Telecommunications Standards Advisory Committee (TSAC)

Singapore Internet Protocol Version 6 (IPv6) Profile

IDA RS IPv6
Issue 1 Rev 2, Jan 2012

Infocomm Development Authority of Singapore
Resource Management & Standards
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438

Acknowledgement

The Infocomm Development Authority of Singapore (IDA) and the Telecommunications Standards Advisory Committee (TSAC) would like to acknowledge the United States Government efforts to prepare for United States Government IPv6 (USGv6) Profile; which we have referenced to prepare for Singapore IPv6 Profile. We would also appreciate the following members of the Technical Committee Working Group 5 (TSTC WG5) for their invaluable contributions to the preparation of this profile:

Chairman : Mr Vincent Lim Sok Seng, Singapore Telecommunications Ltd

No.	Organization	Name
1	A10 Networks, Inc	Mr James Wong
2		Mr Tee Soo Kiat
3	A*Star Computational Resource Centre	Mr Derrick Lau Kah Choy
4		Mr Chua Jen Sen
5	A*Star ISTD	Mr Lim Swee Teck
6	Alcatel-Lucent Singapore Pte Ltd	Mr Lau Kok Khiang
7		Mr Jonathan Lee
8		Mr Lim Peng Koon
9	Cisco Systems (USA) Pte Ltd	Mr Lee Kok Keong
10	Ericsson Telecommunications Pte Ltd	Mr Visut Angkasuwan
11		Mr Henry Jia
12	Huawei International Pte Ltd	Mr Mak Fey Loong
13	IDA	Mr Albert Pichlmaier
14		Mr Andy Ho
15		Mr Wee Meng Teo
16		Mr Neo Hock Tea
17		Mr Ter Kwee Leng
18		Ms Ong Ling Ling
19	Institute of Bioengineering & Nanotechnology (IBN)	Mr Lim Kok Hua
20	Juniper Networks	Mr Dayan Ng
21	Microsoft Singapore Pte Ltd	Mr Chew Tat Leong
22	M1 Limited	Mr Mak Beng Yin
23	M1 Connect Pte Ltd	Mr Freddi Hamdani
24	Nanyang Polytechnic	Mr Kan Siew Leong
25	Nanyang Technological University	Assoc Prof Ng Chee Hock
26		Assoc Prof Lee Bu Sung
27		Mr Xia Yang
28	NTT Singapore Pte Ltd	Mr Masashi Miura
29	Nucleus Connect Pte Ltd	Mr Jonathan Tse Chi Hang
30	Progreso Network (s) Pte Ltd	Mr Victor Tang
31		Mr Wong Khing Chong
32	Red Hat Asia Pacific Pte Ltd	Mr Harish Pillay
33		Mr Ng Hak Beng
34	Singapore Telecommunications Ltd	Mr Stephen Debrass
35	Starhub Ltd	Mr Choy Kum Hoong
36		Ms Wee Meng Sie
37	Tech Mahindra Limited	Mr Raj Sahakari
38		Mr Mannu Kaira
39	Tech Mahindra (Singapore) Pte Ltd	Mr Manoj Bhatia

Telecommunications Standards Advisory Committee (TSAC)

TSAC is responsible for the strategic direction, work programmes and procedures for standards-setting, and acts as the advisory body to IDA in meeting the needs of all stakeholders.

TSAC is supported by a Technical Committee (TSTC), where professional, trade and consumers' interest in information and communications is represented by a wide sector of the info-communications industry, comprising network operators, equipment suppliers and manufacturers, academia and researchers, professional bodies and other government agencies.

Membership

TSAC Chairman:

Mr Raymond Lee	Director (Resource Management & Standards), Infocomm Development Authority of Singapore

TSAC Members:

Mr Lim Yuk Min (TSAC Vice-Chairman)	Deputy Director (Resource Management and Standards), Infocomm Development Authority of Singapore
Mr Darwin Ho Kang Ming	Vice President, Association of Telecommunications Industry of Singapore
Mr Lim Chin Siang	Director (IT & Technologies), Media Development Authority
Mr Patrick Scodeller	Chief Technical Officer, M1 Limited
Assoc Prof Li Kwok Hung	Nanyang Technological University, School of Electrical & Electronic Engineering
Prof Ko Chi Chung	National University of Singapore, Department of Electrical & Computer Engineering
Assoc Prof Tham Chen Khong	National University of Singapore, Department of Electrical & Computer Engineering
Mr Simon Smith	Senior Manager Regulatory, Pacnet Internet (S) Ltd
Mr Edwin Lok	Manager (Engineering), Pacnet Internet (S) Ltd
Mr Lee Siak Kwee	Director (Mobile Network Access), Singapore Telecommunications Ltd
Mr Tan Seow Nguan	Director (Network System Engineering), Singapore Telecommunications Ltd
Mr Lim Cheow Hai	Director (Access Engineering), Singapore Telecommunications Ltd
Mr Soh Keng Hock	Director (Private IP Engineering & VAS), Singapore Telecommunications Ltd

Mrs Leong Suet Mui	Principal Technical Executive, Standards Division, Spring Singapore
Mr Peter Cook	VP (Network Mobile Technology and Planning Group), StarHub Ltd
Mr Mah Chin Paw	The Institution of Engineers, Singapore, AGM (Guthrie Engineering (S) Pte Ltd)
Mr Leong Mun Yuen	CTO and Director, Technology & Planning Group Infocomm Development Authority of Singapore
Ms Woo Yim Leng	Senior Manager, Infocomm Development Authority of Singapore

Contents

This Reference Specification is a living document which is subject to review and revision.

Reference Specifications and Guides are informative documents and are not used for approval of customer equipment. They are either one of the following types of documents:

Informative and interim documents on customer equipment standards which are yet to be adopted by network operators; or

Informative documents describing network standards adopted by the public telecommunication networks in Singapore.

Singapore Internet Protocol Version 6 (IPv6) Profile

1. Purpose and Scope

This Profile has been prepared for Singapore Government Agencies, Enterprise, Residential users and Network Providers; taking reference from United Stated Government IPv6 (USGv6) profile[1][1]. The purpose of Singapore IPv6 Profile is to identify the IPv6 capabilities so as to assist Singapore Government Agencies, Enterprise and Network Providers in the development of specific acquisition and deployment plans. This Profile is NOT designed for transition guide and policies. The objective is to define an unambiguous "working language" with respect to the suite of international standards defining IPv6 (i.e. Internet Engineering Task Force's Request for Comments, IETF RFCs). This assists in assuring quality deployment outcomes.

This Profile defines the basic configuration options for IPv6 capability requirements of specific procurement. Government agencies, enterprise and network providers are expected to work closely with their hardware and software vendors to further revise the specification to meet their requirement.

2. IPv6 Deployment Consideration

One of the key considerations in planning for IPv6 deployment is to ensure co-existence and interoperability with the existing IPv4 infrastructure. The requirements captured in this document are taken from the following IETF specifications for addressing issues of specific deployment and transition scenario for Enterprise and ISPs.

Enterprise Networks:
[RFC4057] IPv6 Enterprise Network Scenarios
[RFC4852] IPv6 Enterprise Network Analysis - IP Layer 3 Focus
[RFC3750] Unmanaged Networks IPv6 Transition Scenarios
[RFC3904] Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks

ISPs and Transit Network Infrastructure:
[RFC4029] Scenarios and Analysis for Introducing IPv6 into ISP Networks
[RFC2185] Routing Aspects of IPv6 Transition

Interoperation with IPv4 Infrastructure:
[RFC4038] Application Aspects of IPv6 Transition
[RFC4213] Basic Transition Mechanisms for IPv6 Hosts and Routers

Security Issues:
[RFC4942] IPv6 Transition/Co-existence Security Considerations
[RFC4864] Local Network Protection for IPv6

3. IPv6 Functional Category

IPv6 capabilities can be defined into several categories as shown below:

i. IPv6 Basic Capabilities
Fundamental operation and configuration of the Internet Protocol (IP) layer

ii. Addressing
Technical requirement for IPv6 address architecture and Cryptographically Generated Addresses (CGAs)

iii. IP Security
Technical requirement for IPSec and its key management protocol

[1] http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

iv. Application Requirement
Technical requirement for network services such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and Socket Application Programming Interface (API)

v. Routing Protocols
Technical requirement for interior and exterior gateway protocol

vi. Transition Mechanisms
Technical requirement to adopt IPv6 in existing IPv4 infrastructure

vii. Network Management
Technical requirement for Simple Network Management Protocol (SNMP) and its Management Information Bases (MIBs)

viii. Multicasting
Technical requirement for generalized multicast and configure options for Single Source Multicast (SSM) capabilities

ix. Mobility
Technical requirement for Mobile IP (MIP) and configure options for Network Mobility (NEMO)

x. Quality of Service
Technical requirement for Differentiated Service (DS) mechanisms in router

xi. Network Protection Device
Technical requirement for Firewall (FW), Application Firewall (APFW), Intrusion Detection System (IDS) and Intrusion Protection System (IPS)

xii. Link Specific
Technical requirement for different link layer technologies

4. IPv6 Capabilities Check List

The requirement levels of IPv6 capabilities defined in terms of functional categories stated in section 3 can be classified into Must (M), Should (S) and Option (O).

There is also conditional case for configuration options with the notation of c(x) where x is M, S or O. Refer to Annex 5 for an example, if 6PE is configured, then RFC4271 (BGP-4) is required at the network provider's router with level M, the notation is c(M). If the conditional is not met, by default the requirement level will be O. If there is no notation, then it implies that the requirement level is undefined or not applicable as of dated 1st Nov 2010.

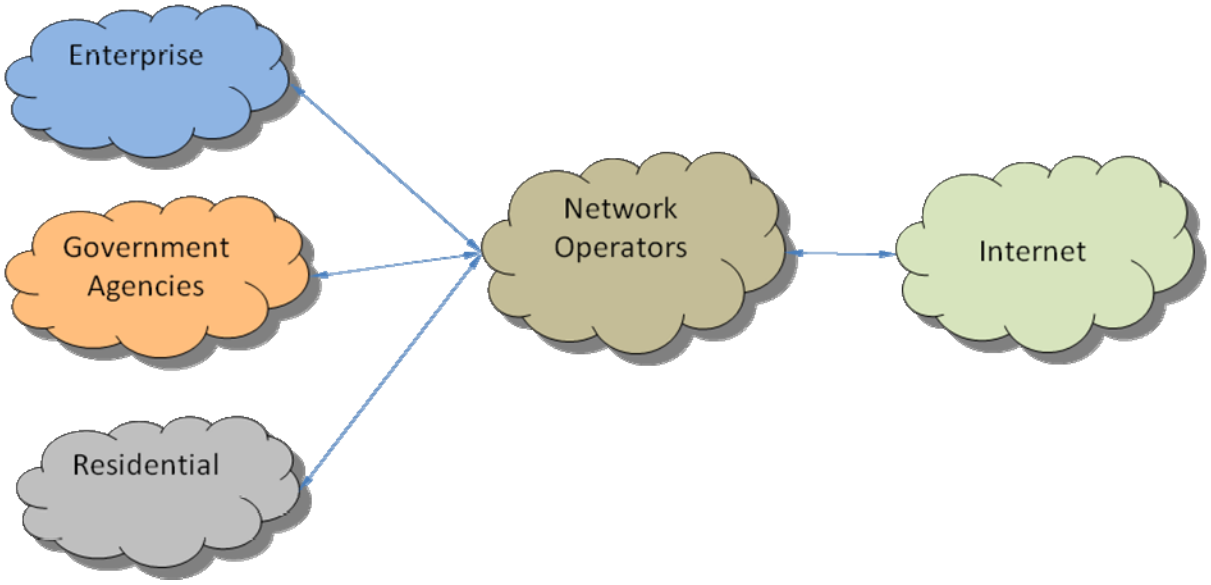
The IPv6 capabilities are covered over are three types of devices: Hosts, Routers and Network Protection Devices, defined as:

i. **Host:** A Host's primary purpose is to support application protocols that are the source and/or destination of IP layer communication such as Personal Computer, Server, etc.

ii. **Router:** A Router's primary purpose is to support the control protocols necessary to enable interconnection of distinct IP sub-networks by IP layer packet forwarding.

iii. **Network Protection Device (NPD):** Firewalls or Intrusion Detection / Prevention devices that examine and selectively block or modify network traffic.

The table in Annex 1- 12 provides the recommended requirement levels of IPv6 capabilities for Host, Routers and NPD at Residential's, Enterprises' & Government Agencies' and Network Operators' Infrastructure.



5. How to Interpret Annex 1 – 12 using Examples

For network providers

Network providers may want to refer to the requirements listed for their procurement tender specification of new service and network audit check for existing service. Network provider may also refer to the column for Residential and Government Agencies & Enterprise requirements if they are offering end-to-end managed services. The network providers may interpret that the requirement level "M" is the basic fundamental requirement for the selected IPv6 functional categories and the requirement levels "S" and "O" are the added-value functions. Some of the added-value functions may require extra cost depending on software and/or hardware vendors' solution and product.

For Government Agencies & Enterprises

Government Agencies and Enterprises may want to refer to the requirements listed for their procurement tender specification of new infrastructure and network audit check for existing infrastructure both for own internal traffic consumption and/or to offer as an e-Service.

For Vendors

Both hardware and software vendors may want to interpret the requirement level "M" as the minimal feature in their solutions and/or product.

6. Feedback

Industries and Government Agencies are encouraged to work with hardware and/or software vendors during tendering phase or technical pilot trial to revise the specification. We will continue to revise the Singapore IPv6 Profile to keep the requirement specification up-to-date based on Industries and Government Agencies feedback.

You may refer to the list of IPv6 compliance equipment at IPv6 Ready Logo website [2]. They have also established a test program to certify equipment.

7. Reference

[1] United States Government IPv6 Profile version 1 by National Institute of Standards and Technology, special publication 500-267, Jul 2008, http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

[2] IPv6 Ready Logo, http://www.ipv6ready.org/

Annex 1: IPv6 Basic Requirements

IETF Specification	IPv6 Basic Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC2460	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
RFC5095	Deprecation of Type 0 Routing Headers	Managed services	c(O)	c(M)			M	M			M	M	M
RFC2711	IPv6 Router Alert Option			M				M				M	M
RFC4443	ICMPv6		M	M			M	M			M	M	M
RFC4884	Extended ICMP for Multi-Part Messages	Managed services	c(O)	c(O)			S	S			S	S	S
RFC1981	Path MTU Discovery for IPv6		M	M			M	M			M	M	M
	Discovery Protocol Requirements		M	M			M	M			M	M	M
RFC2675	IPv6 Jumbograms		O	O		Configurable high-MTU links	c(O)	c(S)		Configurable high-MTU links	c(O)	c(S)	c(O)
RFC4861	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
RFC4861	Address Resolution		M	M			M	M			M	M	M

IETF Specification	IPv6 Basic Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
	NA and NS processing		M	M			M	M			M	M	M
RFC4862	Duplicate Address Detection		M	M			M	M			M	M	M
	Neighbor Unreachability Detection		M	M			M	M			M	M	M
	Redirect functionality		S	M			M	M			M	M	M
RFC5175	IPv6 Router Advertisement Flags Option	Managed services	c(O)	c(O)			S	S			S	S	S
RFC4191	Default Router Preference		S	S			S	S			S	S	S
RFC3971	Secure Neighbor Discovery	SEND	c(S)	c(S)		SEND	c(S)	c(S)		SEND	c(S)	c(S)	c(S)
RFC4862	IPv6 Stateless Address Autoconfig	SLACC	c(S)	c(S)	c(S)	SLACC	c(S)	c(S)	c(S)	SLACC	c(S)	c(S)	c(S)
	Creation of Link Local Addresses	SLACC	c(M)	c(M)		SLACC	c(M)	c(M)		SLACC	c(M)	c(M)	c(M)
RFC4861	Duplicate Address Detection	SLACC	c(M)	c(M)		SLACC	c(M)	c(M)		SLACC	c(M)	c(M)	c(M)
	Creation of Global Addresses	SLACC	c(M)	c(M)		SLACC	c(M)	c(M)		SLACC	c(M)	c(M)	c(M)
	Ability to Disable Creation of Global Addrs	SLACC	c(M)	c(M)		SLACC	c(M)	c(M)		SLACC	c(M)	c(M)	c(M)
RFC4941	Privacy Extensions for IPv6 SLAAC	SLACC	c(M)	c(M)	c(M)	SLACC	c(M)	c(M)	c(M)	SLACC	c(M)	c(M)	c(M)
	<2nd context for MIP Mobile Node>	SLACC+MIP	c(O)			SLACC+MIP	c(S)			SLACC+MIP	c(S)		
RFC3736	Stateless DHCP Service for IPv6	SLACC	c(S)	c(M)		SLACC	c(S)	c(M)		SLACC	c(S)	c(M)	c(M)
RFC3315	Dynamic Host Config Protocol (DHCPv6)	DHCP Client	c(M)			DHCP Client	c(M)			DHCP Client	c(M)		
	Ability to Administratively Disable	DHCP Client	c(M)			DHCP Client	c(M)			DHCP Client	c(M)		
	DHCP Client Functions	DHCP Client	c(M)			DHCP Client	c(M)			DHCP Client	c(M)		
RFC4361	Node-specific Client IDs for DHCPv4	DHCP Client &	c(S)			DHCP Client &	c(S)			DHCP Client &	c(S)		

IETF Specification	IPv6 Basic Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
		IPv4				IPv4				IPv4			
RFC3633	Prefix Delegation	DHCP Prefix	c(O)	C(M)		DHCP Prefix	c(S)	c(S)		DHCP Prefix	c(S)	c(S)	c(S)

Annex 2: Addressing Requirements

IETF Specification	Addressing Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC4291	IPv6 Addressing Architecture		M	M			M	M			M	M	
RFC4007	IPv6 Scoped Address Architecture		M	M			M	M			M	M	
	Ability to manually configure Addresses		M	M			M	M			M	M	
RFC4193	Unique Local IPv6 Unicast Address		O	O			O	O			O	O	
RFC3879	Deprecating Site Local Addresses		M	M			M	M			M	M	
RFC3484	Default Address Selection for IPv6		M	M			M	M			M	M	
	Configurable Selection Policies		S	S			S	S			S	S	
RFC2526	Reserved IPv6 Subnet Anycast Addresses		O	O			O	O			O	O	
RFC3972	Cryptographically Generated Addresses (CGA)	Condition[2]	c(M)	c(M)		Condition[2]	c(M)	c(M)		Condition[2]	c(M)	c(M)	
RFC4581	CGA Extension Field Format	Condition[2]	c(M)	c(M)		Condition[2]	c(M)	c(M)		Condition[2]	c(M)	c(M)	
RFC4982	CGA Support for Multiple Hash Algos.	Condition[2]	c(M)	c(M)		Condition[2]	c(M)	c(M)		Condition[2]	c(M)	c(M)	
RFC5952	A Recommendation for IPv6 Address Text		O	O			O	O			O	O	
RFC6052	IPv6 Addressing of IPv4/IPv6 Translators	Implement Translation	c(O)	c(O)		Implement Translation	c(O)	c(O)		Implement Translation	c(O)	c(O)	
RFC6085	Address Mapping of IPv6 Multicast Packets on Ethernet	Multicast over Ethernet	c(S)	c(S)		Multicast over Ethernet	c(S)	c(S)		Multicast over Ethernet	c(S)	c(S)	

[2] When VPN or other encryption protocol (e.g. SEND) initiate from the specific device is required. For Protection device such as firewall, it should able to work with CGA

Annex 3: IPv6 Security Requirements

IETF Specification	IPv6 Security Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
	IPsec-v3												
RFC4301/RFC6040	Security Architecture for the IP/ Tunnelling of Explicit Congestion Notification		M	M	M		M	M	M		M	M	M
RFC4303	Encapsulating Security Payload		M	M	M		M	M	M		M	M	M
RFC4302	Authentication Header (AH)		M	M	M		M	M	M		M	M	M
RFC3948	UDP Encapsulation of ESP Packets		O	O	O		O	O	O		O	O	O
RFC4835	Cryptographic Algorithms for ESP and AH		M	M	M		M	M	M		M	M	M
RFC4308	Cryptographic Suites for IPsec		O	O	O		O	O	O		O	O	O
RFC4869	Suite B Cryptographic Suites for IPsec		O	O	O		O	O	O		O	O	O
RFC4809	Requirements for an IPsec Cert Mgmnt Profile		S	S	S		S	S	S		S	S	S
	IKEv2												
RFC5996	Internet Key Exchange (IKEv2) Protocol		M	M	M		M	M	M		M	M	M
RFC4307	Cryptographic Algorithms for IKEv2		M	M	M		M	M	M		M	M	M
RFC3526	More MODP DH Groups for IKE		O	O	O	AES	c(S)	c(S)	c(S)		O	O	O
RFC5114	Additional DH Groups for Use with IETF Stds		O	O	O		O	O	O		O	O	O
RFC4945	Internet IPsec PKI Profile of IKEv1, IKEv2 & PKIX		S	S	S	Implementation of CA (Certificate Authority)	c(M)	c(M)	c(M)		S	S	S
	Uses of Cryptographic Algorithms												
RFC2410	NULL Encryption		M	M	M		M	M	M		M	M	M
RFC4835	Cryptographic Algorithms for ESP and AH		M	M	M		M	M	M		M	M	M

IETF Specification	IPv6 Security Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC2451	ESP CBC-mode Algorithms		M	M	M		M	M	M		M	M	M
RFC3602	AES-CBC		M	M	M		M	M	M		M	M	M
RFC3686	AES-CTR		O	O	O	Govt	c(S)	c(S)	c(S)		O	O	O
RFC4309	AES-CCM		O	O	O	Govt	c(S)	c(S)	c(S)		O	O	O
RFC4106	AES-GCM		O	O	O	Govt	c(S)	c(S)	c(S)		O	O	O
RFC4543	AES-GMAC		O	O	O	Govt	c(S)	c(S)	c(S)		O	O	O
RFC2404	HMAC-SHA-1-96		M	M	M		M	M	M		M	M	M
RFC4868	HMAC-SHA-256		O	O	O	Govt	c(S)	c(S)	c(S)		O	O	O
RFC3566	AES-XCBC-MAC-96		O	O	O	Govt	c(S)	c(S)	c(S)		O	O	O
RFC4434	AES-XCBC-PRF-128		O	O	O	Govt	c(S)	c(S)	c(S)		O	O	O
RFC4307	Cryptographic Algorithms for IKEv2		M	M	M		M	M	M		M	M	M
	Transition Mechanisms Requirements												
RFC4213	Transition Mechanise for Hosts & Routers		M	M			M	M			M	M	M
RFC4891	Using IPsec to Secure IPv6-in-IPv4 Tunnels	Tunnelling transition	c(M)	c(M)		Tunnelling transition	c(M)	c(M)		Tunnelling transition	c(M)	c(M)	
RFC2473	Generic Packet Tunneling in IPv6	Tunnelling transition	c(M)	c(M)		Tunnelling transition	c(M)	c(M)		Tunnelling transition	c(M)	c(M)	
RFC4798	Connecting IPv6 islands over IPv4 MPLS (6PE)	MPLS	c(M)	c(M)		MPLS	c(M)	c(M)		MPLS	c(M)	c(M)	
	ICMP												
RFC4890	Recommendations for Filtering ICMPv6 Messages in Firewalls				M				M				M

Annex 4: Application Requirements

IETF Specification	Application Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC3596	DNS Extensions for IPv6	Device supports DNS	c(M)	c(M)	c(M)	Device supports DNS	c(M)	c(M)	c(M)	Device supports DNS	c(M)	c(M)	c(M)
RFC2671	Extension Mechanisms for DNS (EDNS0)	Device supports DNS	c(M)	c(M)	c(M)	Device supports DNS	c(M)	c(M)	c(M)	Device supports DNS	c(M)	c(M)	c(M)
RFC3226	DNSSEC and IPv6 DNS MSG Size Reqs	Device supports DNSSEC	c(M)	c(M)	c(M)	Device supports DNSSEC	c(M)	c(M)	c(M)	Device supports DNSSEC	c(M)	c(M)	c(M)
RFC3986	URI: Generic Syntax	Device supports URIs	c(M)	c(M)	c(M)	Device supports URIs	c(M)	c(M)	c(M)	Device supports URIs	c(M)	c(M)	c(M)
RFC3493	Basic Socket API for IPv6	Device has exposed APIs	c(M)	c(O)	c(O)	Device has exposed APIs	c(M)	c(O)	c(O)	Device has exposed APIs	c(M)	c(O)	c(O)
RFC3542	Advanced Socket API for IPv6	Device has exposed APIs	c(S)	c(O)	c(O)	Device has exposed APIs	c(S)	c(O)	c(O)	Device has exposed APIs	c(S)	c(O)	c(O)
RFC4584	Extension to Sockets API for Mobile IPv6	Device supports MIPv6	c(S)	c(O)	c(O)	Device supports MIPv6	c(S)	c(O)	c(O)	Device supports MIPv6	c(S)	c(O)	c(O)
RFC3678	Socket API Extensions Multicast Source Filters	Device has exposed APIs	c(M)	c(O)	c(O)	Device has exposed APIs	c(M)	c(O)	c(O)	Device has exposed APIs	c(M)	c(O)	c(O)
RFC5014	Socket API for Source Address Selection	Device has exposed APIs	c(S)	c(O)	c(O)	Device has exposed APIs	c(S)	c(O)	c(O)	Device has exposed APIs	c(S)	c(O)	c(O)
RFC3315	DHCPv6 Functions (If host supports DHCP, it should also support DHCPv6)	Device supports DHCP	c(M)	c(M)	c(M)	Device supports DHCP	c(M)	c(M)	c(M)	Device supports DHCP	c(M)	c(M)	c(M)

Annex 5: Routing Protocol Requirements

IETF Specification	Routing Protocol Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC2740	OSPF for IPv6					For IGP; For hardware FW		c(M)	c(O)	For IGP; For hardware FW		c(M)	c(O)
RFC4552	Authentication/Confidentiality for OSPFv3					For IGP; For hardware FW		c(M)	c(O)	For IGP; For hardware FW		c(M)	c(O)
RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments					For IGP; For hardware FW		c(O)	c(O)	For IGP; For hardware FW		c(M)	c(O)
RFC5187	OSPFv3 Graceful Restart					For IGP; For hardware FW		c(S)	c(O)	For IGP; For hardware FW		c(M)	c(O)
RFC5329	Traffic Engineering Extensions to OSPF Version 3					For IGP; For hardware FW		c(S)	c(O)	For IGP; For hardware FW		c(S)	c(O)
RFC5838	Support of Address Families in OSPFv3					For IGP; For hardware FW		c(O)	c(O)	For IGP; For hardware FW		c(M)	c(O)
	RIPng Protocol Applicability Statement					For IGP; For hardware FW		c(M)	c(O)	For IGP; For hardware FW		c(M)	c(O)
RFC4271	Border Gateway Protocol 4 (BGP-4)					For EGP; For hardware FW		c(M)	c(O)	For EGP; For hardware FW		c(M)	c(O)
RFC1772	BGP Application in the Internet					For EGP; For hardware		c(M)	c(O)	For EGP; For hardware		c(M)	c(O)

IETF Specification	Routing Protocol Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
						FW				FW			
RFC4760	BGP Multi-Protocol Extensions					For EGP; For hardware FW		c(M)	c(O)	For EGP; For hardware FW		c(M)	c(O)
RFC2545	BGP Multi-Protocol Extensions for IPv6 IDR					For EGP; For hardware FW		c(M)	c(O)	For EGP; For hardware FW		c(M)	c(O)
RRC4659	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN					For EGP; For hardware FW		c(O)	c(O)	For EGP; For hardware FW		c(M)	c(O)
RFC5701	IPv6 Address Specific BGP Extended Community Attribute					For EGP; For hardware FW		c(O)	c(O)	For EGP; For hardware FW		c(S)	c(O)

Legend:
IGP: Require support of Interior Gateway Protocol
EGP: Require support of Exterior Gateway Protocol

Annex 6: Transition Mechanism Requirements

IETF Specification	Transition Mechanism Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC4038	Application Aspects of IPv6 Transition		S		S		S		S		S		S
RFC4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	IPv4	c(M)	c(M)		IPv4	c(M)	c(M)		IPv4	c(M)	c(M)	
RFC4798	Connecting IPv6 Islands over IPv4 MPLS Using Ipv6 Provider Edge Routers (6PE)					IPv4, MPLS		c(S)		IPv4, MPLS		c(M)	
RFC4659	6VPE					IPv4, MPLS		c(S)		IPv4, MPLS		c(M)	
RFC3056	6to4	IPv4	c(O)	c(O)		IPv4	c(O)	c(O)		IPv4	c(O)	c(O)	
RFC 4380	Teredo	IPv4	c(O)			IPv4	c(O)			IPv4	c(O)		
RFC 5214	ISATAP describes an automatic tunneling technique for dual stack nodes which uses IPv4 network as link layer.	IPv4				IPv4	c(O)	c(O)					
RFC6146	NAT64	IPv4		c(O)		IPv4		c(O)		IPv4		c(O)	
RFC6333	Dual Stack Lite	IPv4, managed service		c(O)		IPv4, managed service				IPv4, managed service		c(O)	
RFC 2765	Stateless IP/ICMP Translation Algorithm (SIIT)	IPv4		c(O)		IPv4		c(O)		IPv4		c(O)	
RFC5569	6RD	IPv4, managed service		c(O)		IPv4, managed service				IPv4, managed service		c(O)	
RFC5969	6RD with PD	IPv4, managed service		c(O)		IPv4, managed service				IPv4, managed service		c(O)	
RFC2784	Generic Routing Encapsulation			S				S				S	

Annex 7: Network Management Requirements

IETF Specification	Network Management Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
	Network Management Requirements												
RFC3411	SNMP v3 Management Framework	Managed services		c(O)		SNMP	c(M)	c(M)		SNMP	c(M)	c(M)	
RFC3412	SNMP Message Process and Dispatch					SNMP	c(M)	c(M)		SNMP	c(M)	c(M)	
RFC3413	SNMP Applications	Managed services		c(O)		SNMP	c(M)	c(M)		SNMP	c(M)	c(M)	
	Command Responder					SNMP	c(M)	c(M)		SNMP	c(M)	c(M)	
	Notification Generator					SNMP	c(S)	c(M)		SNMP	c(S)	c(M)	
RFC3414	User-based Security Model for SNMPv3					SNMP	c(M)	c(M)		SNMP	c(M)	c(M)	
	Management Information Bases												
RFC4293	MIB for the IP	Managed services		c(O)		SNMP	c(M)	c(M)		SNMP	c(M)	c(M)	
RFC4292	MIB for the IP Forwarding Table	Managed services		c(O)		SNMP		c(M)		SNMP		c(M)	
RFC4022	MIB for TCP					SNMP	c(S)	c(S)		SNMP	c(S)	c(S)	
RFC4113	MIB for UDP					SNMP	c(S)	c(S)		SNMP	c(S)	c(S)	
RFC4087	MIB for IP Tunnels					SNMP & IPv4		c(M)		SNMP & IPv4		c(M)	
RFC4807	MIB for IPSec Policy Database Configuration					SNMP & IPSecv3		c(M)		SNMP & IPSecv3		c(M)	
RFC4295	MIB for Mobile IPv6					SNMP & MIP		c(M)		SNMP & MIP		c(M)	
RFC3289	MIB for DiffServ	Managed services		c(O)		SNMP & DS		c(M)		SNMP & DS		c(M)	

Annex 8: Multicasting Requirements

IETF Specification	Multicasting Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC2710	Multicast Listener Discovery (MLD) for IPv6	When Group Management Capability is required	c(M)	c(M)		When Group Management Capability is required	c(M)	M		When Group Management Capability is required	c(M)	M	
RFC3590	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol	When Group Management Capability is required	c(M)	c(M)		When Group Management Capability is required	c(M)	M		When Group Management Capability is required	c(M)	M	
RFC3810	MLD Version 2 for IPv6	PIM-SSM	c(M)	c(M)		PIM-SSM	c(M)	c(M)		PIM-SSM	c(M)	c(M)	
RFC3306	Unicast-Prefix-based IPv6 Multicast Addrs		M	M			M	M			O	O	
RFC3307	Allocation Guidelines for IPv6 Multicast Addrs		M	M			M	M			M	M	
RFC4607	Source-Specific Multicast for IP	PIM-SSM	c(M)	c(M)		PIM-SSM	c(M)	c(M)		PIM-SSM	c(M)	c(M)	
RFC4604	MLDv2 for Source Specific Multicast (SSM)	PIM-SSM	c(M)	c(M)		PIM-SSM	c(M)	c(M)		PIM-SSM	c(M)	c(M)	
RFC4601	PIM Sparse Mode (SM)	PIM-SM		c(M)		PIM-SM		c(M)		PIM-SM		c(M)	
RFC4609	PIM-SM Security Issues / Enhancements	PIM-SM		c(S)		PIM-SM		c(S)		PIM-SM		c(S)	
RFC3956	Embedding Rendezvous Point (RP) Multicast Addr	Inter-domain multicast		c(S)		Inter-domain multicast		c(S)		Inter-domain multicast		c(S)	
RFC4489	A Method for generating link-scoped IPv6 Multicast Addrs	link scoped Multicast addrs		c(S)				c(S)				c(S)	
RFC5059	Bootstrap Router (BSR) Mechanism for PIM	boot-strap routers		c(S)				c(S)				c(S)	
RFC5015	BiDirectional Protocol Independent Multicast (BIDIR-PIM)	shared tree		c(M)				c(M)				c(M)	

Annex 9: Mobility Requirements

IETF Specification	Mobility Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC3775	Mobility Support in IPv6	MIPv6	c(M)	c(M)		MIPv6	c(M)	c(M)		MIPv6	c(M)	c(M)	
RFC3963	Network Mobility (NEMO) Basic Support in IPv6	NEMO		c(M)		NEMO		c(M)		NEMO		c(M)	
RFC4282	The Network Access Identifier	MIPv6	c(S)	c(S)		MIPv6	c(S)	c(S)		MIPv6	c(S)	c(S)	
		PMIPv6		c(M)		PMIPv6		c(M)		PMIPv6		c(M)	
RFC4283	Mobile Node Identifier option for MIPV6	MIPv6	c(S)	c(S)		MIPv6	c(S)	c(S)		MIPv6	c(S)	c(S)	
		PMIPv6		c(M)		PMIPv6		c(M)		PMIPv6		c(M)	
RFC4877	MIPv6 Op with IKEv2 and Revised IPsec Architecture	MIPv6	c(M)	c(M)		MIPv6	c(M)	c(M)		MIPv6	c(M)	c(M)	
RFC5213	Proxy Mobile IPv6	PMIPv6		c(M)		PMIPv6		c(M)		PMIPv6		c(M)	
RFC5380	Hierarchical Mobile IPv6 scheme	MIPv6	c(O)	c(O)		MIPv6	c(O)	c(O)		MIPv6	c(O)	c(O)	
RFC5555	Mobile IPv6 Support for Dual Stack Hosts and Routers	MIPv6/NEMO	c(S)	c(S)		MIPv6/NEMO	c(S)	c(S)		MIPv6/NEMO	c(S)	c(S)	
RFC5844	IPv4 Support for Proxy Mobile IPv6	PMIPv6	c(S)	c(S)		PMIPv6	c(S)	c(S)		PMIPv6	c(S)	c(S)	

Annex 10: Quality of Service Requirements

IETF Specification	Quality of Service Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC2474 (PS)	(DiffServ Header Field)	DS & Managed service	c(M)	c(M)		DS	c(M)	c(M)		DS	c(M)	c(M)	
RFC3140 (PS)	(PHB Encoding - DiffServ)	DS & Managed service	c(M)	c(M)		DS	c(M)	c(M)		DS	c(M)	c(M)	
RFC3168 (PS)	(Explicit Congestion Notification, ECN)	ECN & Managed service	c(S)	c(S)		ECN	c(S)	c(S)		ECN	c(S)	c(S)	
RFC2597 (PS)	(Assured Forwarding)	DS & Managed service		c(S)		DS		c(S)		DS		c(S)	
RFC3246 (PS)	(Expedited Forwarding)	DS & Managed service		c(S)		DS		c(S)		DS		c(S)	
RFC3247 (INF)	(Supplementary EF PHB)	DS & Managed service		c(S)		DS		c(S)		DS		c(S)	
RFC2475 (INF)	(DiffServ Architecture)	DS & Managed service		c(S)		DS		c(S)		DS		c(S)	
RFC3260 (INF)	(New Term & Clarification - DiffServ)	DS & Managed service		c(S)		DS		c(S)		DS		c(S)	
RFC2983 (INF)	(DiffServ and Tunnels)	DS & Managed service		c(S)		DS		c(S)		DS		c(S)	
RFC4594 (INF)	(Config guidelines DiffServ)	DS & Managed		c(S)		DS		c(S)		DS		c(S)	

IETF Specification	Quality of Service Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
		service											
RFC3086 (INF)	(DiffServ per Domain Behaviour)	DS & Managed service		c(S)		DS		c(S)		DS		c(S)	

Legend:
DS: Require support of differentiated services mechanism

Annex 11: Network Protection Device (NPD) Requirements

NIST SP500-267[3]	Network Protection Device (NPD) Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
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				S				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				O				M				M
6.12.4.1.1	Port/Protocol/address Blocking	FW or APFW			c(M)	FW or APFW			c(M)	FW or APFW			c(M)
6.12.4.1.2	Asymmetrical blocking	FW or APFW			c(M)	FW or APFW			c(M)	FW or APFW			c(M)
6.12.4.1.3	IPSec Traffic Handling	FW or APFW			c(S)	FW or APFW			c(M)	FW or APFW			c(M)
6.12.4.1.4	Performance under load, fail-safe	FW or APFW			c(M)	FW or APFW			c(M)	FW or APFW			c(M)
6.12.4.2.1	No violation of Trust Barriers	APFW			c(M)	APFW			c(M)	APFW			c(M)
6.12.4.2.2	Session traffic Auth	APFW			c(M)	APFW			c(M)	APFW			c(M)
6.12.4.2.3	Email, File filtering	APFW			c(M)	APFW			c(M)	APFW			c(M)
6.12.5.1.1	Known attack detection	IDS or IPS			c(M)	IDS or IPS			c(M)	IDS or IPS			c(M)

[3] http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

NIST SP500-267[3]	Network Protection Device (NPD) Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
6.12.5.1.2	Malformed packets detection	IDS or IPS			c(M)	IDS or IPS			c(M)	IDS or IPS			c(M)
6.12.5.1.3	Port Scan detection	IDS or IPS			c(M)	IDS or IPS			c(M)	IDS or IPS			c(M)
6.12.5.1.4	Tunnelled traffic detection				O	IDS or IPS			c(M)	IDS or IPS			c(M)
6.12.5.1.5	Logging and alerts	IDS or IPS			c(M)	IDS or IPS			c(M)	IDS or IPS			c(M)
6.12.5.1.6	Performance under load, fail-safe	IDS or IPS			c(M)	IDS or IPS			c(M)	IDS or IPS			c(M)
6.12.5.2.1	Intrusion Prevention	IPS			c(M)	IPS			c(M)	IPS			c(M)

Legend:
FW: Require support of basic Firewall capabilities
APFW: Require support of application firewall capabilities
IDS: Require support of intrusion detection capabilities
IPS: Require support of intrusion protection capabilities

Annex 12: Link Specific Requirements

IETF Specification	Link Specific Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC2497	IPv6 over ARCnet	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC2590	IPv6 over Frame Relay	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC2464	IPv6 over Ethernet	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC2467	IPv6 over FDDI	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC2491	IPv6 over NBMA network	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC2492	IPv6 over ATM	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC3146	IPv6 over IEEE 1394 Networks	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC3572	IPv6 over MAPOS (SONET/SDH)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC4338	IPv6, IPv4 and ARP packets over Fibre Channel	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC4944	IPv6 over IEEE 802.15.4 Networks	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC5072	IPv6 over PPP	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC5121	Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)	Condition[4]	c(M)	c(M)	c(M)
RFC2507	IP Header Compression	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	
RFC2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	
RFC3173	IP Payload Compression Protocol (IPComp)	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	
RFC4995	Robust Header Compression (ROHC) framework	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	
RFC4996	ROHC Profile for TCP	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	
RFC3095	ROHC Profile for RTP,UDP, ESP and Uncomp	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	

[4] Applicable when the specified link technology is chosen as preferred choice of connectivity

IETF Specification	Link Specific Requirements	Residential				Government Agencies & Enterprise				Network Provider			
		Condition	Host	Router	NPD	Condition	Host	Router	NPD	Condition	Host	Router	NPD
RFC4815	Connections and Clarifications to RFC3095	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	
RFC3843	ROHC Profile for IP Only	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	
RFC3241	ROHC over PPP	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	
RFC4362	ROHC Link Assisted for IP/UDP/RTP	Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)		Condition[4]	c(O)	c(O)	

Annex A: Corrigendum / Addendum

Page	TS Ref.	Items Changed	Effective Date
Changes to IDA RS IPv6 Issue 1, Feb 2011			
		Change of IDA's address at cover page to Mapletree Business City.	1 May 11
11	Annex 3	Insertion of RFC4307 at Annex 3	Jun 11
13-14	Annex 5	Revision of RFC1772, RFC 4760 and insertion of RFC 2545, RFC 4659 and RFC 5701 at Annex 5	Jun 11
9	Annex 2	Insertion of RFC5952, RFC6052 and RFC6085 at Annex 2	Jan 12
10	Annex 3	Insertion of RFC6040, RFC4890, replace RFC4306 & RFC4718 by RFC5996 and revised requirement for RFC4798	Jan 12
16	Annex 6	Update the drafts by RFC6146, RFC6333, RFC5569 and insertion of RFC5969	Jan 12
24-25	Annex 12	Insertion of RFC2464, RFC2467, RFC2491 and RFC2492	Jan 12