TECHNICAL CODE

INTERNET PROTOCOL VERSION 6 (IPv6) – EQUIPMENT COMPLIANCE (SECOND REVISION)

DRAFT FOR PUBLIC COMMENT

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

© Copyright 2026

MCMC MTSFB TC TXXX:2026

Development of technical codes

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) ('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 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 HQ Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8688 8000
Fax : +60 3 8688 1000
Email : stpd@mcmc.gov.my
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my

DRAFT FOR PUBLIC COMMENT

Contents

Page

Committee representation ii
Foreword iii

1. Scope 1
2. Normative references 1
3. Abbreviations 1
4. Terms and definitions 2
6. Equipment categories 3
7. Segments 5
8. Functional requirements 6
9. IPv6 compliance requirement 7
10. Sample test report 8

Annex A Abbreviations 9
Annex B Category of equipment 12
Annex C Network connectivity equipment 14
Annex D IPv6 functions 15
Annex E Request for Comments (RFC) 34
Annex F IPv6 compliance requirement 38
Annex G Sample of test report format 43
Bibliography 44

DRAFT FOR PUBLIC COMMENT

Committee representation

This technical code was developed by Numbering and Electronic Addressing Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

CelcomDigi Telecommunications Sdn Bhd

IPv6 Forum Malaysia

Maxis Broadband Sdn Bhd

Multimedia University

SIRIM Berhad

TIME dotCom Sdn Bhd

TM Technology Services Sdn Bhd

DRAFT FOR PUBLIC COMMENT

Foreword

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

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) revision of normative references to reflect the latest applicable standards and remove references that are no longer relevant;

b) exclusion of power supply, cord, main plugs, electromagnetic compatibility, electrical safety, marking and language requirements, which are addressed in the MCMC MTSFB TC T022, *Communications Equipment - Baseline Requirements*;

c) removal and additional of the terms and definitions used throughout this Technical Code;

d) review and update of the Request for Comments (RFC) references, including replacement of obsolete deprecated RFCs with current specifications;

e) enhancement of the figure to differentiate the network connectivity to public and private networks;

f) refinement of equipment categories to provide non-exhaustive examples of equipment subject to this Technical Code;

g) enhancement of the core IPv6 compliance requirements to align with current industry practices, deployment scenarios, and certification needs; and

h) adoption of the latest IPv6 ready test plans and related conformance specifications as references for IPv6 compliance requirements.

This Technical Code cancels and replaces the MCMC MTSFB TC T013:2019, *Internet Protocol version 6 (IPv6) - Compliant Equipment (First Revision).*

This Technical Code shall continue to be valid and effective until it is replaced or revoked.

DRAFT FOR PUBLIC COMMENT

INTERNET PROTOCOL VERSION 6 (IPv6) – EQUIPMENT COMPLIANCE

1. Scope

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

This Technical Code specifies requirements for equipment with direct internet-facing functionality to remain operational in a native IPv6-only environment, including access to Internet Protocol version 4 (IPv4)-only applications or services through appropriate IPv4 service-continuity mechanisms. Such equipment shall be capable of operating on a native IPv6-only access basis, while maintaining support for IPv4-only and dual-stack access, as applicable.

The requirements of this Technical Code apply regardless of whether equipment is implemented as a physical hardware appliance, a Virtualised Network Function (VNF) running on shared infrastructure, or a software-only instance. Where equipment is implemented in software or virtualised form, compliance shall be assessed based on the functional capability of the deployed instance, independent of the underlying hardware or hosting infrastructure.

This would be in line with the national aspiration to accelerate the adoption of IPv6 services in Malaysia and to allow consumers to access applications 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 references (including any amendments) applies.

MCMC MTSFB TC T022, *Communications Equipment - Baseline Requirements*

RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

RFC 4862, *IPv6 Stateless Address Autoconfiguration*

RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

RFC 8201, *Path MTU Discovery for IP version 6*

IPv6 Ready Core Protocols Test Specification, IPv6 Forum

3. Abbreviations

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

See Annex A.

DRAFT FOR PUBLIC COMMENT

4. Terms and definitions

4.1 464XLAT

A mechanism combining customer-side and provider-side translation for IPv4 service continuity across an IPv6 network.

4.2 Directly connected

Equipment or an equipment interface that establishes an Internet Protocol (IP) connectivity path to the public internet or a service provider network, including where the connectivity is established through a customer-premises network element, provided that the equipment independently establishes such connectivity for the provision or access of a service.

4.3 Dual-stack

A network configuration in which both IPv4 and IPv6 are enabled and supported on the same network interface or access connection, allowing communication using either IP version.

4.4 Equipment

Any communications equipment, whether implemented as hardware, software, or a virtualised instance (including a VNF, container, or cloud-hosted instance).

4.5 Internet access provider

An organisation that provides public internet access through a fixed, mobile, satellite or other internet access network.

4.6 Internet Protocol version 4 (IPv4) service continuity

The capability to maintain access to IPv4-only applications, services or destinations from an IPv6 network through appropriate translation, tunnelling or other service-continuity mechanisms.

4.7 Native Internet Protocol version 6 (IPv6)-only access

A network access configuration in which IPv6 is the only IP version used on the access interface for communications with the network.

4.8 Network Element (NE)

A device or system that provides network connectivity and performs functions such as IP processing, packet routing, packet forwarding, switching, access or gateway functions between network interfaces or destinations.

4.9 Network Security Element (NSE)

A device or system that permits, denies, inspects, filters, monitors and/or controls network traffic between network interfaces to detect, prevent or mitigate potentially malicious or unauthorised activity.

4.10 Next Generation (xG)

Generic designation used in this Technical Code to refer to future generations of mobile and wireless communications systems, including 6G (IMT-2030) and subsequent generations.

Note: The term Next Generation (xG) is used as a technology-neutral designation and does not denote a specific standardised generation unless otherwise specified.

DRAFT FOR PUBLIC COMMENT

4.11 Private network

A network that is restricted to authorised users or organisations and is used for private communications or services, including on-premises network, private Access Point Name (APN), private 4G or 5G network or other dedicated network that does not provide public internet access.

4.12 Public internet access

Connectivity that provides access to the public internet and publicly reachable internet applications, services or destinations through an internet service provider or other service provider.

4.13 Public network

A network that provides connectivity to multiple users or organisations and is operated by a network or service provider for general access, including connectivity to the public internet.

4.14 Terminal/Host

A device or element, which is, network participant that sends and receives packets but does not forward them on behalf of other network devices. Its primary purpose is to support application protocol and services that originate and/or terminate IP layer communications.

5. Baseline requirements

Equipment shall comply with the applicable baseline requirements specified in MCMC MTSFB TC T022.

6. Equipment categories

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

a) Terminal/Host;

b) Network Element (NE); and

c) Network Security Element (NSE).

The applicability of the IPv6 requirements shall be determined based on the equipment function and its network connectivity or interface.

Any equipment directly connected to the public internet providing public internet access shall be subjected to IPv6 compliance certification in accordance with this Technical Code.

For the purpose of this Technical Code, ‘directly connected’ means equipment or an equipment interface that establishes an IP connectivity path directly to the public internet or to a public network providing public internet access. For clarity:

a) Equipment that terminates or originates traffic directly with the public internet via an IPv6 prefix assigned directly by an internet access provider is considered directly connected. Such equipment shall be capable of operating on a native IPv6-only access basis, while maintaining support for IPv4-only and dual-stack access, as applicable.

b) The interface providing public internet access shall support native IPv6-only access operation, regardless of whether the equipment also provides connectivity to a private network. Where the

DRAFT FOR PUBLIC COMMENT

same equipment provides both public internet access and private network connectivity, the equipment shall be subject to IPv6 compliance certification.

c) Interfaces serving the private network are exempted from the native IPv6-only access requirement and may operate in IPv4-only, dual-stack or IPv6 mode. Where the equipment is used exclusively within a private network and does not provide public internet access, the native IPv6-only access requirement and IPv6 compliance certification requirement shall not apply.

d) Equipment connected to the public internet via a home, office or enterprise gateway is considered not directly connected and is not subject to the direct connectivity certification requirement. However, some equipment may require a connection to the service provider network to provide its service. Such equipment shall support IPv6 on the service provider connection where applicable. For example, a femto gateway located behind a home or office gateway shall support a native IPv6-only connection to the service provider's security gateway.

e) Equipment and its applicable applications and services shall support IPv6 access. Where access to an IPv4-only application, service or destination is required, IPv4 service continuity shall be supported through the equipment, gateway or network, as applicable.

Figure 1 illustrates network connectivity to Network Service Provider (NSP) and public internet. A directly connected equipment shall support native IPv6-only operation on its internet-facing access. This does not require content on the internet itself to be IPv6-only, as IPv4-only content and services shall continue to be reachable through translation and service-continuity mechanisms (for further details, see Annex D and F).

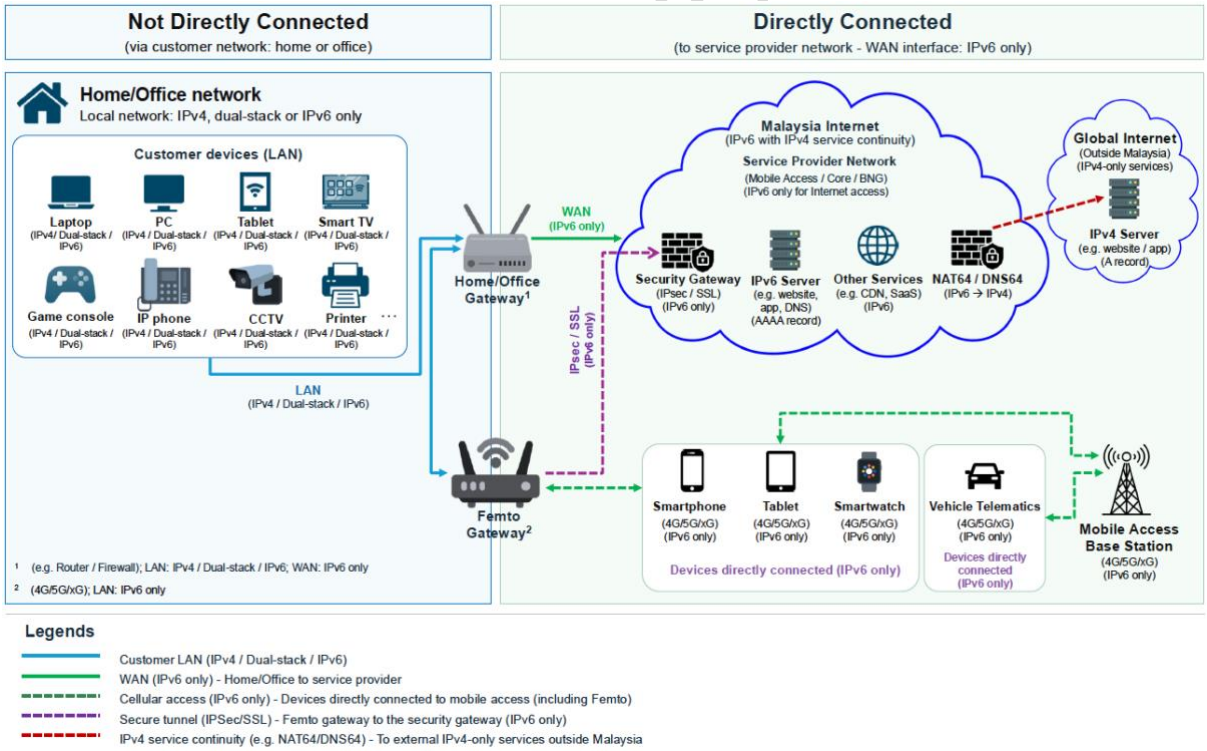

Figure 1. Network connectivity to NSP and public internet

The requirement for native IPv6-only operation applies to the access method of internet-facing equipment, not to the content or services available on the internet.

A single equipment may have multiple network interfaces with different scoping outcomes. Only the interface(s) connecting directly to the public internet are subject to the native IPv6-only requirement.

The non-exhaustive list of equipment and its category which are subject to this Technical Code are as defined in Annex B.

Annex C provides the examples of equipment scope based on network connectivity. It was identified within the scope of this Technical Code, where it connects directly to the public internet. The same equipment type used exclusively within a private network without public internet access is not subject to the native IPv6-only access requirement. The same equipment may have different requirements depending on the interface used for connectivity.

Figure 2 illustrates private network connectivity without public internet access.

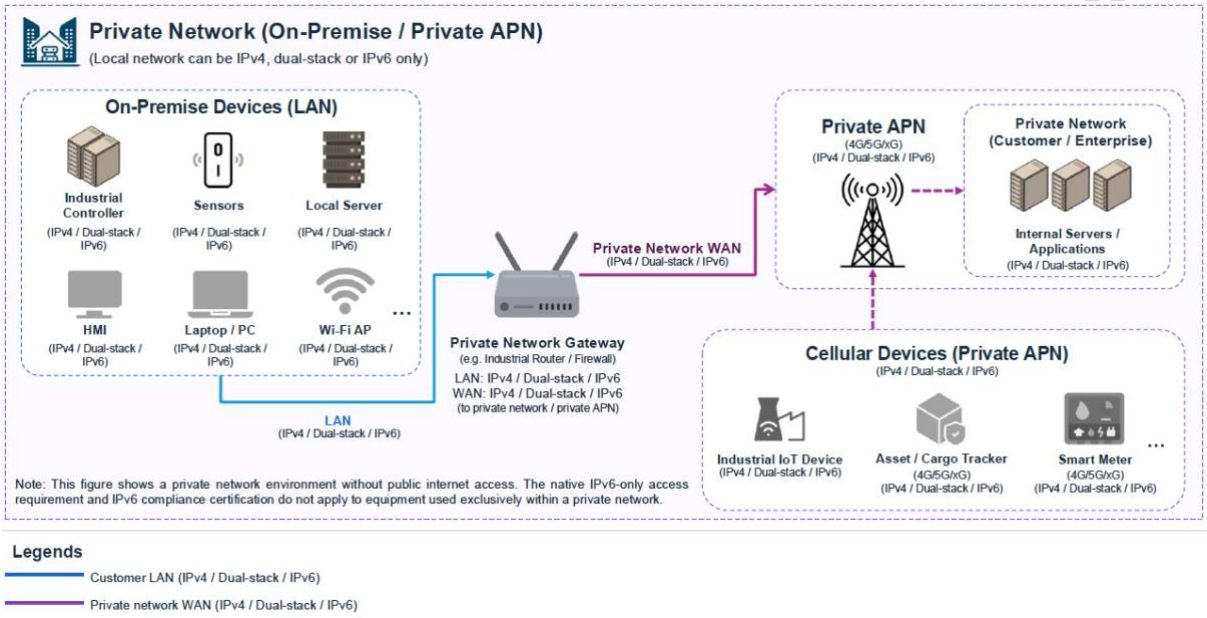

Figure 2. Private network connectivity without public internet access

Annex D provides a recommendation of the RFC specifications which should be fulfilled where applicable according to the primary function of the equipment. While Annex E provides the list of RFCs for reference.

For compliance certification purposes, an equipment shall be assessed as a complete and fully functional entity. Where the equipment implements more than one functional role, the highest function shall determine its classification and applicable compliance requirements under Annex F.

Accordingly, compliance shall be demonstrated against the requirements of that highest function. For example, equipment incorporating both host and NSE functions shall be classified and certified as an NSE.

7. Segments

Segments refer to classes or categories in which IPv6 compliant equipment shall be deployed wherever applicable. For any given function of an IPv6 compliant equipment, the model of equipment to cater for each segment shall 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 Technical Code.

DRAFT FOR P

3 segments are as described below:

a) Consumer

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

i) wired or wireless broadband;

ii) mobile cellular (4G, 5G, xG); and

iii) satellite and other last-mile internet access technologies.

b) Enterprise

i) Private sector; and

ii) public sector.

c) Service providers

i) NSP;

ii) Network Facilities Provider (NFP);

iii) Application Service Provider (ASP);

iv) Content Application Service Provider (CASP);

v) internet exchange;

vi) Cloud Service Provider (CSP); and

vii) data centres.

8. Functional requirements

IPv6 functional requirements are categorised as Table 1 below.

Table 1. 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, temporary address extensions for Stateless Address Autoconfiguration (SLAAC) and Cryptographically Generated Addresses (CGAs).
3	Transition mechanisms	Technical requirement for internet-facing equipment to operate on a native IPv6-only access basis, while retaining the ability to reach both IPv4-only and IPv6 content and services on the Internet through translation and service-continuity mechanisms (e.g., IPv6 Provider Edge (6PE) or IPv6 VPN Provider Edge Router (6VPE), Generic Routing Encapsulation (GRE), Network Address Translation 64 (NAT64), Domain Name System 64 (DNS64), 464XLAT).
4	Link specific	Technical requirement for different link layer technologies.
5	Routing protocols	Technical requirement for interior and exterior gateway protocol.

DRAFT FOR PUBLIC COMMENT

Table 1. IPv6 functional requirements

No	IPv6 functional	Description
6	Multicasting	Technical requirement for generalised multicast and configures options for Single Source Multicast (SSM) capabilities.
7	Network management	Technical requirement for: a) Simple Network Management Protocol (SNMP); b) Management Information Bases (MIBs); and c) telemetry.
8	Application requirement	Technical requirement for network services such as: a) Domain Name System (DNS) including DNS64 where applicable; b) Dynamic Host Configuration Protocol version 4 (DHCPv4), refer to RFC 8925; c) Dynamic Host Configuration Protocol version 6 (DHCPv6), refer to RFC 9915; and d) socket Application Programming Interface (API).
9	Quality of Service (QoS)	Technical requirement for Differentiated Service (DS) mechanisms in the router
10	IP Security (IPSec)	Technical requirement for IPSec and its key management protocol
11	Network protection device	Technical requirement: a) Firewall (FW); b) Application Firewall (APFW); c) Intrusion Detection System (IDS); d) Intrusion Protection System (IPS); and e) Session Border Controller (SBC).

The details of its functions are shown in Annex D.

9. IPv6 compliance requirement

Annex F describes the following 5-core compliance requirement across the 3 categories of equipment in all segments outlined in Clause 6.

a) RFC 8200.

b) RFC 4861.

c) RFC 4862.

d) RFC 8201.

e) RFC 4443.

There are 2 levels of compliance requirement 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 is the same thus have been combined for simplicity.

DRAFT FOR PUBLIC COMMENT

10. Sample test report

As IPv6 standards are still evolving, exceptions shall be granted and/or test cases shall be updated or invalidated based on the development of global standards.

The latest version of the Test Specification Document by IPv6 Forum shall be accepted. Refer to the *IPv6 Ready Core Protocols Test Specification* for the detailed testing steps.

The device shall comply with and pass all the mandatory IPv6 tests as specified in Annex F.

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

DRAFT FOR PUBLIC COMMENT

Annex A
(informative)

Abbreviations

6PE	IPv6 Provider Edge
6VPE	IPv6 VPN Provider Edge Router
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
APFW	Application Firewall
API	Application Programming Interface
APN	Access Point Name
ARP	Address Resolution Protocol
ASP	Application Service Provider
ATM	Automated Teller Machine
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol version 4
BNG	Broadband Network Gateway
CASP	Content Application Service Provider
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CCTV	Closed Circuit Television
CDN	Content Delivery Network
CGA	Cryptographically Generated Address
CPE	Customer Premises Equipment
CSP	Cloud Service Provider
DAD	Duplicate Address Detection
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHCPv4	Dynamic Host Configuration Protocol version 4
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
DNS64	Domain Name System 64
DNSSEC	Domain Name System Security Extensions
DS	Differentiated Services
ECN	Explicit Congestion Notification
EDNS0	Extension Mechanisms for DNS
EF PHB	Expedited Forwarding Per-Hop Behaviour
ESP	Encapsulating Security Payload
FDDI	Fibre Distributed Data Interface
FW	Firewall
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
GRE	Generic Routing Encapsulation
HeNB-GW	Home enodeB Gateway

DRAFT FOR PUBLIC COMMENT

HG	Home Gateway
HMAC	Hash Message Authentication Code
HMI	Human-Machine Interface
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol for IPv6
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IGMPv3	Internet Group Management Protocol version 3
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IoT	Internet of Things
IP	Internet Protocol
IP PBX	Internet Protocol Private Branch Exchange
IPS	Intrusion Protection System
IPSec	IP Security
IPSec-v3	IP Security version 3
IPTV STB	Internet Protocol Television Set Top Box
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS - IS	Intermediate System to Intermediate System
LAN	Local Area Network
LB	Load Balancer
MAPOS	Multiple Access Protocol Over SONET/SDH
MIB	Management Information Base
MIP	Mobile Internet Protocol
MIPv6	Mobile IPv6
MLDv2	Multicast Listener Discovery version 2
MME	Mobility Management Entity
MODP	More Modular Exponential
MPLS	Multi-Protocol Label Switching
MTU	Multicast Listener Discovery
NA	Neighbour Advertisement
NAT64	Network Address Translation 6
NE	Network Element
NF	Network Function
NFP	Network Facility Provider
NS	Neighbour Solicitation
NSE	Network Security Element
NSF	Network Security Function
NSP	Network Service Provider
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSPFv3	Open Shortest Path First version 3
P-GW	Packet Data Network Gateway

DRAFT FOR PUBLIC COMMENT

PHB	Per Hop Behaviour
PIM-SM	Protocol Independent Multicast - Sparse Mode
PMTU	Path Maximum Transmission Unit
POS	Point-Of-Sale
PPP	Point-to-Point Protocol
PREF64	Prefix for NAT64
QoS	Quality of Service
RAN	Radio Access Network
RG	Residential Gateway
S-GW	Serving Gateway
SaaS	Software as a Service
SBC	Session Border Controller
SD-WAN	Software-Defined Wide Area Network
Se-GW	Security Gateway
SEND	Secure Neighbour Discovery
SLAAC	Stateless Address Autoconfiguration
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SSL	Secure Sockets Layer
SSM	Single Source Multicast
UDP	User Datagram Protocol
UE	User Equipment
UPF	User Plane Function
URI	Uniform Resource Identifier
VNF	Virtualised Network Function
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
xG	Next Generation

DRAFT FOR PUBLIC COMMENT

Annex B
(informative)

Category of equipment

Table B.1. Category of equipment

Category	Description	Equipment
Terminal/ Host	User Equipment (UE) that directly connected, assigned an IPv6 prefix or address directly by a service provider.	a) Closed Circuit Television (CCTV) b) Internet of Things (IoT) devices that required IP connectivity c) Card terminal or Point-Of-Sale (POS) terminal d) Automated Teller Machine (ATM) e) Self-service kiosk or ticketing terminal f) Vehicle telematics unit or connected vehicle module g) Fleet management tracking device h) Internet Protocol Television Set Top Box (IPTV STB) i) Smart meter j) Smartphone k) Cellular tablet l) Wearable device m) Asset or cargo tracker n) Other internet-enabled terminal/host equipment o) Satellite broadband equipment
NE	Network Function (NF): a) Physical; b) virtual; or c) cloud-hosted component performing a NF.	a) Broadband Network Gateway (BNG) b) Packet Data Network Gateway (P-GW) or Serving Gateway (S-GW) c) User Plane Function (UPF) d) Internet Protocol Private Branch Exchange (IP PBX) e) Layer 3 switch or router f) Network address translator g) Load Balancer (LB) h) Mobility Management Entity (MME) i) Radio Access Network (RAN) access gateway (e.g., femto gateway, Home enodeB Gateway (HeNB-GW), small cell gateway) j) Residential Gateway (RG) or Home Gateway (HG) k) Fixed wireless access gateway l) Wireless access controller m) Wireless access point n) Software-Defined Wide Area Network (SD-WAN) edge device
NSE	Network Security Function (NSF): a) Physical; b) virtual; or c) cloud-hosted component performing a NSF.	a) Unified threat management b) Web application FW c) Virtual Private Network (VPN) gateway or concentrator d) Secure web gateway e) FW f) IDS g) IPS h) Distributed Denial of Service (DDoS) protection appliance i) Security Gateway (Se-GW)

DRAFT FOR PUBLIC COMMENT

Table B.1. Category of equipment

Category	Description	Equipment
Notes: 1. Equipment may apply for multiple categories. 2. Equipment may function as Terminal/Host, NE and/or NSE. 3. For equipment that are sharing the same Operating System (OS), testing report on one representative model is acceptable, per equipment type.		

IPv6 is also mandated for cellular equipment (under Terminal/Host). However, 3GPP standards shall take precedence over the requirements in Annex F for cellular interfaces.

RG, HG and equivalent broadband Customer Premises Equipment (CPE) are included under NE and, where applicable, shall comply with IPv6 transition, translation and application requirements in Annex D and Annex F.

DRAFT FOR PUBLIC COMMENT

Annex C
(informative)

Network connectivity equipment

Table C.1. Examples of equipment scope based on network connectivity

Equipment	Interface	Connectivity path	In scope	Native IPv6 access requirement
Cellular tablet or smartphone	Cellular	Direct to cellular provider	Yes	Mandatory
Tablet	Wireless Fidelity (Wi-Fi)	Via home or office router	No	a) Optional for applications and services b) IPv4 service continuity shall be maintained where required
Laptop with cellular	Cellular	Direct to cellular provider	Yes	Mandatory
Laptop	Wi-Fi or ethernet	Via home or office router	No	a) Optional b) IPv4 service continuity shall be maintained where required using dual-stack
Smart TV	Wi-Fi or ethernet	Via home or office router	No	a) Optional b) IPv4 service continuity shall be maintained where required
Smartwatch (standalone)	Cellular	Direct to cellular provider	Yes	Mandatory
Smartwatch (paired mode)	Bluetooth	Relayed via phone	No	N/A
Smartwatch (standalone)	Wi-Fi	Via home or office router	No	Optional
Vehicle telematics unit	Cellular	Direct to cellular provider	Yes	Mandatory
instrumentation or industrial sensor (cellular-connected)	Cellular	Direct to cellular provider	Yes	Mandatory
RG	Cellular or fibre	Direct to service provider	Yes	Mandatory for Wide Area Network (WAN), dual-stack for Local Area Network (LAN)
Office or enterprise gateway	Fibre or ethernet	Direct to service provider	Yes	Mandatory for WAN, dual-stack for LAN
Satellite broadband equipment	Satellite	Direct to satellite service provider	Yes	Mandatory

DRAFT FOR PUBLIC COMMENT

Annex D
(informative)

IPv6 functions

The following legends are applied for the IPv6 functions as stipulated in Tables D.1 until D.11:

a) M is mandatory;

b) O is optional;

c) c(M) is conditional mandatory (for specific reason or element);

d) MS is managed services;

e) APFW is Application Firewall;

f) DHCP is Dynamic Host Configuration Protocol (for client);

g) DS is Differentiated Services;

h) FW is Firewall;

i) IDS is Intrusion Detection System;

j) IPS is Intrusion Protection System;

k) IPSec is IP Security;

l) IPSec-v3 is IP Security version 3;

m) IPv4 is Internet Protocol version 4;

n) MIP is Mobile IP;

o) MPLS is Multi-Protocol Label Switching;

p) SLAAC is Stateless Address Autoconfiguration;

q) SNMP is Simple Network Management Protocol; and

r) SSM is Single Source Multicast;

DRAFT FOR PUBLIC COMMENT

Table D.1. Basic IPv6 functions

IETF specification	IPv6 basic functions	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 8200[a,d]	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 4861[a,b,d]	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
	Neighbour Advertisement (NA) and Neighbour Solicitation (NS) processing	-	M	M	-	-	M	M	-	-	M	M	M
RFC 4862[a,b,d]	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 8201[a,d]	Path Maximum Transmission Unit (PMTU) discovery for IPv6	-	M	M	-	-	M	M	-	-	M	M	M
	Discovery protocol requirements	-	M	M	-	-	M	M	-	-	M	M	M
RFC 4443[a,b,d]	Internet Control Message Protocol for IPv6 (ICMPv6)	-	M	M	-	-	M	M	-	-	M	M	M
RFC 8504[a,c]	IPv6 node requirements	-	-	O	-	-	-	O	-	-	-	O	-
RFC 5095[b,d]	Deprecation of Type 0 routing headers	MS	-	M	-	-	M	M	-	-	M	M	M

DRAFT FOR PUBLIC COMMENT

Table D.1. Basic IPv6 functions

IETF specification	IPv6 basic functions	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4884[a,b,d]	Extended Internet Control Message Protocol (ICMP) for multi-part messages	MS	-	c(M)	-	-	-	-	-	-	-	-	-
RFC 2675[b,e]	IPv6 Jumbograms	-	O	O	-	-	-	-	-	-	-	-	-
RFC 5175[b,e]	IPv6 router advertisement flags option	-	M	M	-	-	-	-	-	-	-	-	-
RFC 4191[a,b,d]	Default router preference	-	M	M	M	-	-	-	-	-	-	-	M

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.
[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.
[c] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Br1.
[d] This RFC is aligned with the IPv6 Ready, *Core Protocols Test Specification 5.1.4*.
[e] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

DRAFT FOR PUBLIC COMMENT

Table D.2. IPv6 addressing requirement

IETF specification	IPv6 addressing	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4861[a,b,c]	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 address	SLAAC	M	M	-	SLAAC	M	M	-	SLAAC	M	M	M
RFC 4862[a,b,c]	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 4291[a,b,c]	IPv6 addressing architecture	-	M	M	-	-	M	M	-	-	M	M	-
RFC 4007[a,b]	IPv6 scoped address architecture	-	M	M	-	-	M	M	-	-	M	M	-
	Ability to manually configure addresses	-	M	M	-	-	M	M	-	-	M	M	-
RFC 4193[a,b]	Unique local IPv6 unicast address	-	O	O	-	-	O	O	-	-	O	O	-
RFC 3879[a,b]	Deprecating site local addresses	-	M	M	-	-	M	M	-	-	M	M	-
RFC 6724[a]	Default address selection for IPv6	-	M	M	-	-	M	M	-	-	M	M	-
	Configurable selection policies	-	M	M	-	-	M	M	-	-	M	M	-
RFC 2526[a,b]	Reserved IPv6 subnet anycast addresses	-	O	O	-	-	O	O	-	-	O	O	-
RFC 3972[a,b]	CGA	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-
RFC 4581[a,b]	CGA extension field format	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-

DRAFT FOR PUBLIC COMMENT

Table D.2. IPv6 addressing requirement

IETF specification	IPv6 addressing	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4982[a,b]	CGA support for multiple hash algos	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-
RFC 5952[a]	A recommendation for IPv6 address text	-	O	O	-	-	O	O	-	-	O	O	-
RFC 6085[e]	Address mapping of IPv6 multicast packets on ethernet	-	O	O	-	-	O	O	-	-	O	O	-
RFC 7217[a,c]	Semantically opaque interface identifiers for SLAAC	SLAAC	O	-	-	SLAAC	O	-	-	SLAAC	O	-	-
RFC 8981[d]	Temporary address extensions for IPv6 SLAAC	SLAAC	M	-	-	SLAAC	M	-	-	SLAAC	M	-	-
	Second context for MIP mobile node	-	O	-	-	-	M	-	-	-	M	-	-

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.

[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.

[c] This RFC is aligned with the IPv6 Ready, *Core Protocols Test Specification 5.1.4*.

[d] This RFC supersedes the obsolete RFCs. Where an obsolete RFC is referenced by a recognised standards or technical body (e.g., NIST or the IPv6 Forum), the specific requirement cited from that RFC may remain relevant.

[e] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

Note: Condition is referred when VPN or other encryption protocol (e.g. Secure Neighbour Discovery (SEND)) initiate from the specific devices. For protection devices such as FW, it should be able to work with CGA.

DRAFT FOR PUBLIC COMMENT

Table D.3. Transition mechanism requirements

IETF specification	Transition mechanism	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4213[b]	Basic transition mechanisms for IPv6 hosts and routers	IPv4	M	M	-	IPv4	M	M	-	IPv4	M	M	-
RFC 4798[a,b]	Connecting IPv6 islands over IPv4 MPLS using 6PE routers	-	-	-	-	IPv4, MPLS	-	M	-	IPv4, MPLS	-	M	-
RFC 4659[a]	6VPE	-	-	-	-	IPv4, MPLS	-	M	-	IPv4, MPLS	-	M	-
RFC 6146[a]	NAT64	IPv4	-	M	M	IPv4	-	M	M	IPv4	-	M	M
RFC 6052[d]	IPv6 addressing of IPv4/IPv6 translators	-	O	M	M	-	O	M	M	-	O	M	M
RFC 8781[c]	Discovering Prefix for NAT64 (PREF64) in router advertisements	-	-	M	M			M	M	-	-	M	M
RFC 7050[c]	DNS64-based discovery of the IPv6 prefix used for IPv6 address synthesis	-	--	O	O	-	-	O	-	-	-	O	-
RFC 6147[a]	DNS64 and IPv6-only access with IPv4 service continuity	-	-	M	-	-	-	M	-	-	-	M	-
RFC 6877[a]	464XLAT and IPv6-only access	-	O	M	-	-	O	M	-	-	O	M	-
RFC 7915[a]	IP/ICMP translation algorithm and IPv6-only access	-	-	M	-	-	-	M	-	-	-	M	-
RFC 2784[a,b]	GRE	-	-	O	-	-	-	O	-	-	-	O	-

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.

[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.

[c] This RFC supersedes the obsolete RFCs. Where an obsolete RFC is referenced by a recognised standards or technical body (e.g., NIST or the IPv6 Forum), the specific requirement cited from that RFC may remain relevant.

[d] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

DRAFT FOR PUBLIC COMMENT

Table D.4. Link specific requirements

IETF specification	Link specific	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2464[a,b,c]	IPv6 over ethernet	Condition	M	M	M	-	M	M	M	-	M	M	M
RFC 2467[b,c]	IPv6 over Fibre Distributed Data Interface (FDDI)	-	M	M	M	-	M	M	M	-	M	M	M
RFC 3572[b,c]	IPv6 over Multiple Access Protocol Over SONET/SDH (MAPOS)	-	-	M	M	-	-	M	M	-	-	M	M
RFC 4338[b,c]	IPv6 IPv4 and Address Resolution Protocol (ARP) packets over fibre channel	-	M	M	M	-	M	M	M	-	M	M	M
RFC 4944[a,b,c]	IPv6 over IEEE 802.15.4 networks		-	M	-	-	-	M	-	-	-	M	-
RFC 5072[a,b,c]	IPv6 over Point-to-Point Protocol (PPP)	-	M	M	M	-	M	M	M	-	M	M	M

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.
[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.
[c] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

Note: Condition is applicable when the specified link technology is chosen as preferred choice.

DRAFT FOR PUBLIC COMMENT

Table D.5. Routing protocol

IETF specification	Routing protocol	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 5340[a,b]	Open Shortest Path First (OSPF) for IPv6	-	-	-	-	Condition	-	M	M	Condition	-	M	M
RFC 4552[a,b,c]	Authentication or confidentiality for Open Shortest Path First version 3 (OSPFv3)	-	-	-	-	Condition	-	M	-	Condition	-	M	-
RFC 1195[a,c]	Use of Open Systems Interconnection (OSI) Intermediate System to Intermediate System (IS - IS) for routing in TCP/IP and dual environments	-	-	-	-	-	-	-	-	Condition	-	M	-
RFC 5187[a,c]	OSPFv3 graceful restart	-	-	-	-	-	-	-	-	-	-	M	-
RFC 4271[a,b,c]	Border Gateway Protocol version 4 (BGP-4)	-	-	-	-	Condition	-	c(M)	-	Condition	-	M	-
	Border Gateway Protocol (BGP) application in the internet	-	-	-	-	Condition	-	M	-	Condition	-	M	-
RFC 1772[b,c]	BGP multi-protocol extensions	-	-	-	-	Condition	-	M	-	Condition	-	M	-
RFC 4760[a,b,c]	BGP multi-protocol extensions for IPv6 IDR	-	-	-	-	Condition	-	M	-	Condition	-	M	-
RFC 2545[a,b,c]	BGP MPLS IP VPN extension for IPv6 VPN	-	-	-	-	-	-	-	-	-	-	M	-

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.
[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.
[c] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

Note: Condition for the Interior Gateway Protocol (IGP) and hardware FW.

DRAFT FOR PUBLIC COMMENT

Table D.6. Multicast

IETF specification	Multicast	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 9777[c]	Multicast Listener Discovery version 2 (MLDv2) for IPv6	SSM	M	M	-	SSM	M	M	-	SSM	M	M	-
RFC 3306[a,b,d]	Unicast-prefix-based IPv6 multicast address	Multicast	M	M	-	Multicast	M	M	-	Multicast	M	M	-
RFC 3307[a,b,d]	Allocation guidelines for IPv6 multicast address	Multicast	M	M	-	Multicast	M	M	-	Multicast	M	M	-
RFC 4607[a,b,d]	Source-specific multicast for IP	SSM	-	-	-	SSM	-	-	-	SSM	-	O	-
RFC 4604[a,b,d]	MLDv2 for source specific multicast	SSM	-	-	-	SSM	-	-	-	SSM	-	O	-
RFC 7761[a]	Protocol Independent Multicast - Sparse Mode (PIM-SM)	Multicast -routing	-	-	-	Multicast -routing	-	-	-	Multicast -routing	-	O	-

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.

[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.

[c] This RFC supersedes the obsolete RFCs. Where an obsolete RFC is referenced by a recognised standards or technical body (e.g., NIST or the IPv6 Forum), the specific requirement cited from that RFC may remain relevant.

[d] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

Note: Condition when group management capability is required – Internet Group Management Protocol (IGMP).

DRAFT FOR PUBLIC COMMENT

Table D.7. Network management

IETF specification	Network management	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
Network management requirements													
RFC 3411[a,b,d]	Simple Network Management Protocol version 3 (SNMPv3) management framework	MS	-	-	-	SNMP	M	M	M	SNMP	M	M	M
RFC 3412[a,b,d]	SNMP message process and dispatch	-	-	-	-	SNMP	M	M	M	SNMP	M	M	M
RFC 3413[a,b,d]	SNMP applications	MS	-	-	-	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[a,b,d]	User-based security model for SNMPv3	-	-	-	-	SNMP	M	M	-	SNMP	M	M	-
MIB													
RFC 4293[a,b,d]	MIB for the IP	-	-	-	-	SNMP	M	M	-	SNMP	M	M	-
RFC 4292[a,b,d]	MIB for the IP forwarding table	-	-	-	-	SNMP		M	-	SNMP	-	M	-
RFC 4087[a,b,d]	MIB for IP tunnels	-	-	-	-	SNMP & IPv4	-	M	-	SNMP & IPv4	-	M	-
RFC 4807[a,b,d]	MIB or IPSec policy database configuration	-	-	-	-	SNMP & IPSec-v3	-	M	-	SNMP & IPSec-v3	-	M	-

DRAFT FOR PUBLIC COMMENT

Table D.7. Network management

IETF specification	Network management	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4295[b,d]	MIB for Mobile IPv6 (MIPv6)	-	-	-	-	SNMP & MIP	-	M	-	SNMP & MIP	-	M	-
RFC 3289[a,b,d]	MIB for DiffServ	-	-	-	-	SNMP & DS	-	M	-	SNMP & DS	-	M	-
Telemetry													
RFC 9343[c]	IPv6 application of the alternate-marking method		-	-	-	-	-	-	-	-	-	O	-

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.
[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.
[c] This RFC supersedes the obsolete RFCs. Where an obsolete RFC is referenced by a recognised standards or technical body (e.g., NIST or the IPv6 Forum), the specific requirement cited from that RFC may remain relevant.
[d] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

DRAFT FOR PUBLIC COMMENT

Table D.8. Application

IETF specification	Application	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 3596[a,b,d]	DNS extensions for IPv6	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M
RFC 6891[c]	Extension Mechanisms for DNS (EDNS0)	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M
RFC 3226[a,b,d]	Domain Name System Security Extensions (DNSSEC) and IPv6 DNS message	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M
	Size requirements	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M
RFC 3986[a,b,d]	Uniform Resource Identifier (URI): Generic syntax	Condition	M	M	M	Condition	M	M	M	Condition	M	M	M
RFC 3493[b,d]	Basic socket API for IPv6	Condition	M	-	-	Condition	M	-	-	Condition	M	-	-
RFC 9915[c]	DHCPv6 functions (If host supports DHCP, it should also support DHCPv6)	Condition	O	O	O	Condition	O	O	O	Condition	O	O	O
RFC 6147[a]	DNS64 and IPv6-only access with IPv4 service continuity	-	-	M	-	-	-	M	-	-	M	-	-
RFC 8925[c]	IPv6-Only preferred option for DHCPv4	-	-	O	-	-	-	O	-	-	M	-	-
RFC 9915[c]	Stateless DHCP service for IPv6	SLAAC	M	M	-	SLAAC	M	M	-	SLAAC	M	M	M
	DHCPv6	DHCP	M	-	-	DHCP	M	-	-	DHCP	M	-	-
	Ability to administratively disable	DHCP	M	-	-	DHCP	M	-	-	DHCP	M	-	-

DRAFT FOR PUBLIC COMMENT

Table D.8. Application

IETF specification	Application	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 9915[c]	DHCP client functions	DHCP	M	-	-	DHCP	M	-	-	DHCP	M	-	-
	Prefix delegation	DHCP	M	M	-	DHCP	M	M	-	DHCP	M	M	M
RFC 4361[b,d]	Node-specific client IDs for DHCPv4	DHCP	M	-	-	DHCP	M	-	-	DHCP	M	-	-

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.

[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.

[c] This RFC supersedes the obsolete RFCs. Where an obsolete RFC is referenced by a recognised standards or technical body (e.g., NIST or the IPv6 Forum), the specific requirement cited from that RFC may remain relevant.

[d] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

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 9915 is when the device supports DHCP.

DRAFT FOR PUBLIC COMMENT

Table D.9. QoS

IETF specification	QoS	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2474[a,b,c,d]	DiffServ header field	Condition	M	M	-	DS	M	M	-	DS	M	M	-
RFC 3140[a,b,d]	Per Hop Behaviour (PHB) encoding – DiffServ	Condition	M	M	-	DS	M	M	-	DS	M	M	-
RFC 3168[a,b,c,d]	Explicit Congestion Notification (ECN)	-	-	-	-	-	-	-	-	Condition	-	O	-
RFC 2597[a,b,d]	Assured forwarding	-	-	-	-	-	-	-	-	Condition	-	O	-
RFC 3246[a,b,d]	Expedited forwarding	-	-	-	-	-	-	-	-	Condition	-	O	-
RFC 3247[a,b,d]	Supplementary Expedited Forwarding Per-Hop Behaviour (EF PHB)	-	-	-	-	-	-	-	-	Condition	-	O	-
RFC 2475[b,d]	DiffServ architecture	-	-	-	-	-	-	-	-	Condition	-	O	-
RFC 3260[b,d]	New term and clarification - DiffServ	-	-	-	-	-	-	-	-	Condition	-	O	-
RFC 2983[b,d]	DiffServ and tunnels	-	-	-	-	-	-	-	-	Condition	-	O	-
RFC 4594[b,d]	Config guidelines DiffServ	-	-	-	-	-	-	-	-	Condition	-	O	-

DRAFT FOR PUBLIC COMMENT

Table D.9. QoS

IETF specification	QoS	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 3086[b,d]	DiffServ per domain behaviour	-	-	-	-	-	-	-	-	Condition	-	O	-

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.
[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.
[c] This RFC is aligned with the IPv6 Ready, *Core Protocols Test Specification 5.1.4*.
[d] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

Notes:
1. Condition is DS and managed service.
2. Optional for NSP and NFP network elements.

DRAFT FOR PUBLIC COMMENT

Table D.10. IPv6 security

IETF specification	IPv6 security	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 3971[a]	SEND	-	O	O	-	-	M	M	-	-	M	M	M
RFC 2451[a,b,c]	Encapsulating Security Payload (ESP) Cipher Block Chaining (CBC) mode algorithms	-	-	-	-	-	-	-	-	-	-	O	O
RFC 3602[b,c]	Advanced Encryption Standard (AES) - CBC	-	-	-	-	-	-	O	O	-	-	O	O
RFC 3686[b,c]	AES-CTR	-	-	-	-	-	-	O	O	-	-	O	O
RFC 4309[b,c]	AES -Counter with CBC-MAC (CCM)	-	-	-	-	-	-	O	O	-	-	O	O
RFC 4106[b,c]	AES-Galois/Counter Mode (GCM)	-	-	-	-	-	-	O	O	-	-	O	O
RFC 4543[b,c]	AES-Galois Message Authentication Code (GMAC)	-	-	-	-	-	-	O	O	-	-	O	O
RFC 2404[b,c]	Hash Message Authentication Code (HMAC)-SHA-1-96	-	-	-	-	-	-	O	O	-	-	O	O
RFC 4868[b,c]	HMAC-SHA-256	-	-	-	-	-	-	O	O	-	-	O	O
RFC 3566[b,c]	AES-XCBC-MAC-96	-	-	-	-	-	-	O	O	-	-	O	O
RFC 4434[b,c]	AES-XCBC-PRF-128	-	-	-	-	-	-	O	O	-	-	O	O
Transition mechanisms requirements													
RFC 8247[a]	Algorithm implementation requirements and usage guidance for the Internet Key Exchange version 2 (IKEv2)	-	M	M	M	-	M	M	M	-	M	M	M
RFC 4213[b,c]	Transition mechanise for hosts and routers	-	M	M	-	-	M	M	-	-	M	M	-
RFC 4891[b,c]	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[a,b,c]	Generic packet tunnelling in IPv6	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-	Condition	c(M)	c(M)	-
RFC 4798[a,b,c]	Connecting IPv6 islands over IPv4 MPLS 6PE	MPLS	M	M	-	MPLS	M	M	-	MPLS	M	M	-

DRAFT FOR PUBLIC COMMENT

Table D.10. IPv6 security

IETF specification	IPv6 security	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
ICMP													
RFC 4890[c]	Recommendations for filtering ICMPv6 messages in FW	-	-	-	M	-	-	-	M	-	-	-	M
IPSec-v3													
RFC 4301 or RFC 6040[a,b,c]	Security architecture for the IP or tunnelling of explicit congestion notification	-	O	-	-	-	O	-	-	-	O	-	-
RFC 4303[a,b,c]	ESP	-	M	M	-	-	M	M	-	-	M	-	-
RFC 4302[b,c]	Authentication Header (AH)	-	O	-	-	-	O	-	-	-	O	-	-
RFC 3948[b,c]	User Datagram Protocol (UDP) encapsulation of ESP packets	-	O	-	-	-	O	-	-	-	O	-	-
RFC 4809[b,c]	Requirements for an IPSec cert management profile	-	-	O	O	-	-	O	O	-	-	O	O
IKEv2													
RFC 7296[a,c]	IKEv2 protocol	-	M	M	M	-	M	M	M	-	M	M	M
RFC 8247[a]	Algorithm implementation requirements and usage guidance for the IKEv2	-	M	M	M	-	M	M	M	-	M	M	M
RFC 3526[a]	More Modular Exponential (MODP) DH groups for Internet Key Exchange (IKE)	-	-	-	-	-	-	-	-	-	-	O	O
Uses of cryptographic algorithms													
RFC 2410[b,c]	NULL encryption	-	M	M	M	-	M	M	M	-	M	M	M
RFC 8221[a]	Cryptographic algorithms for ESP and AH	-	M	M	M	-	M	M	M	-	M	M	M

[a] This RFC is aligned with the 2020 edition of Special Publication (NIST SP) - 500-267Ar1.
[b] This RFC is aligned with the 2008 edition of Special Publication (NIST SP) - 500-267.
[c] This RFC is aligned with the IDA RS IPv6, *Singapore IPv6 Profile*.

Note: Condition is tunnelling transition.

DRAFT FOR PUBLIC COMMENT

Table D.11. Network security equipment

NIST SP - 500-267Ar1	Network security	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
4.14.3.1	IPv6 connectivity	-	-	-	M	-	-	-	M	-	-	-	M
4.14.3.2	Dual stack	-	-	-	O	-	-	-	O	-	-	-	O
4.14.3.3	Administrative functionality	-	-	-	M	-	-	-	M	-	-	-	M
4.14.3.3	Authentication and authorisation	-	-	-	M	-	-	-	M	-	-	-	M
4.14.3.5	Security of control and communications	-	-	-	-	-	-	-	M	-	-	-	M
4.14.3.6	Persistence	-	-	-	M	-	-	-	M	-	-	-	M
4.14.3.7	Logging and alerts	-	-	-	M	-	-	-	M	-	-	-	M
4.13.4.8	Fragmented packet handling	-	-	-	M	-	-	-	M	-	-	-	M
4.13.4.9	Tunnelled traffic handling	-	-	-	M	-	-	-	M	-	-	-	M
4.14.4.1	Port or protocol or address blocking	FW or APFW	-	-	M	FW or APFW	-	-	M	FW or APFW	-	-	M
4.14.4.2	Asymmetrical blocking	FW or APFW	-	-	M	FW or APFW	-	-	M	FW or APFW	-	-	M
4.14.4.3	IPv6 traffic filtering	FW or APFW	-	-	M	FW or APFW	-	-	M	FW or APFW	-	-	M
4.14.4.4	IPSec traffic handling	FW or APFW	-	-	-	FW or APFW	-	-	M	FW or APFW	-	-	M
4.14.4.5	Performance under load, fail-safe	FW or APFW	-	-	M	FW or APFW	-	-	M	FW or APFW	-	-	M
4.14.4.6	Logging	FW or APFW	-	-	M	FW or APFW	-	-	M	FW or APFW	-	-	M

DRAFT FOR PUBLIC COMMENT

Table D.11. Network security equipment

NIST SP - 500-267Ar1	Network security	Consumer				Enterprise				Service provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
4.14.5.1	No violation of trust barriers	APFW	-	-	M	APFW	-	-	M	APFW	-	-	M
4.14.5.2	Session traffic Auth	APFW	-	-	M	APFW	-	-	M	APFW	-	-	M
4.14.5.3	Email, file filtering	APFW	-	-	M	APFW	-	-	M	APFW	-	-	M
4.14.6.1	Known attack detection	IDS or IPS	-	-	M	IDS or IPS	-	-	M	IDS or IPS	-	-	M
4.14.6.2	Port-scanning detection	IDS or IPS	-	-	M	IDS or IPS	-	-	M	IDS or IPS	-	-	M
4.14.6.3	Tunnelled traffic detection	IDS or IPS	-	-	O	IDS or IPS	-	-	M	IDS or IPS	-	-	M
4.14.6.4	Logging and alerts	IDS or IPS	-	-	M	IDS or IPS	-	-	M	IDS or IPS	-	-	M
4.14.6.5	Performance under load, fail-safe	IDS or IPS	-	-	M	IDS or IPS	-	-	M	IDS or IPS	-	-	M
4.14.7.1	Intrusion prevention	IPS	-	-	M	IPS	-	-	M	IPS	-	-	M

DRAFT FOR PUBLIC COMMENT

Annex E
(informative)

Request for Comments (RFC)

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

RFC	Title
RFC 1195	Use of OSI IS-IS for routing in TCP/IP and dual environments
RFC 1772	Application of the Border Gateway Protocol in the Internet
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2410	The NULL Encryption Algorithm and Its Use with IPsec
RFC 2451	The ESP CBC-Mode Cipher Algorithms
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks
RFC 2467	Transmission of IPv6 Packets over FDDI Networks
RFC 2473	Generic Packet Tunnelling in IPv6 Specification
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Services
RFC 2491	IPv6 over Non-Broadcast Multiple Access (NBMA) networks
RFC 2507	IP Header Compression
RFC 2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links
RFC 2526	Reserved IPv6 Subnet Anycast Addresses
RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC 2597	Assured Forwarding 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	Differentiated Services and Tunnels
RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
RFC 3086	Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification
RFC 3095	RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed
RFC 3140	Per Hop Behavior Identification Codes
RFC 3146	Transmission of IPv6 Packets over IEEE 1394 Networks
RFC 3168	The Addition of Explicit Congestion Notification (ECN) to IP
RFC 3173	IP Payload Compression Protocol (IPComp)
RFC 3226	DNSSEC and IPv6 A6 aware server/resolver message size requirements
RFC 3241	Robust Header Compression (ROHC) over PPP
RFC 3246	An Expedited Forwarding PHB (Per-Hop Behavior)
RFC 3247	Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)
RFC 3260	New Terminology and Clarifications for Diffserv
RFC 3289	Management Information Base for the Differentiated Services Architecture
RFC 3306	Unicast-Prefix-based IPv6 Multicast Addresses

DRAFT FOR PUBLIC COMMENT

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

RFC	Title
RFC 3307	Allocation Guidelines for IPv6 Multicast Addresses
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (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 Application Program Interface (API) for IPv6
RFC 3566	The AES-XCBC-MAC-96 algorithm and its use with IPsec
RFC 3572	Internet Protocol Version 6 over MAPOS (Multiple Access Protocol Over SONET/SDH)
RFC 3590	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
RFC 3596	DNS Extensions to Support IP Version 6
RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec
RFC 3678	Socket Interface Extensions for Multicast Source Filters
RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
RFC 3843	RObust Header Compression (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	Network Mobility (NEMO) Basic Support Protocol
RFC 3971	SEcure Neighbor Discovery (SEND)
RFC 3972	Cryptographically Generated Addresses (CGA)
RFC 3986	Uniform Resource Identifier (URI): Generic Syntax
RFC 4007	IPv6 Scoped Address Architecture
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4038	Application Aspects of IPv6 Transition
RFC 4087	IP Tunnel MIB
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC 4113	Management Information Base for the User Datagram Protocol (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 Border Gateway Protocol 4 (BGP-4)
RFC 4283	Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
RFC 4291	IP Version 6 Addressing Architecture
RFC 4292	IP Forwarding Table MIB
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4295	Mobile IPv6 Management Information Base
RFC 4301	Security Architecture for the Internet Protocol
RFC 4302	IP Authentication Header

DRAFT FOR PUBLIC COMMENT

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

RFC	Title
RFC 4303	IP Encapsulating Security Payload (ESP)
RFC 4308	Cryptographic Suites for IPsec
RFC 4309	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (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 Four (DHCPv4)
RFC 4362	RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP
RFC 4380	Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)
RFC 4434	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) 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 OSPFv3
RFC 4581	Cryptographically Generated Addresses (CGA) Extension Field Format
RFC 4584	Extension to Sockets API for Mobile IPv6
RFC 4594	Configuration Guidelines for DiffServ Service Classes
RFC 4604	Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (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 MPLS Using IPv6 Provider Edge Routers (6PE)
RFC 4807	IPsec Security Policy Database Configuration MIB
RFC 4809	Requirements for an IPsec Certificate Management Profile
RFC 4815	RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095
RFC 4861	Neighbor Discovery for IP version 6 (IPv6)
RFC 4862	IPv6 Stateless Address Autoconfiguration
RFC 4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
RFC 4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture
RFC 4884	Extended ICMP to Support Multi-Part Messages
RFC 4890	Recommendations for Filtering ICMPv6 Messages in Firewalls
RFC 4891	Using IPsec to Secure IPv6-in-IPv4 Tunnels
RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
RFC 4945	The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
RFC 4982	Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (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	IP Version 6 over PPP
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6

DRAFT FOR PUBLIC COMMENT

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

RFC	Title
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 Mobile IPv6
RFC 5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 5329	Traffic Engineering Extensions to OSPF Version 3
RFC 5340	OSPF for IPv6
RFC 5380	Hierarchical Mobile IPv6 (HMIPv6) Mobility Management
RFC 5555	Mobile IPv6 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 RObust Header Compression (ROHC) Framework
RFC 5838	Support of Address Families in OSPFv3
RFC 5844	IPv4 Support for Proxy Mobile IPv6
RFC 5952	A Recommendation for IPv6 Address Text Representation
RFC 5969	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification
RFC 6040	Tunnelling of Explicit Congestion Notification
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 6147	DNS64: DNS Extensions for Network Address 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 (Historic)	Suite B Cryptographic Suites for IPsec
RFC 6724	Default Address Selection for Internet Protocol Version 6 (IPv6)
RFC 6846	RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)
RFC 6877	464XLAT: Combination of Stateful and Stateless Translation
RFC 6891	Extension Mechanisms for DNS (EDNS(0))
RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 7542	The Network Access Identifier
RFC 7761	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
RFC 7915	IP/ICMP Translation Algorithm
RFC 8200	Internet Protocol, Version 6 (IPv6) Specification
RFC 8201	Path MTU Discovery for IP version 6
RFC 8221	Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 8247	Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 8981	Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6
RFC 9777	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 9915	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

DRAFT FOR PUBLIC COMMENT

Annex F
(normative)

IPv6 compliance requirement

Table F.1. Section 1 - RFC 8200 IPv6 specification

RFC 8200	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	O	-	M	O
	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	O	-	M	O
	v6LC.1.1.10: IP Forwarding - source and destination address - intermediate node (routers only)	-	O	O	-	O	O
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)	-	O	O	-	O	O
	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	O	-	M	O
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
	Test v6LC.1.3.5: Overlapping fragments	-	O	O	-	O	O
	Test v6LC.1.3.6: First fragment doesn't contain all headers	-	O	O	-	O	O

DRAFT FOR PUBLIC COMMENT

Table F.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	O
	Test v6LC.2.1.2: Resolution wait queue	-	-	-	-	M	O
	Test v6LC.2.1.3: Prefix information option processing, on-link flag (hosts only)	-	-	-	M	O	O
	Test v6LC.2.1.4: Host prefix list (hosts only)	-	-	-	M	O	O
	Test v6LC.2.1.5: Neighbour solicitation origination, address resolution	-	-	-	-	M	O
	Test v6LC.2.1.6: Neighbour solicitation origination, reachability confirmation	-	-	-	-	M	O
	Test v6LC.2.1.7: Invalid neighbour solicitation handling	-	-	-	-	M	O
	Test v6LC.2.1.8: Neighbour solicitation processing, no NCE	-	-	-	-	M	O
	Test v6LC.2.1.9: Neighbour solicitation processing, NCE state *INCOMPLETE*	-	-	-	-	M	O
	Test v6LC.2.1.10: Neighbour solicitation processing, NCE state *REACHABLE*	-	-	-	-	M	O
	Test v6LC.2.1.11: Neighbour solicitation processing, NCE state *STALE*	-	-	-	-	M	O
	Test v6LC.2.1.12 Neighbour solicitation processing, NCE state *PROBE*	-	-	-	-	M	O
	Test v6LC.2.1.13: Neighbour solicitation processing, *IsRouterFlag* (host only)	-	-	-	M	O	O
	Test v6LC.2.1.14: Neighbour solicitation processing, anycast (routers only)	-	-	-	-	M	O
	Test v6LC.2.1.15: Invalid neighbour advertisement handling	-	-	-	-	O	O
	Test v6LC.2.1.16: Neighbour advertisement processing, no NCE	-	-	-	-	O	O
	Test v6LC.2.1.17: Neighbour advertisement processing, NCE state *INCOMPLETE*	-	-	-	-	O	O
	Test v6LC.2.1.18: Neighbour advertisement processing, NCE state *REACHABLE*	-	-	-	-	O	O
	Test v6LC.2.1.19: Neighbour advertisement processing, NCE state *STALE*	-	-	-	-	O	O
	Test v6LC.2.1.20: Neighbour advertisement processing, NCE state *PROBE*	-	-	-	-	O	O
	Test v6LC.2.1.21: Neighbour advertisement processing, R-bit change (hosts only)	-	-	-	M	O	O
Group 2: Router and prefix discovery	Test v6LC.2.2.1: Router solicitations (hosts only)	-	-	-	M	O	O
	Test v6LC.2.2.2: Router solicitations, solicited router advertisement (hosts only)	-	-	-	M	O	O
	Test v6LC.2.2.3: Host ignores router solicitations (hosts only)	-	-	-	M	O	O
	Test v6LC.2.2.4: Router ignores invalid router solicitations (routers only)	-	-	-	-	M	O
	Test v6LC.2.2.5: Router sends valid router advertisement (routers only)	-	-	-	-	M	O

DRAFT FOR PUBLIC COMMENT

Table F.2. Section 2 - RFC 4861 neighbour discovery for IPv6

RFC 4861	Test case	Consumer			Enterprise/ Service provider		
		Host	NE	NSE	Host	NE	NSE
Group 2: Router and prefix discovery	Test v6LC.2.2.6: Router does not send router advertisements on non-advertising interface (routers only)	-	-	-	-	M	O
	Test v6LC.2.2.7: Sending unsolicited router advertisements (routers only)	-	-	-	-	M	O
	Test v6LC.2.2.8: Ceasing to be an advertising interface (routers only)	-	-	-	-	M	O
	Test v6LC.2.2.9: Processing router solicitations (routers only)	-	-	-	-	M	O
	Test v6LC.2.2.10: Router solicitation processing, neighbour cache (routers only)	-	-	-	-	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	O	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	-	-	-	-	O	O
	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
	Test v6LC.2.2.24: Router advertisement DNS (router only)	-	-	-	-	M	O
	Test v6LC.2.2.25: Processing router advertisement DNS (host only)	-	-	-	O	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

DRAFT FOR PUBLIC COMMENT

Table F.2. Section 2 - RFC 4861 neighbour discovery for IPv6

RFC 4861	Test case	Consumer			Enterprise/ Service provider		
		Host	NE	NSE	Host	NE	NSE
Group 3: Redirect function	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
	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	O
	Test v6LC.2.3.17: Redirect - receive (routers only)	-	-	-	-	M	O

Table F.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 auto configuration and duplicate address detection	Test v6LC.3.1.1: Address autoconfiguration and test	-	-	-	M	M	O
	Test v6LC.3.1.2: Receiving Duplicate Address Detection (DAD) neighbour solicitations and advertisements	-	-	-	M	M	O
	Test v6LC.3.1.3: Validation of DAD neighbour solicitations	-	-	-	M	M	O
	Test v6LC.3.1.4: Validation of DAD neighbour advertisements	-	-	-	M	M	O
	Test v6LC.3.1.5: Receiving neighbour solicitations for address resolution	-	-	-	M	M	O
Group 2: Router advertisement processing and address lifetime	Test v6LC.3.2.1: Global address autoconfiguration and DAD	-	-	-	M	M	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
	Test v6LC.3.2.6: Stable addresses (host only)	-	-	-	M	O	O
	Test v6LC.3.2.7: Resolving DAD conflicts (host only)	-	-	-	M	O	O

DRAFT FOR PUBLIC COMMENT

Table F.4. Section 4 - RFC 8201 path 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 Multicast Listener Discovery (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	O	O
Test v6LC.4.1.9: Checking for increase in PMTU	-	-	-	M	M	M
Test v6LC.4.1.10: Multicast destination - one router	-	-	-	O	O	O
Test v6LC.4.1.11: Multicast destination - two routers	-	-	-	O	O	O
Test v6LC.4.1.12: Validate packet too big	-	-	-	O	O	O

Table F.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	-	-	-	O	O	O
Test v6LC.5.1.2: Replying echo requests	-	-	-	M	M	M
Test v6LC.5.1.3: Destination unreachable message generation	-	-	-	O	O	O
Test v6LC.5.1.4: Packet too big message generation (routers only)	-	-	-	-	O	O
Test v6LC.5.1.5: Hop limit exceeded (time exceeded generation) (routers only)	-	-	-	-	M	O
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	O
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	-	-	-	O	O	O
Test v6LC.5.1.13: Error condition with non-unique source - anycast	-	-	-	-	M	O

DRAFT FOR PUBLIC COMMENT

Annex G
(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		

DRAFT FOR PUBLIC COMMENT

Bibliography

[1] 3rd Generation Partnership Project (3GPP) standards

[2] Special Publication (NIST SP) - 500-267, *A Profile for IPv6 in the U.S. Government - Version 1.0*

[3] Special Publication (NIST SP) - 500-267Ar1, *NIST IPv6 Profile*

[4] Special Publication (NIST SP) - 500-267Br1, *USGv6 Profile*

[5] IDA RS IPv6, *Singapore Internet Protocol version 6 (IPv6) Profile*

DRAFT FOR PUBLIC COMMENT

Acknowledgements

Members of the Numbering and Electronic Addressing Working Group

Working Group Leaders

Ts Azura Mat Salim (Chair)	TM Technology Services Sdn Bhd
Mr Lee Wei Han (Vice Chair I)	Maxis Broadband Sdn Bhd
Dr Navaneethan C. Arjuman (Vice Chair II)	Multimedia University

Drafting Committee Member

The following subject matter experts served as members of the Drafting Committee and involved in the development, drafting, and technical deliberation of this Technical Code:

Dr Navaneethan C. Arjuman (Draft lead)	Multimedia University
Ms Norkhadhra Nawawi (Counsellor)	Malaysian Technical Standards Forum Bhd
Ir Ts Dr Hafizah Zainol Abidin	CelcomDigi Telecommunications Sdn Bhd
Ts Hanaffy Goeffery Ramli	CelcomDigi Telecommunications Sdn Bhd
Ts Salim Mohamad Ghani	Hewlett-Packard Enterprise
Mr Avas Gaire	IPv6 Forum Malaysia
Mr Naresh Sureswaran Naidu	IPv6 Forum Malaysia
Prof Emeritus Sureswaran Ramadass	IPv6 Forum Malaysia
Mr Lee Wei Han	Maxis Broadband Sdn Bhd
Mr Muhammad Faiz Rahmat	SIRIM Berhad
Ts Azura Mat Salim	TM Technology Services Sdn Bhd
Ts Mohd Faizal bin Abd Raup	TM Technology Services Sdn Bhd

Contributors

The following members were not part of the Drafting Committee but supported the development of this Technical Code by participating in the review process and providing technical comments, recommendations, and feedback to enhance the quality and completeness of the Technical Code:

Ms Yemmy Soong	Apple Inc.
Mr Yan Kim Fui	Cisco Systems (M) Sdn Bhd
Mr Samsol Hairi Sameon	Digital Nasional Berhad
Mr See Ler Herng	HONOR Technology (Malaysia) Sdn Bhd
Ms Nur Aziemah Azizan	JIE Business Sdn Bhd
Dr Mohd Mazlan Abdul Razak	TIME dotcom Sdn Bhd
Mr Tan Yaw Han	TIME dotcom Sdn Bhd

DRAFT FOR PUBLIC COMMENT