TECHNICAL CODE

SPECIFICATIONS FOR INTERNET PROTOCOL VERSION 6 (IPv6) COMPLIANT EQUIPMENT

Developed by

Registered by

Registered date:

4 October 2016

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)
4805-2-2, Block 4805, Persiaran Flora
CBD Perdana 2
Cyber 12
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8322 1441/1551
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 organizations:

Celcom Axiata Berhad

Cisco Systems Malaysia

DiGi Telecommunications Sdn Bhd

Huawei Technologies

Jaring Communications Sdn Bhd

Maxis Broadband Sdn Bhd

REDtone IoT Sdn Bhd

Riger Corporation Sdn Bhd

SIRIM QAS International Sdn Bhd

Telekom Malaysia Berhad

TIME dotCom Bhd

FOREWORD

This Technical Code for Specifications for Internet Protocol version 6 (IPv6) Compliant Equipment ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standard Forum Berhad ('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.

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

MCMC MTSFB TC T013:2016

SPECIFICATIONS FOR INTERNET PROTOCOL VERSION 6 (IPv6) COMPLIANT EQUIPMENT

1. Scope

This Technical Code defines the technical requirements for equipment to be IPv6 compliant. The technical requirements cover hardware and software with respect to the following functions:

a) Host/Node:
Host is referring to the 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.

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

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

In the event the equipment is multifunctional, the minimum technical requirement of its primary function shall be fulfilled.

The equipment that shall comply with this technical code are listed in Annex A.

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.

A Profile for IPv6 in the U.S. Government – Recommendations of the National Institute of Standards and Technology, Version 1.0 Special Publication 500-267 by Doug Montgomery, Stephen Nightingale, Sheila Frankel and Mark Carson

Internet Engineering Task Force (IETF) document – (Request for Comments (RFCs) listed in Annex B)

Singapore Internet Protocol version 6 (IPv6) Profile - IDA RS IPv6 Issue 1Rev 2, Jan 2012 USG v6

3rd Generation Partnership Project (3GPP) standard

3. Abbreviations

For the purposes of this Technical Code, the following abbreviation applies

3GPP	3rd Generation Partnership Project
AH	Authentical Header
AP	Access Point
APFW	Application FireWall
API	Application Programming Interface

CBC	Cipher-Block-Chaining
CGA	Cryptographically Generated Address
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol Version 6
DNS	Domain Name System
DS	Differentiated Services
ESP	Encapsulating Security Payload
FDDI	Fiber Distributed Data Interface
FW	Firewall
HMAC	Hash Message Authentication Code
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange Version 2
IP	Internet Protocol
IPS	Intrusion Protection System
IPSec	IP Security
IPTV	Internet Protocol Television
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
LB	Load Balancer
LTE	Long-Term Evolution
MIB	Management Information Base
MIP	Mobile Internet Protocol
MPLS	Multi-Protocol Label Switching
MS	Malaysian Standard
MTU	Maximum Transmission Unit
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
PIM	Protocol Independent Multicast
RFC	Request for Comments
RPC	Remote Procedure Call
RTP	Real-Time Transport Protocol
SHA	Secure Hash Algorithm
SLACC	Stateless Address Autoconfiguration
SNMP	Simple Network Management Protocol
SSM	Single Source Multicast
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WiMAX	Worldwide Interoperability for Microwave Access X

4. Requirements

4.1 General Requirements

4.1.1 Power Supply Requirements

The equipment may be AC or DC powered. For AC powered equipment, the operating voltage shall be 230 V (+ 10%, -6%) and frequency 50 Hz ± 1% as according to MS IEC 60038 or latest requirement by relevant regulatory body. For DC powered voltage, the operating voltage shall be 48 V (Malaysia Standard).

Where external power supply is used, e.g. AC adaptor or battery, it shall not affect the capability of the equipment to meet this specification.

Adaptor must be pre-approved by the relevant regulatory body before it can be used with the equipment.

4.1.2 Power supply cord and mains plug requirements

The equipment shall be fitted with a suitable and appropriate approved power supply cord and mains plug. Both are regulated products and must be pre-approved by the relevant regulatory body before it can be used with the equipment.

The Power Supply Cord shall be certified to:

a) MS 2112-5 or BS EN 50525-2-11 or IEC 60227-5 (PVC insulated – flexible cables/cords);or
b) MS 140 or MS 2127-4 or IEC 60245-1 & IEC 60245-4 (Rubber insulated – flexible cables / cords)

The main plug shall be certified according to:

a) 13 A fused plugs: MS 589: Part 1 or BS 1363: Part 1; or
b) 15 A fused plugs; MS 1577; or
c) 2.5 A, 250 V, flat non-rewirable two-pole plugs: MS 1578 or BS EN 50075.

4.1.3 Electromagnetic compatibility requirements

The equipment shall comply with the limits for conducted disturbance at the mains terminals and telecommunication ports, and the limits for radiated disturbance defined in the MS CISPR 22 and equivalent.

4.1.4 Electrical safety requirements

The equipment shall comply with the MS IEC 60950-1 safety standard and equivalent. The requirements in MS IEC 60950-1 that are applicable to the equipment e.g. class of equipment, type of telecommunication network voltage (TNV) circuit and types of components shall be identified and complied with.

4.1.5 Marking requirements

The equipment shall be marked with the following information:
a) Supplier/manufacturer’s name or identification mark;
b) Supplier/manufacturer’s model or type reference; and
c) other markings as required by the relevant standards

The markings shall be legible, indelible and readily visible.

4.1.6 Language

All markings, software and related documents shall be in Bahasa Melayu or English language.

4.2 Functional Requirements

4.2.1 IPv6 functional requirements are categorized as below:

No	IPv6 Functional	Description
1	IPv6 Basic Capabilities	Fundamental operation and configuration of the Internet Protocol (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 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 generalized multicast and configure options for Single Source Multicast (SSM) capabilities
7	Network Management	Technical requirement for Simple Network Management Protocol (SNMP) and it s Management Information Bases (MIBs)
8	Application Requirement	Technical requirement for network services such as : i. Domain Name System (DNS) ; ii. Dynamic Host Configuration Protocol (DHCP) ; iii. 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 router
11	IP Security	Technical requirement for IPSec and its key management protocol
12	Network Protection Device	Technical requirement: i. Firewall (FW); ii. Application Firewall (APFW); iii. Intrusion Detection System (IDS); iv. Intrusion Protection System (IPS); and v. Session Border Controller (SBC)

The details of its functional are shown in Annex C.

4.2.2 Notation

The following notations are used in the Specification:

M - Mandatory requirement
O - Optional requirement
c(M) - Conditional Mandatory (for specific reason or element)

Annex A
(Normative Reference)

Mandated equipment

A1 Classification

The equipment or element which are subject to this Technical Code are classified as hardware and software as defined in Table A1.

Table A1. List of equipment

Classification	Category	Equipment
Hardware	Terminals	All types of computers; User Equipment (UE)/Mobile Devices with at least 4G support; and IP Phone.
	Network Element	Layer 2 Switch; Layer 3 Switch/Router; and Load Balancer (LB).
	Network Security Element	Firewall (FW); Application Firewall (APFW); Intrusion Protection System (IPS); Intrusion Detection System (IDS); and Session Border Controller (SBC).
	Systems	Domain Name System (DNS); Dynamic Host Configuration Protocol (DHCP); Business Support Systems (BSS); Network Management System (NMS); RADIUS/AAA; Home Location Register (HLR); Home Subscriber Server (HSS); and Policy and Charging Rules Function (PCRF)
	Networked Surveillance System(IP Based)	Closed Circuit Television (CCTV); IP Camera; and Network Management System (NMS).
	Network Peripheral	Residential / HomeGateway (RGW) / (HG); Optical Network Terminal (ONT) / Optical Network Unit (ONU); WiFi Access Point; Femto Access Point; WiMAX Access Point; Broadband Powerline (BPL) Ethernet / Modem; and IPTV Set Top Box (IPTV STB).
	Service Provider System	Broadband Remote Access Server (BRAS); Radio Access Network (NodeB, eNodeB and etc.); Mobility Management Entity (MME); Serving GPRS Support Node (SGSN); GPRS Support Node (GGSN); Serving Gateway (S-GW); and

Classification	Category	Equipment
		Packet Data Network Gateway (P-GW)
	Future Network System	IP Multimedia Subsystem (IMS); Software Defined Networking (SDN); and Network Functions Virtualization (NFV).
Software	Operating System (OS)	IPhone Operations System (IOS); Androids; Windows; Linux; and Mac OS X.
	Middleware	Open Database Connectivity (ODBC); API:Java Database Connectivity (API:JDBC); Open Network Computing RPC (ONC RPC); Open Software foundation RPC (OSF RPC); Remote Method Invocation (RMI); Distributed Computing Environmen (DCE); Common Object Request Broker Architecture(CORBA); and Distributed Component Object Model (DCOM).
	Applications/Services	Web Browser; DNS File Transfer Protocol (DNS FTP); Telnet; Real-Time Transport Protocol (RTP); Network Time Protocol (NTP); and Session-Initiation-Protocol (SIP).

NOTES:

1. Applicable for models (Hardware and Software) released from January 2017**.**
2. Equipment may apply for multiple categories.
3. Equipment may function as Host, NE and/or NSE.

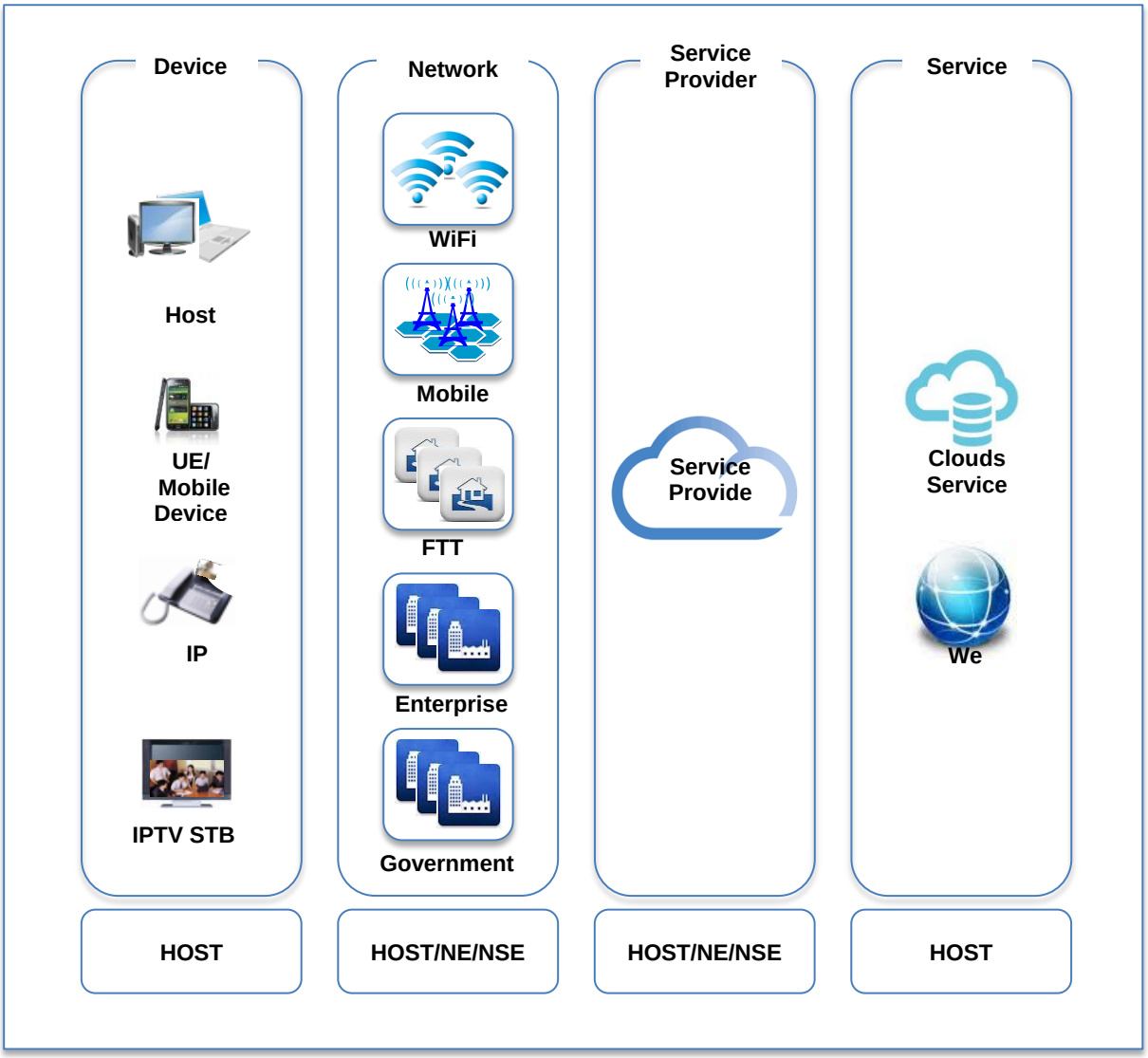

Figure A1. Illustration of equipment listed in Table A1 based on category and function

A2. Function

A2.1 Host

In the figure above, the host for the devices are those elements highlighted. Beside Personal Computer and Servers, host also covers the following items:

A2.1.1 User Equipment (UE) / Mobile Device

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

A2.1.2 DHCP

An IPv6 Node that is deployed as a DHCPv6 Server MUST implement the server requirements specified by RFC 3315, DHCPv6 and should implement IPv6 Prefix Delegation as specified by RFC 3633. RFC 3769 provides additional background on the design of Prefix Delegation.

A2.1.3 DHCP Relay Agent

An IPv6 Node that is deployed as a DHCPv6 Relay Agent must implement the relay agent requirements specified by RFC 3315 and DHCPv6.

A2.2 Network Elements

A.2.2.1 Layer 2 Switch

A switch or 'Layer 2 switch' is a device that is primarily used for forwarding Ethernet frames based on their attributes. Exchanging Ethernet information with other Ethernet switches is usually part of its function.

A.2.2.2 Layer 3 Switch

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

A.2.2.3 Load Balancer (LB)

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

A2.3 Network Security Equipment

Network Security Equipment (NSE) is often also a Layer 2 switch or a Router/Layer 3 switch. NSE comprises of:

a) Firewall (FW);
b) Intrusion Detection System (IDS);
c) Intrusion Protection System (IPS); and
d) Session Border Controller (SBC)

A2.3.1 Firewall (FW)

A firewall is a network security system either hardware- or software- based, that controls incoming and outgoing network traffic based on a set of rules.

A2.3.2 Intrusion Detection System (IDS)

An Intrusion Detection System is a device with software application that monitors network or system activities for malicious activities or policy violations and produces electronic report to a management station.

A2.3.3 Intrusion Protection System (IPS)

An Intrusion Protection System consists of network security appliances that prevents network and/or system from malicious activities, vulnerability and threat.

A2.3.4 Session Border Controller (SBC)

A session border controller is a device regularly deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually there are media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications. Table A2 lists the equipment based on its function.

Table A2. List of equipment based on its function

No	Function	Equipment
1.	Host	All types of computers; User Equipment (UE)/Mobile Devices with at least 4G support; and IP Phone
2.	Network element	Layer 2 Switch; Layer 3 Switch / Routers; WiMAX Gateway; Serving GPRS Support Node (SGSN); Mobility Management Entity (MME); Serving Gateway (SGW); Packet Data Network Gateway (PGW); Policy Control and Enforcement Function (PCEF); Broadband Remote Access Server (BRAS); Multi-Service Access Node (MSAN); Packet Transport Network (PTN); NODE B; E-UTRAN Node B (eNODE B); Base Station, Session 2 Node (GGSN),
3.	Network Security Element (NSE)	Firewalls(FW); Intrusion Prevention System (IPS); Intrusion Detection System (IDS); Application Firewall (AFW)

A3. Segments

Segment for equipment is referring to the IPv6 to be deployed. Three (3) classes of segment, as shown in Figure A2.

A3.1 Mass Network

Mass Network is referring to the retails end uses, whether they are fixed at home, or moving (Mobile & WiFi):

a) Fixed (Home/Residential); and
b) Mobile (3G/LTE/5G).

A3.2 Enterprise

a) Enterprise; and
b) Government Agencies.

A3.3 Service Providers

a) Telcos and Celcos;

b) Network Service Provider; and
c) Internet Service Provider.

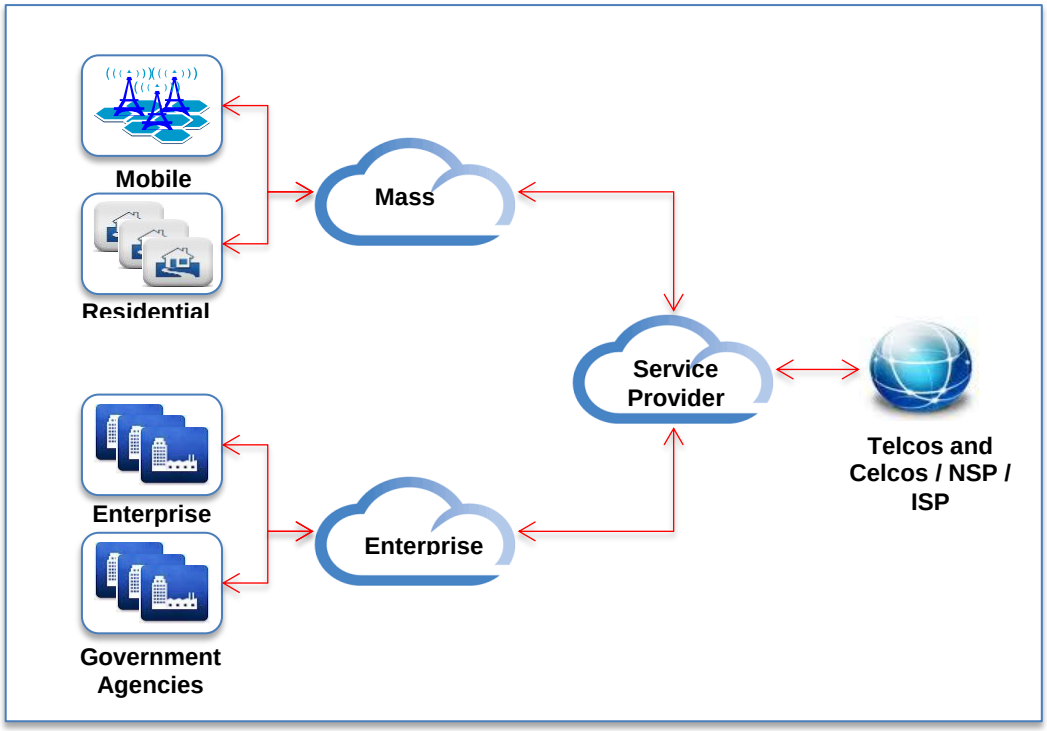

Figure A2 .The three classes of segment

Annex B
(Normative Reference)

List of Request for Comments

Table B1. List of Request for Comments (RFCs)

No	RFC	List of RFC
1	RFC 1195	Use of OSI Intermediate System to Intermediate System (IS-IS) for Routing in TCP/IP and Dual Environments
2	RFC 1772	Application of the Border Gateway Protocol in the Internet
3	RFC 1981	Path MTU Discovery for IP version 6
4	RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
5	RFC 2410	The NULL Encryption Algorithm and Its Use With IPsec
6	RFC 2451	The Encapsulating Security Payload (ESP) CBC-Mode Cipher Algorithms
7	RFC 2460	Internet Protocol Version 6 (IPv6) Specification
8	RFC 2464	Transmission of IPv6 Packets over Ethernet Networks
9	RFC 2467	Transmission of IPv6 Packets over FDDI Networks
10	RFC 2473	Generic Packet Tunneling in IPv6
11	RFC 2474 (PS)	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
12	RFC 2475 (INF)	An Architecture for Differentiated Services
13	RFC 2491	IPv6 over Non-Broadcast Multiple Access (NBMA) networks
14	RFC 2492	IPv6 over Asynchronous Transfer Mode (ATM) Networks
15	RFC 2497	Transmission of IPv6 Packets over ARCnet Networks
16	RFC 2507	IP Header Compression
17	RFC 2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links
18	RFC 2526	Reserved IPv6 Subnet Anycast Addresses
19	RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
20	RFC 2590	Transmission of IPv6 Packets over Frame Relay Networks Specification
21	RFC 2597 (PS)	Assured Forwarding PHB Group
22	RFC 2671	Extension Mechanisms for DNS (EDNS0)
23	RFC 2675	IPv6 Jumbograms
24	RFC 2710	Multicast Listener Discovery (MLD) for IPv6
25	RFC 2711	IPv6 Router Alert Option
26	RFC 2740	Open Shortest Path First (OSPF) for IPv6
27	RFC 2765	Stateless IP/ICMP Translation Algorithm (SIIT)
28	RFC 2784	Generic Routing Encapsulation (GRE)
29	RFC 2983 (INF)	Differentiated Services and Tunnels
30	RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
31	RFC 3086 (INF)	Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification

No	RFC	List of RFC
32	RFC 3095	RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed
33	RFC 3140 (PS)	Per Hop Behavior Identification Codes
34	RFC 3146	Transmission of IPv6 Packets over IEEE 1394 Networks
35	RFC 3168 (PS)	The Addition of Explicit Congestion Notification (ECN) to IP
36	RFC 3173	IP Payload Compression Protocol (IPComp)
37	RFC 3226	DNSSEC and IPv6 A6 aware server/resolver message size requirements
38	RFC 3241	Robust Header Compression (ROHC) over PPP
39	RFC 3246 (PS)	An Expedited Forwarding PHB (Per-Hop Behavior)
40	RFC 3247 (INF)	Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)
41	RFC 3260 (INF)	New Terminology and Clarifications for Diffserv
42	RFC 3289	Management Information Base (MIB) for the Differentiated Services Architecture
43	RFC 3306	Unicast-Prefix-based IPv6 Multicast Addresses
44	RFC 3307	Allocation Guidelines for IPv6 Multicast Addresses
45	RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
46	RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
47	RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
48	RFC 3413	Simple Network Management Protocol (SNMP) Applications
49	RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
50	RFC 3484	Default Address Selection for Internet Protocol version 6 (IPv6)
51	RFC 3493	Basic Socket Interface Extensions for IPv6
52	RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
53	RFC 3542	Advanced Socket Application Program Interface (API) for IPv6
54	RFC 3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
55	RFC 3572	Internet Protocol Version 6 over MAPOS (Multiple Access Protocol Over Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH))
56	RFC 3590	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
57	RFC 3596	DNS Extensions to Support IP Version 6
58	RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec
59	RFC 3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
60	RFC 3678	Socket Interface Extensions for Multicast Source Filters
61	RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
62	RFC 3736	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
63	RFC 3769	Requirements for IPv6 Prefix Delegation
64	RFC 3775	Mobility Support in IPv6

No	RFC	List of RFC
65	RFC 3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
66	RFC 3843	RObust Header Compression (ROHC): A Compression Profile for IP
67	RFC 3879	Deprecating Site Local Addresses
68	RFC 3948	UDP Encapsulation of IPsec ESP Packets
69	RFC 3956	Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
70	RFC 3963	Network Mobility (NEMO) Basic Support Protocol
69	RFC 3971	SEcure Neighbor Discovery (SEND)
70	RFC 3972	Cryptographically Generated Addresses (CGA)
71	RFC 3986	Uniform Resource Identifier (URI) Generic Syntax
72	RFC 4007	IPv6 Scoped Address Architecture
73	RFC 4022	MIB for the Transmission Control Protocol (TCP)
74	RFC 4038	Application Aspects of IPv6 Transition
75	RFC 4087	IP Tunnel Management Information Base (MIB)
76	RFC 4106	The Use of Galois/Counter Mode (GCM)in IPsec Encapsulating Security Payload (ESP)
77	RFC 4113	MIB for the User Datagram Protocol (UDP)
78	RFC 4191	Default Router Preferences and More-Specific Routes
79	RFC 4193	Unique Local IPv6 Unicast Addresses
80	RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
81	RFC 4271	A Border Gateway Protocol 4 (BGP-4)
82	RFC 4282	The Network Access Identifier
83	RFC 4283	Mobile Node Identifier option for Mobile IPv6 (MIPv6)
84	RFC 4291	IP Version 6 Addressing Architecture
85	RFC 4292	IP Forwarding Table Management Information Base (MIB)
86	RFC 4293	Management Information Base (MIB) for the Internet Protocol (IP)
87	RFC 4295	Mobile IPv6 Management Information Base (MIB)
88	RFC 4301	Security Architecture for the IP/ Tunnelling of Explicit Congestion Notification
89	RFC 4302	IP Authentication Header
90	RFC 4303	IP Encapsulating Security Payload (ESP)
91	RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
92	RFC 4308	Cryptographic Suites for IPsec
93	RFC 4309	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)
94	RFC 4338	Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel
95	RFC 4361	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
96	RFC 4362	RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP
97	RFC 4380	BGP Extended Communities Attribute

No	RFC	List of RFC
98	RFC 4434	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
99	RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
100	RFC 4489	A Method for Generating Link-Scoped IPv6 Multicast Addresses
101	RFC 4543	The Use of Galois Message Authentication Code (GMAC) in IPsec Encapsulating Security Payload (ESP) and AH
102	RFC 4552	Authentication/Confidentiality for OSPFv3
103	RFC 4581	Cryptographically Generated Addresses (CGA) Extension Field Format
104	RFC 4584	Extension to Sockets Application Program Interface (API) for Mobile IPv6
105	RFC 4594 (INF)	Configuration Guidelines for DiffServ Service Classes
106	RFC 4601	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
107	RFC 4604	Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
108	RFC 4607	Source-Specific Multicast for IP
109	RFC 4609	Protocol Independent Multicast - Sparse Mode (PIM-SM): Multicast Routing Security Issues and Enhancements
110	RFC 4659	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
112	RFC 4760	Multiprotocol Extensions for BGP-4
112	RFC 4798	Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)
113	RFC 4807	IPsec Security Policy Database Configuration Management Information Base (MIB)
114	RFC 4809	Requirements for an IPsec Certificate Management Profile
115	RFC 4815	RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095
116	RFC 4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
117	RFC 4861	Neighbor Discovery for IP version 6 (IPv6)
118	RFC 4862	IPv6 Stateless Address Autoconfiguration
119	RFC 4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
120	RFC 4869	Suite B Cryptographic Suites for IPsec
121	RFC 4877	Mobile IPv6 (MIPv6) Operation with Internet Key Exchange Version 2 (IKEv2) and Revised IPsec Architecture
122	RFC 4884	Extended ICMP to Support Multi-Part Messages
123	RFC 4890	Recommendations for Filtering ICMPv6 Messages in Firewalls
124	RFC 4891	Using IPsec to Secure IPv6-in-IPv4 Tunnels
125	RFC 4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6
126	RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
127	RFC 4945	The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

No	RFC	List of RFC
128	RFC 4982	Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)
129	RFC 4995	The RObust Header Compression (ROHC) Framework
130	RFC 4996	RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)
131	RFC 5014	IPv6 Socket Application Program Interface (API) for Source Address Selection
132	RFC 5015	Bidirectional Protocol Independent Multicast (BIDIR-PIM)
133	RFC 5059	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
134	RFC 5072	IP Version 6 over Point-to-Point Protocol (PPP)
135	RFC 5095	Deprecation of Type 0 Routing Headers in IPv6
136	RFC 5114	Additional DH Groups for Use with IETF Standards
137	RFC 5121	Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks
138	RFC 5175	IPv6 Router Advertisement Flags Option
139	RFC 5187	OSPFv3 Graceful Restart
140	RFC 5213	Proxy Mobile IPv6
141	RFC 5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
142	RFC 5329	Traffic Engineering Extensions to OSPF Version 3
143	RFC 5380	Hierarchical Mobile IPv6 (HMIPv6) Mobility Management
144	RFC 5555	Mobile IPv6 Support for Dual Stack Hosts and Routers
145	RFC 5569	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)
146	RFC 5701	IPv6 Address Specific BGP Extended Community Attribute
147	RFC 5838	Support of Address Families in OSPFv3
148	RFC 5844	IPv4 Support for Proxy Mobile IPv6
149	RFC 5952	A Recommendation for IPv6 Address Text Representation
150	RFC 5969	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) - Protocol Specification
151	RFC 5996	Internet Key Exchange Version 2 (IKEv2) Protocol
152	RFC 6040	Tunneling of Explicit Congestion Notification
153	RFC 6052	IPv6 Addressing of IPv4/IPv6 Translators
154	RFC 6085	Address Mapping of IPv6 Multicast Packets on Ethernet
155	RFC 6146	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
156	RFC 6333	Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion

Note: a) PS – Proposed Standard
b) INF - Information

Annex C
(Normative Reference)

IPv6 Functional Requirements

Table C1. IPv6 Basic Requirement

IETF Specification	IPv6 Basic Requirement	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2460	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 & unrecognized 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 1981	Path MTU Discovery for IPv6	-	M	M	-	-	M	M	-	-	M	M	M
	Discovery Protocol Requirements	-	M	M	-	-	M	M	-	-	M	M	M
RFC 2675	IPv6 Jumbograms	-	O	O	-	-	-	-	-	-	-	-	-
RFC 4861	Neighbor 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	DuplicateAddress Detection	-	M	M	-	-	M	M	-	-	M	M	M
	Neighbor 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	-	-	-	-	-	-	-	-	-

IETF Specification	IPv6 Basic Requirement	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4191	Default Router Preference	-	-	-	-	-	-	-	-	-	-	-	M
RFC 3971	Secure Neighbor Discovery	-	M	M	-	-	M	M	-	-	M	M	M
RFC 4862	IPv6 Stateless Address Autoconfig	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
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	-	SLACC	M	M	M
RFC 3315	Dynamic Host Config Protocol (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 C2. IPv6 Addressing Requirement

IETF Specification	IPv6 Addressing Requirement	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 3484	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	Cryptographically Generated Addresses (CGA)	Condition[1]	c(M)	c(M)	-	Condition[1]	c(M)	c(M)	-	Condition[1]	c(M)	c(M)	-
RFC 4581	CGA Extension Field Format	Condition[1]	c(M)	c(M)	-	Condition[1]	c(M)	c(M)	-	Condition[1]	c(M)	c(M)	-
RFC 4982	CGA Support for Multiple Hash Algos	Condition[1]	c(M)	c(M)	-	Condition[1]	c(M)	c(M)	-	Condition[1]	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	-

[1] 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 C3. Transition Mechanism Requirements

IETF Specification	Transition Mechanism Requirement	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 IPv6 Provider Edge Routers(6PE)	-	-	-	-	IPv4, MPLS	-	M	-	IPv4, MPLS	-	M	-
RFC 4659	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 tunneling 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 2765	Stateless IP/ICMP Translation Algorithm (SIIT)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5569	6RD	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5969	6RD with PD	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2784	Generic Routing Encapsulation	-	-	O	-	-	-	O	-	-	-	O	-

Table C4. Link Specific Requirements

IETF Specification	Link Specific Requirement	Mass Network				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2497	IPv6 over ARCnet	-	O	O	O	-	O	O	O	-	O	O	O
RFC 2590	IPv6 over Frame Relay	-	O	O	O	-	O	O	O	-	O	O	O
RFC 2464	IPv6 over Ethernet	Condition[2]	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 2492	IPv6 over ATM	-	M	M	M	-	M	M	M	-	M	M	M
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	IP Payload Compression Protocol (IPComp)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4995	Robust Header Compression (ROHC) framework	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4996	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	-	-	-	-	-	-	-	-	-	-	-	-

[2] Applicable when the specified link technology is chosen as preferred choice

Table C5. Routing Protocol Requirements

IETF Specification	Routing Protocol Requirement	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2740	OSPF for IPv6	-	-	-	-	Condition[3]	-	M	M	Condition[3]	-	M	M
RFC 4552	Authentication/Confidentiality for OSPFv3	-	-	-	-	Condition[3]	-	M	-	Condition[3]	-	M	-
RFC 1195	Use of OSI IS- IS for Routing in TCP/IP and Dual Environtments	-	-	-	-	-	-	-	-	Condition[3]	-	M	-
RFC 5187	OSPFv3 Graceful Restart	-	-	-	-	-	-	-	-	-	-	M	-
RFC 5329	Traffic Engineering Extensions to OSPF Version 3												
RFC 5838	Support of Address Families in OSPFv3	-	-	-	-	-	-	-	-	-	-		-
	RIPng Protocol Applicability Statement	-	-	-	-	Condition[3]	-	c(M)	-	Condition[3]	-	M	-
RFC 4271	Border Gateway Protocol 4 (BGP-4)	-	-	-	-	Condition[3]	-	c(M)	-	Condition[3]	-	M	
RFC 1772	BGP Application in the Internet	-	-	-	-	Condition[3]	-	M	-	Condition[3]	-	M	
RFC 4760	BGP Multi Protocol Extensions	-	-	-	-	Condition[3]	-	M	-	Condition[3]	-	M	
RFC 2545	BGP Multi-Protocol Extensions for IPv6 IDR	-	-	-	-	Condition[3]	-	M	-	Condition[3]	-	M	
RRC 4659	BGP MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN	-	-	-	-	-	-	-	-	-	-	M	-
RFC 5701	IPv6 Address Specific BGP Extended Community Attribute	-	-	-	-	-	-	-	-	-	-	-	-

[3] For IGP; For hardware FW

Table C6. Multicasting Requirements

IETF Specification	Multicasting Requirement	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2710	Multicast Listener Discovery (MLD) for IPv6	Condition[4]	M	M	-	Condition[4]	M	M	-	Condition[4]	M	M	-
RFC 3590	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol	Condition[4]	M	M	-	Condition[4]	M	M	-	Condition[4]	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 (SSM)	PIM-SSM	M	M	-	PIM-SSM	M	M	-	PIM-SSM	M	M	-
RFC 4601	PIM Sparse Mode (SM)	PIM-SSM	-	M	-	PIM-SSM	-	M	-	PIM-SSM	-	M	-
RFC 4609	PIM-SM Security Issues / Enhancements	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3956	Embedding Rendezvous Point (RP) Multicast Addr	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4489	A Method for generating link-scoped IPv6 Multicast Address	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5059	Bootstrap Router (BSR) Mechanism for PIM	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5015	BiDirectional Protocol Independent Multicast (BIDIR-PIM)	-	-	-	-	-	-	-	-	-	-	-	-

[4] When Group Management Capability is Required -IGMP

Table C7. Network Management Requirements

IETF Specification	Network Management Requirement	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
	Network Management Requirements	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3411	SNMP v3 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 Mobile IPv6	-	-	-	-	SNMP & MIP	-	M	-	SNMP & MIP	-	M	-
RFC 3289	MIB for DiffServ	-	-	-	-	SNMP & DS	-	M	-	SNMP & DS	-	M	-

Table C8. Application Requirements

IETF Specification	Application Requirement	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 3596	DNS Extensions for IPv6	Condition[5]	M	M	M	Condition[5]	M	M	M	Condition[5]	M	M	M
RFC 2671	Extension Mechanisms for DNS (EDNS0)	Condition[5]	M	M	M	Condition[5]	M	M	M	Condition[5]	M	M	M
RFC 3226	DNSSEC and IPv6 DNS MSG Size Reqs	Condition[6]	M	M	M	Condition[6]	M	M	M	Condition[6]	M	M	M
RFC 3986	URI: Generic Syntax	Condition[7]	M	M	M	Condition[7]	M	M	M	Condition[7]	M	M	M
RFC 3493	Basic Socket API for IPv6	Condition[8]	M	-	-	Condition[8]	M	-	-	Condition[8]	M	-	-
RFC 3542	Advanced Socket API for IPv6	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4584	Extension to Sockets API for Mobile IPv6	-	-	-	-	-	-	-	-	-	-	-	-
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[9]	M	M	M	Condition[9]	M	M	M	Condition[9]	M	M	M

[5] Device supports DNS
[6] Device supports DNSSEC
[7] Device supports URIs
[8] Device has exposed APIs
[9] Device supports DHCP

Table C9. Mobility Requirements

IETF Specification	Mobility Requirement	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 3775	Mobility Support in IPv6	MIPv6	M	M	-	MIPv6	M	M	-	MIPv6	M	M	-
RFC 3963	Network Mobility (NEMO) Basic Support in IPv6	NEMO	-	M	-	NEMO		M	-	NEMO		M	-
RFC 4282	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 IPse Architecture	MIPv6	M	M	-	MIPv6	M	M	-	MIPv6	M	M	-
RFC 5213	Proxy Mobile IPv6	PMIPv6		M	-	PMIPv6		M	-	PMIPv6		M	-
RFC 5380	Hierarchical Mobile IPv6 scheme	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5555	Mobile IPv6 Support for Dual Stack Hosts And Routers	-	-	-	-	-	-	-	-	-	-	-	-
RFC 5844	IPv4 Support for Proxy Mobile IPv6	-	-	-	-	-	-	-	-	-	-	-	-

Table C10. Quality of Service Requirements

IETF Specification	Quality of Service Requirement	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 2474 (PS)[a]	(DiffServ Header Field)	Condition[10]	M	M	-	DS	M	M	-	DS	M	M	-
RFC 3140 (PS)[a]	(PHB Encoding – DiffServ)	Condition[10]	M	M	-	DS	M	M	-	DS	M	M	-
RFC 3168 (PS)[a]	(Explicit Congestion Notification, ECN)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2597 (PS)[a]	(Assured Forwarding)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3246 (PS)[a]	(Expedited Forwarding)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3247 (INF)[b]	(Supplementary EF PHB)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2475 (INF[b]	(DiffServ Architecture)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3260 (INF)[b]	(New Term & Clarification - DiffServ)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2983 (INF)[b]	(DiffServ and Tunnels)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4594 (INF)[b]	(Config guidelines DiffServ)	-	-	-	-	-	-	-	-	-	-	-	-
RFC 3086 (INF)[b]	(DiffServ per Domain Behaviour)	-	-	-	-	-	-	-	-	-	-	-	-

[10] DS and Managed service
[a] PS – Proposed Standard
[b] INF - Information

Table C11. IPv6 Security Requirement

IETF Specification	IPv6 Security Requirement	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 4307	Cryptographic Algorithms for IKEv2	-	M	M	M	-	M	M	M	-	M	M	M
	Transition Mechanisms Requirements	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4213	Transition Mechanise for Hosts & Routers	-	M	M	-	-	M	M	-	-	M	M	-
RFC 4891	Using IPsec to Secure IPv6-in IPv4 Tunnels	Condition[11]	c(M)	c(M)	-	Condition[11]	c(M)	c(M)	-	Condition[11]	c(M)	c(M)	-
RFC 2473	Generic Packet Tunneling in IPv6	Condition[11]	c(M)	c(M)	-	Condition[11]	c(M)	c(M)	-	Condition[11]	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 Firewalls	-	-	-	M	-	-	-	M	-	-	-	M
	IPsec-v3	-		-	-	-	-	-	-	-	-	-	-
RFC 4301/ RFC 6040	Security Architecture for theIP/ Tunnelling of Explicit Congestion Notification	-	M	-	-	-	-	-	-	-	-	-	-
RFC 4303	Encapsulating Security Payload	-	M	-	-	-	-	-	-	-	-	-	-
RFC 4302	Authentication Header (AH)	-	M	-	-	-	-	-	-	-	-	-	-
RFC 3948	UDP Encapsulation of ESP Packets	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4835	Cryptographic Algorithms for ESP and AH	-	M	-	-	-	-	-	-	-	-	-	-

[11] Tunneling transition

IETF Specification	IPv6 Security Requirement	Mass				Enterprise				Service Provider			
		Condition	Host	NE	NSE	Condition	Host	NE	NSE	Condition	Host	NE	NSE
RFC 4308	Cryptographic Suites for IPsec	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4869	Suite B Cryptographic Suites for IPsec	-	-	-	-	-	-	-	-	-	-	-	-
RFC 4809	Requirements for an IPsec Cert Mgmnt Profile	-	-	-	-	-	-	-	-	-	-	-	-
	IKEv2	-				-				-			
RFC 5996	Internet Key Exchange (IKEv2) Protocol	-	M	M	M	-	M	M	M	-	M	M	M
RFC 4307	Cryptographic Algorithms for 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	-	-	-	-	-	-	-	-	-	-	-	-
	Uses of Cryptographic Algorithms	-	-	-	-	-	-	-	-	-	-	-	-
RFC 2410	NULL Encryption	-	M	M	M	-	M	M	M	-	M	M	M
RFC 4835	Cryptographic Algorithms for ESP and AH	-	M	M	M	-	M	M	M	-	M	M	M

Table C12. Network Security Equipment Requirements

NIST SP500-267[3]	Network SecurityRequirement	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 authorization	-	-	-	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	Tunneled 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
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

Acknowledgement

Committee of the workshop on the IPv6 technical document development 2014:

Mr. Zaharin Mohd Nadzri (Leader)	Celcom Axiata Berhad
Ms. Yuzie Aznita Mat Yasin	SIRIM QAS International Sdn Bhd
Mr. Nicholas Eddy	Cisco System Inc.
Mr. Now Chieng Juan	DiGi Telecommunication Sdn Bhd
Mr. Wang Xiaolei	Huawei Technologies Co. Ltd
Mr. Shahrizal Sidin	Jaring Communications Sdn Bhd
Mr. Chris Ng Chin Cheng	Maxis Broadband Sdn Bhd
Mr. Muhammad Alqaf Azmi	Riger Corporation (M) Sdn Bhd
Mr. Ahmad Faizain Pardi/	SIRIM QAS International Sdn Bhd
Ms. Fauziah Fadzil /	
Ms. Khairunnisa Ab Halim/	
Mr. Wan Iidil Abdul Rahman	
Ms. Raja Nor Suha Raja Shahrul Zaman	Telekom Malaysia Berhad
Mr. Victor Ong Wai Kit	Time dotCom. Berhad