSec certificate management profile
RFC 4815	ROHC: Corrections and clarifications to RFC 3095
RFC 4861	Neighbour discovery for IPv6
RFC 4862	IPv6 Stateless Address Autoconfiguration (SLAAC)
RFC 4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec
RFC 4877	MIPv6 operation with Internet Key Exchange version 2 (IKEv2) and the revised IPSec architecture
RFC 4884	Extended Internet Control Message Protocol (ICMP) to support multi-part messages
RFC 4890	Recommendations for filtering ICMPv6 messages in FW
RFC 4891	Using IPSec to secure IPv6-in-IPv4 tunnels
RFC 4941	Privacy extensions for stateless address autoconfiguration in IPv6
RFC 4944	Transmission of IPv6 packets over IEEE 802.15.4 networks
RFC 4945	The internet IPSec Public Key Infrastructure (PKI) profile of IKEv1/ Internet Security Association and Key Management Protocol (ISAKMP), IKEv2, and PKIX
RFC 4982	Support for multiple hash algorithms in CGAs
RFC 5014	IPv6 socket API for source address selection
RFC 5015	Bidirectional Protocol Independent Multicast (BIDIR-PIM)
RFC 5059	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
RFC 5072	IPv6 over PPP
RFC 5095	Deprecation of Type 0 routing headers in IPv6
RFC 5114	Additional Diffie-Hellman groups for use with IETF standards
RFC 5121	Transmission of IPv6 via the IPv6 convergence sublayer over IEEE 802.16 networks
RFC 5175	IPv6 router advertisement flags option
RFC 5187	OSPFv3 Graceful Restart
RFC 5213	Proxy MIPv6
RFC 5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 5329	OSPFv3 Graceful Restart
RFC 5340	Open Shortest Path First (OSPF) for IPv6

Table A.1. Request for Comment (RFC) list *(concluded)*

RFC Number	Title
RFC 5380	Hierarchical Mobile IPv6 (HMIPv6) mobility management
RFC 5555	MIPv6 support for dual stack hosts and routers
RFC 5569	IPv6 Rapid Deployment on IPv4 Infrastructures (6RD)
RFC 5701	IPv6 address specific BGP extended community attribute
RFC 5795	The ROHC framework
RFC 5838	Support of address families in OSPFv3
RFC 5844	IPv4 support for proxy MIPv6
RFC 5952	A recommendation for IPv6 address text representation
RFC 5969	6RD - Protocol specification
RFC 6040	Tunnelling of ECN
RFC 6052	IPv6 addressing of IPv4/IPv6 translators
RFC 6085	Address mapping of IPv6 multicast packets on ethernet
RFC 6146	Stateful NAT64: Network address and protocol translation from IPv6 clients to IPv4 servers
RFC 6275	Mobility support in IPv6
RFC 6333	Dual-Stack lite broadband deployments following IPv4 exhaustion
RFC 6379	Suite B cryptographic suites for IPSec
RFC 6724	Default address selection for IPv6
RFC 6846	ROHC: A profile for TCP/IP (ROHC-TCP)
RFC 6891	Extension mechanisms for DNS (EDNS0)
RFC 7296	IKEv2
RFC 7542	The network access identifier
RFC 7761	PIM-SM: Protocol specification (Revised)
RFC 7915	IP/ICMP translation algorithm
RFC 8200	IPv6 Specification
RFC 8201	Path MTU discovery for IPv6
RFC 8221	Cryptographic algorithm implementation requirements and usage guidance for ESP and AH
RFC 8247	Algorithm implementation requirements and usage guidance for the IKEv2

Annex B
(Informative)

Abbreviation

3GPP	3rd Generation Partnership Project
6PE	IPv6 Provider Edge
6RD	IPv6 Rapid Deployment on IPv4 Infrastructures
6VPE	IPv6 VPN Provider Edge Router
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
APFW	Application Firewall
API	Application Programming Interface
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol version 4
BIDIR-PIM	Bidirectional Protocol Independent Multicast
BRAS	Broadband Remote Access Server
BSR	Bootstrap Router
CBC	Cipher Block Chaining
CCM	Cipher Block Chaining-Message Authentication Code
CCTV	Closed Circuit Television
CGA	Cryptographically Generated Address
DHCP	Dynamic Host Configuration Protocol
DHCPv4	Dynamic Host Configuration Protocol version 4
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DS	Differentiated Services
ECN	Explicit Congestion Notification
EF	Expedite Forwarding
ESP	Encapsulating Security Payload
FDDI	Fibre Distributed Data Interface
FW	Firewall
GCM	Galois/Counter Mode
GGSN	Gateway GPRS Support Node
GMAC	Galois Message Authentication Code

GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
HMAC	Hash Message Authentication Code
HMIPv6	Hierarchical Mobile IPv6
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol for IPv6
IDS	Intrusion Detection System
IGMPv3	Internet Group Management Protocol version 3
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IS-IS	Intermediate System to Intermediate System
IoT	Internet of Things
IP	Internet Protocol
IPComp	IP Payload Compression Protocol
IPS	Intrusion Protection System
IPSec	IP Security
IPTV STB	IPTV Set Top Box
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IP PABX	Internet Protocol Public Automatic Branch Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
LB	Load Balancer
MAPOS	Multiple Access Protocol Over SONET/SDH
MIB	Management Information Base
MIP	Mobile Internet Protocol
MIPv6	Mobile IPv6
MLD	Multicast Listener Discovery
MLDv2	Multicast Listener Discovery version 2
MME	Mobility Management Entity
MODP	More Modular Exponential
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translations
NBMA	Non-Broadcast Multiple Access
NE	Network Element
NEMO	Network Mobility

NSE	Network Security Element
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSPFv3	Open Shortest Path First version 3
PC	Personal Computer
PHB	Per Hop Behaviour
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast - Sparse Mode
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
P-GW	Packet Data Network Gateway
RG	Residential Gateway
ROHC	RObust Header Compression
RP	Rendezvous Point
RTP	Real-Time Transport Protocol
SBC	Section Border Controller
SEND	SEcure Neighbour Discovery
SGSN	Serving GPRS Support Node
SLAAC	Stateless Address Autoconfiguration
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SSM	Single Source Multicast
S-GW	Serving Gateway
TCP	Transmission Control Protocol
TV	Television
UDP	User Datagram Protocol
UE	User Equipment
URI	Uniform Resource Identifier
USM	User-based Security Model
VPN	Virtual Private Network
WiFi	Wireless Fidelity

Annex C
(Normative)

IPv6 functions

Table C.1. Basic IPv6 functions

IETF Specification	IPv6 Basic Functions	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 8200	IPv6 specification	-	M	M	-	-	M	M	-	-	M	M	M
	IPv6 packets: send, receive	-	M	M	-	-	M	M	-	-	M	M	M
	IPv6 packet forwarding	-	-	M	-	-	-	M	-	-	-	M	M
	Extension headers: processing	-	M	M	-	-	M	M	-	-	M	M	M
	Hop-by-hop and unrecognised options	-	M	M	-	-	M	M	-	-	M	M	M
	Fragment headers: send, receive, process	-	M	M	-	-	M	M	-	-	M	M	M
	Destination options extensions	-	M	M	-	-	M	M	-	-	M	M	M
RFC 5095	Deprecation of Type 0 routing headers	Managed services	-	c(M)	-	-	M	M	-	-	M	M	M
RFC 2711	IPv6 router alert option	-	-	M	-	-	-	M	-	-	-	M	M
RFC 4443	ICMPv6	-	M	M	-	-	M	M	-	-	M	M	M
RFC 4884	Extended ICMP for multi-part messages	Managed services	-	c(M)	-	-	-	-	-	-	-	-	-
RFC 8201	Path MTU discovery for IPv6	-	M	M	-	-	M	M	-	-	M	M	M
	Discovery protocol requirements	-	M	M	-	-	M	M	-	-	M	M	M

Table C.1. Basic IPv6 functions *(continued)*

IETF Specification	IPv6 Basic Functions	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2675	IPv6 Jumbograms	-	O	O	-	-	-	-	-	-	-	-	-
RFC 4861	Neighbour discovery for IPv6	-	M	M	-	-	M	M	-	-	M	M	M
	Router discovery	-	M	M	-	-	M	M	-	-	M	M	M
	Prefix discovery	-	M	M	-	-	M	M	-	-	M	M	M
	Address resolution	-	M	M	-	-	M	M	-	-	M	M	M
	NA and NS processing	-	M	M	-	-	M	M	-	-	M	M	M
RFC 4862	Duplicate address detection	-	M	M	-	-	M	M	-	-	M	M	M
	Neighbour unreachability detection	-	M	M	-	-	M	M	-	-	M	M	M
	Redirect functionality	-	-	M	-	-	M	M	-	-	M	M	M
RFC 5175	IPv6 router advertisement flags option	-	M	M	-	-	-	-	-	-	-	-	-
RFC 4191	Default router preference	-	-	-	-	-	-	-	-	-	-	-	M
RFC 3971	Secure neighbour discovery	-	M	M	-	-	M	M	-	-	M	M	M
RFC 4862	IPv6 SLAAC	SLAAC	M	M	M	SLAAC	M	M	M	SLAAC	M	M	M
	Creation of link local addresses	SLAAC	M	M	-	SLAAC	M	M	-	SLAAC	M	M	M
RFC 4861	Duplicate address detection	SLAAC	M	M	-	SLAAC	M	M	-	SLAAC	M	M	M
	Creation of global addresses	SLAAC	M	M	-	SLAAC	M	M	-	SLAAC	M	M	M
	Ability to disable creation of global addrs	SLAAC	M	M	-	SLAAC	M	M	-	SLAAC	M	M	M

Table C.1. Basic IPv6 functions *(concluded)*

IETF Specification	IPv6 Basic Functions	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4941	Privacy extensions for IPv6 SLAAC	SLAAC	M	M	M	SLAAC	M	M	M	SLAAC	M	M	M
	2nd context for MIP mobile node	-	O	-	-	-	M	-	-	-	M	-	-
RFC 3736	Stateless DHCP service for IPv6	SLAAC	M	M	-	SLAAC	M	M	-	SLAAC	M	M	M
	DHCPv6	DHCP Client	M	-	-	DHCP Client	M	-	-	DHCP Client	M	-	-
	Ability to administratively disable	DHCP Client	M	-	-	DHCP Client	M	-	-	DHCP Client	M	-	-
	DHCP client functions	DHCP Client	M	-	-	DHCP Client	M	-	-	DHCP Client	M	-	-
RFC 4361	Node-specific client IDs for DHCPv4	DHCP Client	M	-	-	DHCP Client	M	-	-	DHCP Client	M	-	-
RFC 3633	Prefix delegation	DHCP Client	M	M	-	DHCP Client	M	M	-	DHCP Client	M	M	M

Table C.2. IPv6 addressing requirement

IETF Specification	IPv6 Addressing	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4291	IPv6 addressing architecture	-	M	M	-	-	M	M	-	-	M	M	-
RFC 4007	IPv6 scoped address architecture	-	M	M	-	-	M	M	-	-	M	M	-
	Ability to manually configure addresses	-	M	M	-	-	M	M	-	-	M	M	-
RFC 4193	Unique local IPv6 unicast address	-	O	O	-	-	O	O	-	-	O	O	-
RFC 3879	Deprecating site local addresses	-	M	M	-	-	M	M	-	-	M	M	-
RFC 6724	Default address selection for IPv6	-	M	M	-	-	M	M	-	-	M	M	-
	Configurable selection policies	-	M	M	-	-	M	M	-	-	M	M	-
RFC 2526	Reserved IPv6 subnet anycast addresses	-	O	O	-	-	O	O	-	-	O	O	-
RFC 3972	CGA	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-
RFC 4581	CGA extension field format	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-
RFC 4982	CGA support for multiple hash algos	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-
RFC 5952	A recommendation for IPv6 address text	-	O	O	-	-	O	O	-	-	O	O	-
RFC 6052	IPv6 addressing of IPv4/IPv6 translators	-	O	O	-	-	O	O	-	-	O	O	-
RFC 6085	Address mapping of IPv6 multicast packets on ethernet	-	O	O	-	-	O	O	-	-	O	O	-

NOTE. Condition is referred when VPN or other encryption protocol (e.g SEND) initiate from the specific devices is required. For protection devices such as firewall. It should able to work with CGA

Table C.3. Transition mechanism requirements

IETF Specification	Transition Mechanism	Mass Network				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4038	Application aspects of IPv6 transition	-	M	M	M	-	M	M	M	-	M	M	M
RFC 4213	Basic transition mechanisms for IPv6 hosts and routers	IPv4	M	M	-	IPv4	M	M	-	IPv4	M	M	-
RFC 4798	Connecting IPv6 islands over IPv4 MPLS using 6PE Routers	-	-	-	-	IPv4, MPLS	-	M	-	IPv4, MPLS	-	M	-
RFC 4659	IPv6 VPN Provider Edge Router (6VPE)	-	-	-	-	IPv4, MPLS	-	M	-	IPv4, MPLS	-	M	-
RFC 3056	6to4	IPv4	-	M	-	IPv4	-	M	-	IPv4	-	M	-
RFC 4380	Teredo	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5214	ISATAP describes an automatic tunnelling technique for dual stack nodes which uses IPv4 network as link layer	-	-	-	-	-	-	-	-	-	-	-	-
RFC 6146	NAT64	IPv4	-	M	M	IPv4	-	M	M	IPv4	-	M	M
RFC 6333	Dual Stack Lite	-	-	-	-	-	-	-	-	-	-	-	-
RFC 7915	IP/ICMP Translation Algorithm	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5569	6RD	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5969	6RD with PD	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2784	GRE	-	-	O	-	-	-	O	-	-	-	O	-

Table C.4. Link specific requirements

IETF Specification	Link Specific	Mass Network				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2464	IPv6 over ethernet	Condition	M	M	M	-	M	M	M	-	M	M	M
RFC 2467	IPv6 over FDDI	-	M	M	M	-	M	M	M	-	M	M	M
RFC 2491	IPv6 over NBMA network	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3146	IPv6 over IEEE 1394 Networks	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3572	IPv6 over MAPOS (SONET/SDH)	-	M	M	M	-	M	M	M	-	M	M	M
RFC 4338	IPv6 IPv4 and ARP packets over fibre channel	-	M	M	M	-	M	M	M	-	M	M	M
RFC 4944	IPv6 over IEEE 802.15.4 Networks	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5072	IPv6 over PPP	-	M	M	M	-	M	M	M	-	M	M	M
RFC 5121	Transmission of IPv6 via the IPv6 convergence sublayer over IEEE 802.16 networks	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2507	IP header compression	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2508	Compressing IP/UDP/RTP Headers for low- speed serial links	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3173	IPComp	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5795	ROHC framework	-	-	-	-	-	-	-	-	-	-	-	-
RFC 6846	ROHC Profile for TCP	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3095	ROHC Profile for RTP, UDP, ESP and Uncomp	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4815	Connections and Clarifications to RFC3095	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3843	ROHC Profile for IP Only	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3241	ROHC over PPP	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4362	ROHC link assisted for IP/UDP/RTP	-	-	-	-	-	-	-	-	-	-	-	-
NOTE. Condition is applicable when the specified link technology is chosen as preferred choice													

Table C.5. Routing protocol

IETF Specification	Routing Protocol	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 5340	OSPF for IPv6	-	-	-	-	Condition	-	M	M	Condition	-	M	M
RFC 4552	Authentication/confidentiality for OSPFv3	-	-	-	-	Condition	-	M	-	Condition	-	M	-
RFC 1195	Use of OSI IS - IS for routing in TCP/IP and dual environments	-	-	-	-	-	-	-	-	Condition	-	M	-
RFC 5187	OSPFv3 graceful restart	-	-	-	-	-	-	-	-	-	-	M	-
RFC 5329	Traffic engineering extensions to OSPFv3	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5838	Support of address families in OSPFv3	-	-	-	-	-	-	-	-	-	-	-	-
	RIPng protocol applicability statement	-	-	-	-	Condition	-	c(M)	-	Condition	-	M	-
RFC 4271	BGP-4	-	-	-	-	Condition	-	c(M)	-	Condition	-	M	-
RFC 1772	BGP application in the Internet	-	-	-	-	Condition	-	M	-	Condition	-	M	-
RFC 4760	BGP multi-protocol extensions	-	-	-	-	Condition	-	M	-	Condition	-	M	-
RFC 2545	BGP multi-protocol extensions for IPv6 IDR	-	-	-	-	Condition	-	M	-	Condition	-	M	-
RRC 4659	BGP MPLS IP VPN extension for IPv6 VPN	-	-	-	-	-	-	-	-	-	-	M	-
RFC 5701	IPv6 address specific BGP extended community attribute	-	-	-	-	-	-	-	-	-	-	-	-
NOTE. Condition for the Interior Gateway Protocol (IGP) and hardware FW													

Table C.6. Multicast

IETF Specification	Multicast	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2710	MLD for IPv6	Condition	M	M	-	Condition	M	M	-	Condition	M	M	-
RFC 3590	Source address selection for the MLD protocol	Condition	M	M	-	Condition	M	M	-	Condition	M	M	-
RFC 3810	MLD version 2 for IPv6	PIM-SSM	M	M	-	PIM-SSM	M	M	-	PIM-SSM	M	M	-
RFC 3306	Unicast-prefix-based IPv6 multicast address	-	M	M	-	-	M	M	-	-	-	-	-
RFC 3307	Allocation guidelines for IPv6 multicast addrs	-	M	M	-	-	M	M	-	-	M	M	-
RFC 4607	Source-specific multicast for IP	PIM-SSM	M	M	-	PIM-SSM	M	M	-	PIM-SSM	M	M	-
RFC 4604	MLDv2 for source specific multicast	PIM-SSM	M	M	-	PIM-SSM	M	M	-	PIM-SSM	M	M	-
RFC 7761	PIM-SM	PIM-SSM	-	M	-	PIM-SSM	-	M	-	PIM-SSM	-	M	-
RFC 4609	PIM-SM security issues / enhancements	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3956	Embedding RP multicast addr	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4489	A method for generating link-scoped IPv6 multicast address	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5059	BSR mechanism for PIM	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5015	BIDIR-PIM	-	-	-	-	-	-	-	-	-	-	-	-
NOTE. Condition when group management capability is required - IGMP													

Table C.7. Network management

IETF Specification	Network Management	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
Network Management Requirements													
RFC 3411	SNMPv3 management framework	Managed services	-	-	-	SNMP	M	M	M	SNMP	M	M	M
RFC 3412	SNMP message process and dispatch	-	-	-	-	SNMP	M	M	M	SNMP	M	M	M
RFC 3413	SNMP applications	Managed services	-	-	-	SNMP	M	M	M	SNMP	M	M	M
	Command responder	-	-	-	-	SNMP	M	M	M	SNMP	M	M	M
	Notification generator	-	-	-	-	SNMP	-	M	-	SNMP	M	M	-
RFC 3414	User-based security model for SNMPv3	-	-	-	-	SNMP	M	M	-	SNMP	M	M	-
Management Information Bases													
RFC 4293	MIB for the IP	-	-	-	-	SNMP	M	M	-	SNMP	M	M	-
RFC 4292	MIB for the IP forwarding table	-	-	-	-	SNMP		M	-	SNMP	-	M	-
RFC 4022	MIB for TCP	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4113	MIB for UDP	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4087	MIB for IP tunnels	-	-	-	-	SNMP & IPv4	-	M	-	SNMP & IPv4	-	M	-
RFC 4807	MIB or IPSec policy database configuration	-	-	-	-	SNMP & IPSecv3	-	M	-	SNMP & IPSecv3	-	M	-
RFC 4295	MIB for MIPv6	-	-	-	-	SNMP & MIP	-	M	-	SNMP & MIP	-	M	-
RFC 3289	MIB for DiffServ	-	-	-	-	SNMP & DS	-	M	-	SNMP & DS	-	M	-

Table C.8. Application

IETF Specification	Application	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 3596	DNS extensions for IPv6	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M
RFC 6891	Extension mechanisms for DNS (EDNS0)	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M
RFC 3226	DNSSEC and IPv6 DNS MSG Size Reqs	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M
RFC 3986	URI: generic syntax	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M
RFC 3493	Basic socket API for IPv6	Condition	M	-	-	Condition	M	-	-	Condition	M	-	-
RFC 3542	Advanced socket API for IPv6	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4584	Extension to sockets API for MIPv6	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3678	Socket API extensions multicast source filters	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5014	Socket API for source address selection	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3315	DHCPv6 functions (If host supports DHCP, it should also support DHCPv6)	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M

NOTES:

1. Condition for the RFC 3596 and RFC 6891 is when the device supports DNS.
2. Condition for the RFC 3226 is when the device supports DNSSEC.
3. Condition for the RFC 3986 is when the device supports URIs.
4. Condition for the RFC 3493 is when the device has exposed to APIs.
5. Condition for the RFC 3315 is when the device supports DHCP.

Table C.9. Mobility

IETF Specification	Mobility	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 6275	Mobility support in IPv6	MIPv6	M	M	-	MIPv6	M	M	-	MIPv6	M	M	-
RFC 3963	NEMO basic support in IPv6	NEMO	-	M	-	NEMO	-	M	-	NEMO	-	M	-
RFC 7542	The network access identifier	PMIPv6	-	M	-	PMIPv6	-	M	-	PMIPv6	-	M	-
RFC 4283	Mobile node identifier option for MIPV6	PMIPv6	-	M	-	PMIPv6	-	M	-	PMIPv6	-	M	-
RFC 4877	MIPv6 Op with IKEv2 and revised IPs architecture	e MIPv6	M	M	-	MIPv6	M	M	-	MIPv6	M	M	-
RFC 5213	Proxy MIPv6	PMIPv6		M	-	PMIPv6	-	M	-	PMIPv6	-	M	-
RFC 5380	Hierarchical MIPv6 scheme	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5555	MIPv6 support for dual stack hosts and routers	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5844	IPv4 support for proxy mobile IPv6	-	-	-	-	-	-	-	-	-	-	-	-

Table C.10. Quality of service

IETF Specification	Quality of Service	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2474 (PS)	DiffServ Header Field	Condition	M	M	-	DS	M	M	-	DS	M	M	-
RFC 3140 (PS)	PHB Encoding – DiffServ	Condition	M	M	-	DS	M	M	-	DS	M	M	-
RFC 3168 (PS)	Explicit congestion notification, ECN	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2597 (PS)	Assured forwarding	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3246 (PS)	Expedited forwarding	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3247 (INF)	Supplementary EF PHB	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2475 (INF)	DiffServ architecture	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3260 (INF)	New term and clarification - DiffServ	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2983 (INF)	DiffServ and tunnels	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4594 (INF)	Config guidelines DiffServ	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3086 (INF)	DiffServ per domain behaviour	-	-	-	-	-	-	-	-	-	-	-	-

NOTES:

1. Condition is DS and managed service.
2. PS - Proposed Standard
3. INF - Information

Table C.11. IPv6 Security

IETF Specification	IPv6 Security	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2451	ESP CBC mode algorithms	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3602	AES-CBC	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3686	AES-CTR	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4309	AES-CCM	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4106	AES-GCM	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4543	AES-GMAC	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2404	HMAC-SHA-1-96	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4868	HMAC-SHA-256	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3566	AES-XCBC-MAC-96	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4434	AES-XCBC-PRF-128	-	-	-	-	-	-	-	-	-	-	-	-
RFC 8247	Algorithm implementation requirements and usage guidance for the IKEv2	-	M	M	M	-	M	M	M	-	M	M	M
Transition Mechanisms Requirements													
RFC 4213	Transition mechanise for hosts and routers	-	M	M	-	-	M	M	-	-	M	M	-
RFC 4891	Using IPsec to secure IPv6-in IPv4 tunnels	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-
RFC 2473	Generic packet tunnelling in IPv6	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-
RFC 4798	Connecting IPv6 islands over IPv4 MPLS 6PE	MPLS	M	M	-	MPLS	M	M	-	MPLS	M	M	-
ICMP													
RFC 4890	Recommendations for filtering ICMPv6 messages in FW	-	-	-	M	-	-	-	M	-	-	-	M

Table C.11. IPv6 Security *(continued)*

IETF Specification	IPv6 Security	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
IPSec-v3													
RFC 4301/ RFC 6040	Security architecture for the IP/ tunnelling of explicit congestion notification	-	M	-	-	-	-	-	-	-	-	-	-
RFC 4303	ESP	-	M	-	-	-	-	-	-	-	-	-	-
RFC 4302	AH	-	M	-	-	-	-	-	-	-	-	-	-
RFC 3948	UDP encapsulation of ESP packets	-	-	-	-	-	-	-	-	-	-	-	-
RFC 8221	Cryptographic algorithms for ESP and AH	-	M	-	-	-	-	-	-	-	-	-	-
RFC 4308	Cryptographic suites for IPSec	-	-	-	-	-	-	-	-	-	-	-	-
RFC 6379	Suite B cryptographic suites for IPSec	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4809	Requirements for an IPSec cert management profile	-	-	-	-	-	-	-	-	-	-	-	-
IKEv2													
RFC 7296	IKEv2 protocol	-	M	M	M	-	M	M	M	-	M	M	M
RFC 8247	Algorithm implementation requirements and usage guidance for the IKEv2	-	M	M	M	-	M	M	M	-	M	M	M
RFC 3526	More MODP DH groups for IKE	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5114	Additional DH groups for use with IETF Stds	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4945	Internet IPsec PKI Profile of IKEv1, IKEv2 & PKIX	-	-	-	-	-	-	-	-	-	-	-	-

Table C.11. IPv6 Security *(concluded)*

IETF Specification	IPv6 Security	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
Uses of Cryptographic Algorithms													
RFC 2410	NULL encryption	-	M	M	M	-	M	M	M	-	M	M	M
RFC 8221	Cryptographic algorithms for ESP and AH	-	M	M	M	-	M	M	M	-	M	M	M
NOTE. Condition is tunnelling transition.													

Table C.12. Network Security Equipment

NIST SP500- 267	Network Security	Mesh				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
6.12.3.1	IPv6 connectivity	-	-	-	M	-	-	-	M	-	-	-	M
6.12.3.2	Dual stack	-	-	-	M	-	-	-	M	-	-	-	M
6.12.3.3	Administrative functionality	-	-	-	M	-	-	-	M	-	-	-	M
6.12.3.4	Authentication and authorisation	-	-	-	M	-	-	-	M	-	-	-	M
6.12.3.5	Security of control and communications	-	-	-	-	-	-	-	M	-	-	-	M
6.12.3.6	Persistence	-	-	-	M	-	-	-	M	-	-	-	M
6.12.3.7	Logging and alerts	-	-	-	M	-	-	-	M	-	-	-	M
6.12.3.8	Fragmented packet handling	-	-	-	M	-	-	-	M	-	-	-	M
6.12.3.9	Tunnelled traffic handling	-	-	-	M	-	-	-	M	-	-	-	M
6.12.4.1.1	Port/protocol/address blocking	FW or APFW	-	-	M	FW or APFW	-	-	M	FW or APFW	-	-	M
6.12.4.1.2	Asymmetrical blocking	FW or APFW	-	-	M	FW or APFW	-	-	M	FW or APFW	-	-	M
6.12.4.1.3	IPSec traffic handling	FW or APFW	-	-	-	FW or APFW	-	-	M	FW or APFW	-	-	M
6.12.4.1.4	Performance under load, fail-safe	FW or APFW	-	-	M	FW or APFW	-	-	M	FW or APFW	-	-	M
6.12.4.2.1	No violation of trust barriers	APFW	-	-	M	APFW	-	-	M	APFW	-	-	M
6.12.4.2.2	Session traffic Auth	APFW	-	-	M	APFW	-	-	M	APFW	-	-	M
6.12.4.2.3	Email, file filtering	APFW	-	-	M	APFW	-	-	M	APFW	-	-	M
6.12.5.1.1	Known attack detection	IDS or IPS	-	-	M	IDS or IPS	-	-	M	IDS or IPS	-	-	M
6.12.5.1.2	Malformed packets detection	IDS or IPS	-	-	M	IDS or IPS	-	-	M	IDS or IPS	-	-	M

Table C.12. Network Security Equipment *(continued)*

NIST SP500- 267	Network Security	Mesh				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
6.12.5.1.3	Port scan detection	IDS or IPS	-	-	M	IDS or IPS	-	-	M	IDS or IPS	-	-	M
6.12.5.1.4	Tunnelled traffic detection	IDS or IPS	-	-	O	IDS or IPS	-	-	M	IDS or IPS	-	-	M
6.12.5.1.5	Logging and alerts	IDS or IPS	-	-	M	IDS or IPS	-	-	M	IDS or IPS	-	-	M
6.12.5.1.6	Performance under load, fail-safe	IDS or IPS	-	-	M	IDS or IPS	-	-	M	IDS or IPS	-	-	M
6.12.5.2.1	Intrusion prevention	IPS	-	-	M	IPS	-	-	M	IPS	-	-	M

Annex D
(Normative)

IPv6 compliance requirement

Table D.1. Section 1 - RFC 8200 IPv6 Specification

IETF	Test Case	Consumer			Enterprise/Service Provider		
		Host	NE	NSE	Host	NE	NSE
Group 1: IPv6 Header	v6LC.1.1.1: Version field	M	M	M	M	M	M
	v6LC.1.1.2: Traffic class non-zero - end node	M	M	M	M	M	M
	v6LC.1.1.3: Traffic class non-zero - intermediate node (routers only)	-	M	M	-	M	M
	v6LC.1.1.4: Flow label non-zero	M	M	M	M	M	M
	v6LC.1.1.5: Payload length	M	M	M	M	M	M
	v6LC.1.1.6: No next header after IPv6 header	M	M	M	M	M	M
	v6LC.1.1.7: Unrecognised next header	M	M	M	M	M	M
	v6LC.1.1.8: Hop limit zero - end node	M	M	M	M	M	M
	v6LC.1.1.9: Hop limit decrement - intermediate node (routers only)	-	M	M	-	M	M
	v6LC.1.1.10: IP Forwarding - source and destination address - intermediate node (routers only)	-	M	M	-	M	M

Table D.1. Section 1 - RFC 8200 IPv6 Specification *(continued)*

RFC 8200	Test Case	Consumer			Enterprise/Service Provider		
		Host	NE	NSE	Host	NE	NSE
Group 2: Extension Headers and Options	v6LC.1.2.1: Next header zero	M	M	M	M	M	M
	v6LC.1.2.2: No next header after extension header	M	M	M	M	M	M
	v6LC.1.2.3: Unrecognised next header in extension header - end node	M	M	M	M	M	M
	v6LC.1.2.4: Extension header processing order	M	M	M	M	M	M
	v6LC.1.2.5: Option processing order	M	M	M	M	M	M
	v6LC.1.2.6: Options processing, hop-by-hop options header - end node	M	M	M	M	M	M
	v6LC.1.2.7: Options processing, hop-by-hop options header - intermediate node (routers only)	-	M	M	-	M	M
	v6LC.1.2.8: Option processing, destination options header	M	M	M	M	M	M
	v6LC.1.2.9: Unrecognised routing type - end node	M	M	M	M	M	M
	v6LC.1.2.10: Unrecognised routing type - intermediate node	M	M	M	M	M	M
Group 3: Fragmentation	v6LC.1.3.1: Fragment reassembly	M	M	M	M	M	M
	v6LC.1.3.2: Reassembly time exceeded	M	M	M	M	M	M
	v6LC.1.3.3: Fragment header M-bit set, payload length invalid	M	M	M	M	M	M
	v6LC.1.3.4: Stub fragment header	M	M	M	M	M	M

Table D.2. Section 2 - RFC 4861 Neighbour Discovery for IPv6

RFC 4861	Test Case	Consumer			Enterprise/Service Provider		
		Host	NE	NSE	Host	NE	NSE
Group 1: Address Resolution and Neighbour Unreachability Detection	Test v6LC.2.1.1: On-link determination	-	-	-	-	M	-
	Test v6LC.2.1.2: Resolution wait queue	-	-	-	-	M	-
	Test v6LC.2.1.3: Prefix information option processing, on-link flag (hosts only)	-	-	-	M	-	-
	Test v6LC.2.1.4: Host prefix list (hosts only)	-	-	-	M	-	-
	Test v6LC.2.1.5: Neighbour solicitation origination, address resolution	-	-	-	-	M	-
	Test v6LC.2.1.6: Neighbour solicitation origination, reachability confirmation	-	-	-	-	M	-
	Test v6LC.2.1.7: Invalid neighbour solicitation handling	-	-	-	-	M	-
	Test v6LC.2.1.8: Neighbour solicitation processing, no NCE	-	-	-	-	M	-
	Test v6LC.2.1.9: Neighbour solicitation processing, NCE state INCOMPLETE	-	-	-	-	M	-
	Test v6LC.2.1.10: Neighbour solicitation processing, NCE state REACHABLE	-	-	-	-	M	-
	Test v6LC.2.1.11: Neighbour solicitation processing, NCE state STALE	-	-	-	-	M	-
	Test v6LC.2.1.12 Neighbour solicitation processing, NCE state PROBE	-	-	-	-	M	-
	Test v6LC.2.1.13: Neighbour solicitation processing, IsRouterFlag (host only)	-	-	-	-	-	O
	Test v6LC.2.1.14: Neighbour solicitation processing, anycast (routers only)	-	-	-	-	M	O
	Test v6LC.2.1.15: Invalid neighbour advertisement handling	-	-	-	-	-	-
	Test v6LC.2.1.16: Neighbour advertisement processing, no NCE	-	-	-	-	-	-
	Test v6LC.2.1.17: Neighbour advertisement processing, NCE state INCOMPLETE	-	-	-	-	-	-
	Test v6LC.2.1.18: Neighbour advertisement processing, NCE state REACHABLE	-	-	-	-	-	-
	Test v6LC.2.1.19: Neighbour advertisement processing, NCE state STALE	-	-	-	-	-	-

Table D.2. Section 2 - RFC 4861 Neighbour Discovery for IPv6 *(continued)*

RFC 4861	Test Case	Consumer			Enterprise/Service Provider		
		Host	NE	NSE	Host	NE	NSE
Group 1: Address Resolution and Neighbour Unreachability Detection	Test v6LC.2.1.20: Neighbour advertisement processing, NCE state PROBE	-	-	-	-	-	-
	Test v6LC.2.1.21: Neighbour advertisement processing, R-bit change (hosts only)	-	-	-	-	O	O
Group 2: Router and Prefix Discovery	Test v6LC.2.2.1: Router solicitations (hosts only)	-	-	-	-	O	O
	Test v6LC.2.2.2: Router solicitations, solicited router advertisement (hosts only)	-	-	-	-	O	O
	Test v6LC.2.2.3: Host ignores router solicitations (hosts only)	-	-	-	-	O	O
	Test v6LC.2.2.4: Router ignores invalid router solicitations (routers only)	-	-	-	M	M	O
	Test v6LC.2.2.5: Router sends valid router advertisement (routers only)	-	-	-	M	M	O
	Test v6LC.2.2.6: Router does not send router advertisements on non-advertising interface (routers only)	-	-	-	M	M	O
	Test v6LC.2.2.7: Sending unsolicited router advertisements (routers only)	-	-	-	M	M	O
	Test v6LC.2.2.8: Ceasing to be an advertising interface (routers only)	-	-	-	M	M	O
	Test v6LC.2.2.9: Processing router solicitations (routers only)	-	-	-	M	M	O
	Test v6LC.2.2.10: Router solicitation processing, neighbour cache (routers only)	-	-	-	M	M	O
	Test v6LC.2.2.11: Default router switch (hosts only)	-	-	-	M	O	O
	Test v6LC.2.2.12: Router advertisement processing, validity (hosts only)	-	-	-	M	O	O
	Test v6LC.2.2.13: Router advertisement processing, cur hop limit	-	-	-	M	M	O
	Test v6LC.2.2.14: Router advertisement processing, router lifetime (hosts only)	-	-	-	M	O	O
	Test v6LC.2.2.15: Router advertisement processing, reachable time	-	-	-	M	O	O

Table D.2. Section 2 - RFC 4861 Neighbour Discovery for IPv6 *(continued)*

RFC 4861	Test Case	Consumer			Enterprise/Service Provider		
		Host	NE	NSE	Host	NE	NSE
Group 2: Router and Prefix Discovery	Test v6LC.2.2.16: Router advertisement processing neighbour cache (hosts only)	-	-	-	M	O	O
	Test v6LC.2.2.17: Router advertisement processing, IsRouter flag (hosts only)	-	-	-	M	O	O
	Test v6LC.2.2.18: Router advertisement processing, reachable time	-	-	-	M	O	O
	Test v6LC.2.2.19: Router advertisement processing, on-link determination (hosts only)	-	-	-	M	O	O
Group 3: Redirect Function	Test v6LC.2.3.1: Redirected on-link: valid (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.2: Redirected on-link: suspicious (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.3: Redirected on-link: invalid (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.4: Redirected to alternate router: valid (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.5: Redirected to alternate router: suspicious (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.6: Redirected to alternate router: invalid (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.7: Redirected twice (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.8: Invalid option (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.9: No destination cache entry (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.10: Neighbour cache updated, no neighbour cache entry (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.11: Neighbour cache updated from state INCOMPLETE (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.12: Neighbour cache updated from state REACHABLE (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.13: Neighbour cache updated from state STALE (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.14: Neighbour cache updated from state PROBE (hosts only)	-	-	-	M	O	O

Table D.2. Section 2 - RFC 4861 Neighbour Discovery for IPv6 *(concluded)*

RFC 4861	Test Case	Consumer			Enterprise/Service Provider		
		Host	NE	NSE	Host	NE	NSE
Group 3: Redirect Function	Test v6LC.2.3.15: Invalid redirect does not update neighbour cache (hosts only)	-	-	-	M	O	O
	Test v6LC.2.3.16: Redirect - transmit (routers only)	-	-	-	M	M	O
	Test v6LC.2.3.17: Redirect - receive (routers only)	-	-	-	M	M	O

Table D.3. Section 3 - RFC 4862 IPv6 Stateless Address Autoconfiguration

RFC 4862	Test Case	Consumer			Enterprise/Service Provider		
		Host	NE	NSE	Host	NE	NSE
Group 1: Address Autoconfigu-ration and Duplicate Address Detection	Test v6LC.3.1.1: Address autoconfiguration and test	-	-	-	M	M	M
	Test v6LC.3.1.2: Receiving DAD neighbour solicitations and advertisements	-	-	-	M	M	M
	Test v6LC.3.1.3: Validation of DAD neighbour solicitations	-	-	-	M	M	M
	Test v6LC.3.1.4: Validation of DAD neighbour advertisements	-	-	-	M	M	M
	Test v6LC.3.1.5: Receiving neighbour solicitations for address resolution	-	-	-	M	M	M
Group 2: Router Advertisement Processing and Address Lifetime	Test v6LC.3.2.1: Global address autoconfiguration and DAD	-	-	-	M	O	O
	Test v6LC.3.2.2: Address lifetime expiry (hosts only)	-	-	-	M	O	O
	Test v6LC.3.2.3: Multiple prefixes and network renumbering (hosts only)	-	-	-	M	O	O
	Test v6LC.3.2.4: Prefix-information option processing (hosts only)	-	-	-	M	O	O
	Test v6LC.3.2.5: Prefix-information option processing, lifetime (hosts only)	-	-	-	M	O	O

Table D.4. Section 4 - RFC 1981 Path Maximum Transmission Unit (MTU) Discovery for IPv6

Test Case	Consumer			Enterprise/Service Provider		
	Host	NE	NSE	Host	NE	NSE
Test v6LC.4.1.1: Confirm Ping	-	-	-	M	M	M
Test v6LC.4.1.2: Stored PMTU	-	-	-	M	M	M
Test v6LC.4.1.3: Non-zero ICMPv6 code	-	-	-	M	M	M
Test v6LC.4.1.4: Reduce PMTU on-link	-	-	-	M	M	M
Test v6LC.4.1.5: Reduce PMTU off-link	-	-	-	M	M	M
Test v6LC.4.1.6: Receiving MTU below IPv6 minimum link MTU	-	-	-	M	M	M
Test v6LC.4.1.7: Increase estimate	-	-	-	M	M	M
Test v6LC.4.1.8: Router advertisement with MTU option (hosts only)	-	-	-	M	M	M
Test v6LC.4.1.9: Checking for increase in PMTU	-	-	-	M	M	M
Test v6LC.4.1.10: Multicast destination - one router	-	-	-	M	M	M
Test v6LC.4.1.11: Multicast destination - two routers	-	-	-	M	M	M

Table D.5. Section 5 - RFC 4443 Internet Control Message Protocol (ICMPv6)

Test Case	Consumer			Enterprise/Service Provider		
	Host	NE	NSE	Host	NE	NSE
Test v6LC.5.1.1: Transmitting echo requests	-	-	-	M	M	M
Test v6LC.5.1.2: Replying echo requests	-	-	-	M	M	M
Test v6LC.5.1.3: Destination unreachable message generation	-	-	-	M	M	M
Test v6LC.5.1.4: Packet too big message generation (routers only)	-	-	-	M	M	M
Test v6LC.5.1.5: Hop limit exceeded (time exceeded generation) (routers only)	-	-	-	M	M	M
Test v6LC.5.1.6: Erroneous header field (parameter problem generation)	-	-	-	M	M	M
Test v6LC.5.1.7: Unrecognised next header (parameter problem generation)	-	-	-	M	M	M
Test v6LC.5.1.8: Unknown informational message type	-	-	-	M	M	M
Test v6LC.5.1.9: Error condition with ICMPv6 error message (routers only)	-	-	-	M	M	M
Test v6LC.5.1.10: Error condition with multicast destination	-	-	-	M	M	M
Test v6LC.5.1.11: Error condition with non-unique source - unspecified	-	-	-	M	M	M
Test v6LC.5.1.12: Error condition with non-unique source - multicast	-	-	-	M	M	M
Test v6LC.5.1.13: Error condition with non-unique source - anycast	-	-	-	M	M	M

Annex E
(Informative)

Sample of test report format

IPv6 Conformance Test Report

Evaluation Details			
Device Model		Firmware ver.	
Model Series	*(Optional)*	Device Chassis	*(Optional)*
Tested By			
Checked By			

Evaluation Result Summary			
Section 1, Group	**Test Category**	**Result**	**Remarks**
1.0	IPv6 Header	*(Not tested)*	
2.0	Extension Headers and Options	*(Not tested)*	
3.0	Fragmentation	*(Not tested)*	

Test Approved by	Stamp and Date	Signature
(Name/Company/Title)		

Bibliography

[1] *Singapore Internet Protocol version 6 (IPv6) Profile* - IDA RS IPv6 Issue 1Rev 2, Jan 2012 USG V6

[2] *3rd Generation Partnership Project (3GPP) standard*

[3] Network Computing
https://www.networkcomputing.com/networking/white-box-switches-are-you-ready/1465296666

[4] SDxCentral
https://www.sdxcentral.com/cloud-converged-datacenter-whitebox-definitions-what-is-white-box-networking/

[5] TechTarget
https://searchsdn.techtarget.com/definition/white-box-switch

[6] Transport Information Service
http://www.tis-gdv.de/tis_e/ware/maschinen/haushalt/haushaltsgeraete.htm

Acknowledgement

Ms Azura Mat Salim (Chairman)	Telekom Malaysia Berhad
Mr Yan Kim Fui (Vice Chairman)	Cisco Systems Malaysia
Ms Norkhadhra Nawawi (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Lewis Walmesley-Browne	American Malaysian Chamber of Commerce
Mr Eng Wee Chun	Apple Inc.
Mr Hanaffy Geoffrey Ramli	Digi Telecommunication Sdn Bhd
Mr Chew Kian Kheong/ Mr Isaac Chan/ Mr Salim Mohamad Ghani	Hewlett Packard Enterprise
Mr Adil Hidayat Rosli	My6 Initiative Berhad
Mr T. Vemalrajah	Panasonic AVC Networks
Dr Dzaharudin Mansor	Persatuan Industri Komputer dan Multimedia Malaysia
Mr Ahmad Faizan Pardi/ Mr Wan Mohd Iidil/ Ms Khairunnisa Ab. Halim	SIRIM Berhad
Dr Leon Mun Wai	Sony EMCS (M) Sdn Bhd
Mr Arief Khalid	Telekom Malaysia Berhad
Mr Rosli Abdullah	webe digital sdn bhd