TECHNICAL CODE

INTERNET PROTOCOL VERSION 6 (IPv6) - DEPLOYMENT REQUIREMENTS TO COMPLETE TRANSITION TO IPv6

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

MCMC MTSFB TC GXXX:2022

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.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

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

Contents

Page

Committee representation

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:

American Malaysian Chamber of Commerce

Celcom Axiata Berhad

Cisco Systems Malaysia

Digi Telecommunication Sdn Bhd

Maxis Broadband Sdn Bhd

My6 Initiative Berhad

SIRIM QAS International Sdn. Bhd.

Telekom Malaysia Berhad

webe digital sdn bhd

Foreword

This technical code for Internet Protocol version 6 (IPv6) - Deployment Requirements to Complete Transition to IPv6 ('Technical Code') was developed pursuant to the section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Numbering and Electronic Addressing Working Group.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INTERNET PROTOCOL VERSION 6 (IPv6) - DEPLOYMENT REQUIREMENTS TO COMPLETE TRANSITION TO IPv6

1. Scope

This Technical Code specifies the deployment requirements for organisations to complete the transition to Internet Protocol version 6 (IPv6). The full transition to IPv6 is the only viable solution to sustain the development of internet.

Despite the criticality of Internet Protocol version 4 (IPv4) address exhaustion, organisations in Malaysia have been rather slow to adopt IPv6 and the same trend is evident in developing nations all around the world.

This Technical Code will assist organisations:

a) that have not or are considering to deploy IPv6 in their network and services;

b) that have initiated transition but looking to enhance IPv6 in their network and services;

c) in creating push factor to move towards native IPv6; and

d) with greenfield deployments that are looking for quick wins.

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

2. Normative references

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

See Annex A.

3. Abbreviations

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

See Annex B.

4. Terms and definitions

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

4.1 Applications Service Provider (ASP)

A person who provides an applications service.

4.2 Internet Protocol version 4 (IPv4)

Uses 32-bit addresses and is the current version of the Internet Protocol (IP).

4.3 Internet Protocol version 6 (IPv6)

Uses 128-bit addresses and is designed to replace and enhance IPv4.

4.4 Mobile Virtual Network Operators (MVNO)

A wireless communication service operator that provides telecommunications services through the infrastructure and network of existing Mobile Network Operators (MNOs).

4.5 Network element

The definition in MCMC MTSFB TC T013 shall apply.

4.6 Network security element

The definition in MCMC MTSFB TC T013 shall apply.

4.7 Network Service Provider (NSP)

A person who provides network services.

4.8 Terminal/host

The definition in MCMC MTSFB TC T013 shall apply.

5. Overview

In the last 10 years or so in Malaysia, the transition to IPv6 was mainly focused on dual-stack, which is becoming increasingly complex to sustain and inevitably prolongs the life of IPv4. With the advent of disruptive technologies such as Internet of Things (IoT), autonomous vehicles and advancement in wireless communications, it is very clear that complete transition to an IPv6-only environment is the viable solution for internet services.

The deployment requirement for IPv6 goes through the standard development life cycle of the following phases:

a) Phase 1 - Plan, design and testing;

b) Phase 2 - Implementation; and

c) Phase 3 - Monitoring.

Deployment process does not end at implementation phase, instead it is an on-going process that goes into learning and adapting as part of improvement to the initial plan and design.

The following content in this Technical Code will be structured according to this continuous IPv6 deployment life cycle. Organisations looking to fully adopt IPv6 may consider each of the checklist throughout the cycle as guidance as tabulate in the Table 1.

Table 1. IPv6 deployment life cycle

Phase	Requirements
Phase 1: Plan and design	a) IPv6 readiness assessment b) Network assessment c) Security assessment d) IPv6 addressing plan i) Subnet planning ii) Prefix size iii) Obtaining IPv6 address e) Services i) Internet presence services ii) Domain Name Systems (DNS) iii) Email
Phase 2: Testing	a) Device compliance b) Network compliance
Phase 3: Implementation	a) Transition mechanism b) IPv6 connectivity by default to service provider/peering c) Internet presence services i) DNS ii) Web Services iii) Email d) Security
Phase 4: Monitoring	a) Monitoring and enforcement b) IPv6 security vulnerability, risks, threats and impacts (post-deployment) c) Service experience

6. Phase 1 - Plan and design

6.1 Internet Protocol version 6 (IPv6) readiness assessment

IPv6 readiness evaluation establishes a baseline for current architecture and identifies gaps for successful IPv6 migration. Organisations should inventorize their current Information Technology (IT) infrastructure to see which assets will be impacted by the transition to IPv6 for network and system applications.

The inventory should include but not limited to the networking hardware, applications and Operating Systems (OS) that will be affected by the IPv6 transition :

a) Devices - interface.

b) Operating Systems (OS)

c) Application - limited web services, connectivity, protocol.

The inventory data should be used to update their underlying architecture's current technology and service component views, specifically as follows:

a) Service component

The service component architectural view should be updated to incorporate IP dependency information for organisation’s IT assets. Assets, which depend on IP (but are not IPv6 compliant) can be identified directly from the architecture and prioritised accordingly within the organisation’s capital planning activities.

b) Technology

The technology architectural view should be updated to reflect which IT assets within the organisation either provide or require IP services, and whether those assets, such as routers and servers, are capable of being upgraded to support IPv6.

The readiness assessment can be further broken down into four sub-phases as follows:

a) assessment planning (refer 6.1.1);

b) assessment execution (refer 6.1.2);

c) analysis and findings (refer 6.1.3); and

d) reporting and recommendations (refer 6.1.4).

6.1.1 Assessment planning

The initial engagement should start with a planning and information gathering session. The objective of this stage is to establish project team members of the stakeholder within the organisation. Other key objectives for this phase are to finalise the scope of work and project timeline.

6.1.2 Assessment execution

A holistic approach needs to be done using a combination of assessment tools as well as conducting a face-to-face interview to achieve desired outcome as tabulate in the Table 2.

Table 2. Assessment tools

Assessment tools	Description
Interview or questionnaire	Engaging discussion with the client Information and Communications Technology (ICT)'s team and its provider or supplier to understand its current network and system infrastructure environment by answering a series of questions.
Network diagram	Reviewing current physical and logical network diagram.
Network discovery	Running network discovery tools to establish a list of network devices, servers, and hosts on the client network.
Network scanning	Running scanning tools to establish inventory lists of operating software for the discovered devices.
Validation	Verify OS or software features information retrieved with actual information by requesting confirmation from the organisation's ICT personnel or the provider or supplier.

6.1.3 Analysis and findings

Once the list of asset inventory and other important information regarding IPv6 requirements have been gathered, the next step organisations need to take is to confirm capabilities and readiness on identified devices to more effectively determine the appropriate IPv6 design.

Based on the hardware and firmware information, organisations should crosscheck with the manufacturer or principal on the IPv6 support (and features) for each of those devices. The following approach varies depending on the type of manufacturer:

a) using web feature navigator tools to list down IPv6 features supported;

b) refer to product-specific datasheets and IP feature matrix; and

c) contact directly with the manufacturer or principal (if the information could not be found using previous methods).

6.1.4 Results and recommendations

The final phase of the IPv6 readiness assessment is to develop the internal IPv6 readiness and recommendations report, which shall summarise but not limited to the following items.

a) Critical assessment findings.

b) Data and statistics regarding individual systems and vulnerabilities.

c) Recommendations for improvement.

This report can be presented to all stakeholders. A Transfer of Knowledge session may also be conducted to the organisation's ICT team to brief on the assessment results and to share the IPv6 implementation design.

6.2 Network assessment

6.2.1 Internet Protocol version 6 (IPv6) architecture and design

Design development is a hands-on approach whereby the technical requirements and design goals are integrated into IPv6 architectural design based on leading practices and case studies. It involves transition design for the network, applications, and services. This phase includes the development of the following:

a) A business case justification, including requirements and risk analysis.

b) A solution concept with the proposed network topology.

c) Recommended protocols and features to implement the required IPv6 solution.

d) A high-level design for a resilient, scalable, secured, modular network infrastructure with the targeted availability defined by the organization, including a high-level IPv6 address plan.

e) Design definition specific to business/technical requirements and primary metrics.

f) A solution gap analysis and implementation design (refer Figure 1), including high-level integration considerations.

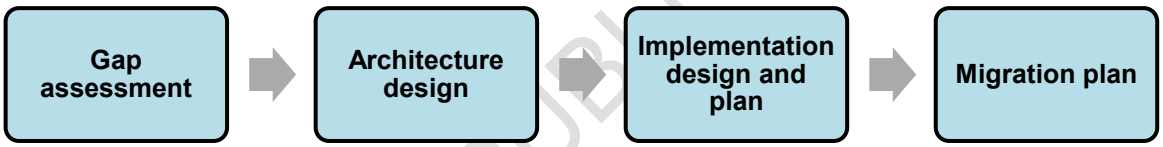

Figure 1. Gap analysis and implementation process flow

Based on Figure 1, IPv6 architecture and design are formulated based on the comprehensive IPv6 readiness assessment findings. IPv6 architecture and design provide an outlook of IPv6 implementation design and plan. It gives details of incremental migration from IPv4 to IPv6. During this phase, the scope of work enablement is defined and a design blueprint is created.

Organisations should create a design blueprint and a transition strategy to introduce IPv6 without disrupting the IPv4 network.

The implementation design should ensure IPv6 network and application solution architecture cover the following:

a) IPv4 or IPv6 interconnectivity - Individual IPv4 and IPv6 networks are connected via various tunnelling mechanisms, dual stacks, etc.

b) IPv6 routing - Reachability across IPv4 and IPv6 through the appropriate deployment of IPv6 routing protocol.

c) IPv6 security, Quality of Service (QoS), multicast services, and monitoring.

d) Monitoring of IPv6 traffic sessions across the network.

e) Ensure Network Management System (NMS) applications or solutions are seamlessly able to support and monitor IPv4 and IPv6 networks.

f) Ensure seamless integration to Operations Support System (OSS) and Business Support System (BSS) applications and services (e.g. Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), etc.).

The migration plan should not only be limited to the network but also the services and applications.

6.3 Security assessment

Preliminary security assessment is essential during the planning stage to determine if there is any vulnerability in the capability of network and devices in providing IPv6 security control.

Organisations may use vulnerability security assessment tools to conduct the security assessment such as the following:

a) open ports;

b) rouge devices; and

c) OS vulnerability

Organisations shall incorporate the findings in their overall IPv6 readiness assessment report with a declaration and sign off by their security team.

6.4 Internet Protocol (IP) addressing plan

RFC 6241, *IP Version 6 Addressing Architecture* describes the different types of IPv6 addresses, its notation and provides the basis of the following recommendation. Organisations are advised to understand the IPv6 addressing architecture before going into process of subnet planning and requesting for IPv6 address.

6.4.1 Subnet planning

Considerations for subnet planning should include the following:

a) Network size.

b) Number of users.

c) Number of nodes deployed.

d) Number of connected devices.

e) Multihoming requirements.

6.4.2 Prefix size

The maximum prefix size that can be obtained from Asia Pacific Network Information Centre (APNIC) is /32. Organisations may request for smaller subnet from service provider depending on the consideration. APNIC guidelines for IPv6 allocation and assignment requests depicts as follows:

a) A minimum of a /48 to organisations, as follow:

   i) that are multihoming, serving as critical communication infrastructure or requires provider-independent IPv6 assignment; and

   ii) that have multiple smaller networks or multiple Local Area Network (LAN)

b) /56 for smaller organisations with multiple LAN requirement.

c) /64 if only one subnet is required (similar to single IPv4 address).

6.4.3 Obtaining Internet Protocol version 6 (IPv6) address

Organisations should obtain IPv6 address from either of the following:

a) APNIC as the Regional Internet Registry (RIR) if the organisation plans to do multihoming to more than one service provider; or

b) service provider.

7. Phase 2 - Testing

7.1 Device compliance

All IPv6 capable directly connected equipment to the service provider shall be certified starting 10 July 2020 and onwards. This encompasses the following equipment categories:

a) terminals/hosts (e.g. 4G or 5G access points);

b) network elements (e.g. switching or gateway equipment); and

c) network security elements (e.g. firewalls).

All tested equipment shall comply to the following requirements:

a) general requirements on power supply, power supply cords and plugs, electromagnetic compatibility, markings, language and electrical safety; and

b) IPv6 compliance i.e., 5-core Request for Comments (RFCs) are as follows:

   i) RFC 8200;

   ii) RFC 4861;

   iii) RFC 4862;

   iv) RFC 8201; and

   v) RFC 4443.

Once certified, the equipment will carry mandatory certification mark to indicate they have been certified in accordance with the Communications and Multimedia (Technical Standards) Regulations 2000. The compliance requirement shall fulfil the MCMC MTSFB TC T013.

7.2 Network compliance

IPv6 Ready Logo Program by IPv6 Forum is a conformance and interoperability testing program designed to verify protocol implementation and interoperability between products. It offers access to testing tools and global laboratories.

8. Phase 3 - Implementation

8.1 Transition mechanism

Completing the transition to IPv6 requires many different environments to be capable of operating completely on IPv6 without being dependent on IPv4. As IPv4 is fully exhausted thus IPv6 should be fully adopted by new technologies and deployment.

Dual-stack connectivity or other transition technology should be deemed as temporary because the end goal should be an IPv6-only state. However, the selection of transition technology depends on the organisation's objective, capability and service requirement.

8.1.1 Dual-stack (RFC 4213)

The most common method of transition to support IPv6 in existing networks. In dual-stack environment (see Figure 2), all networking elements support both IPv4 and IPv6 versions but may incur additional processing and resources to handle both simultaneously.

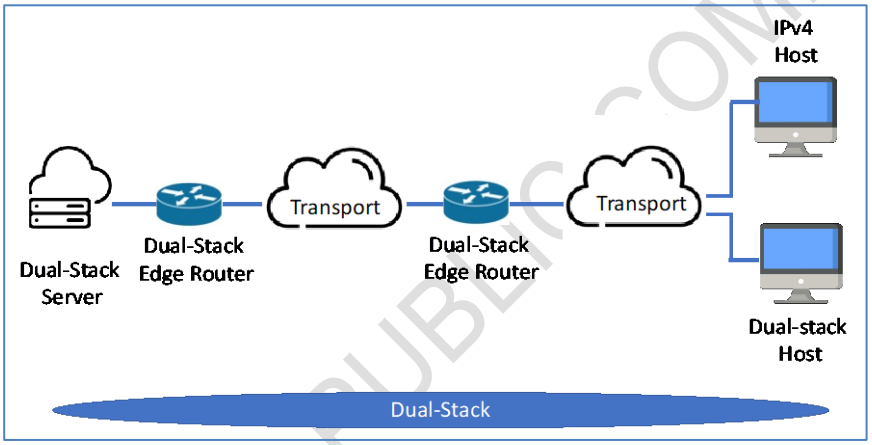

Figure 2. Dual-stack connectivity

8.1.2 Tunnelling (RFC 7059)

There is various mechanism for tunnelling available for providing IPv6 connectivity over IPv4 network (see Figure 3). This option may be required for situations where it is not possible to get native IPv6 connectivity. However, encapsulating IPv6 packets in IPv4 packets may have some effect on performance and security that should be considered when deciding the best transition mechanism.

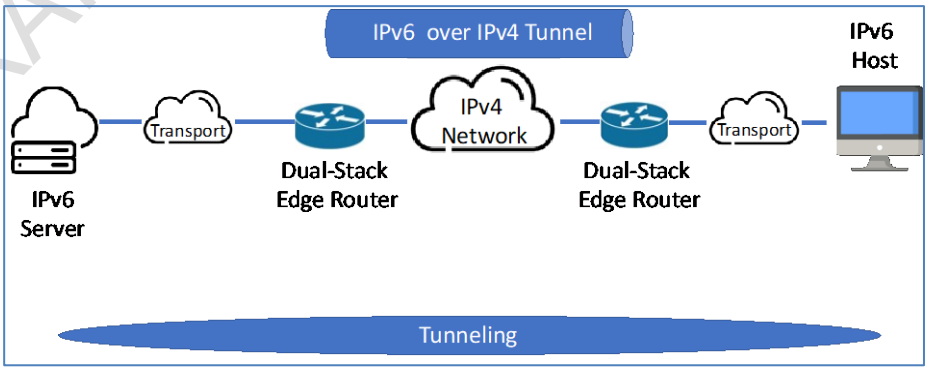

Figure 3. Tunnelling connectivity

8.1.3 464XLAT (RFC 6877)

The 464XLAT is deployed on IPv6 transport and supports end-to-end IPv6 connectivity (see Figure 4). However, this connectivity also allows for IPv4 service extension using a combination of stateful, Provider-Side Translator (PLAT) and stateless translation, Customer-Side Translator (CLAT).

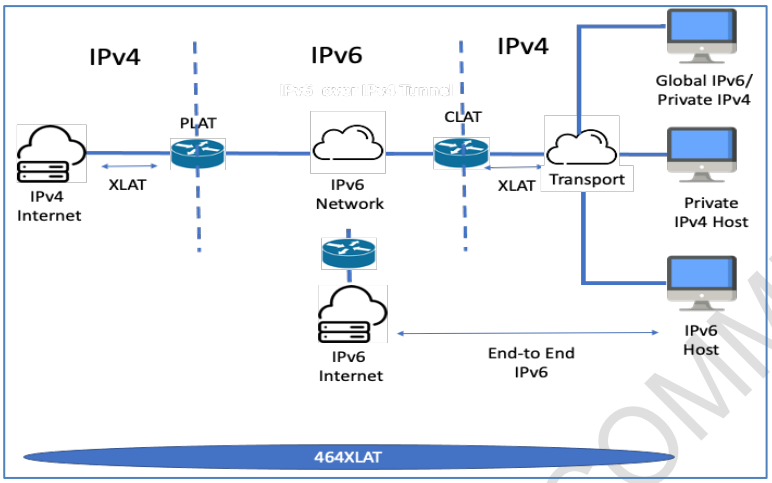

Figure 4. 464XLAT connectivity

Table 3 indicates that for IPv6 host to IPv4 server communication, single translation will happen while IPv4 host to IPv4 server communication will incur double translation. The 464XLAT architecture works for IPv4 in client-server model, but not in peer-to-peer communication.

Table 3. Translation in 464XLAT

Server	Application and host	Traffic treatment	Location of translation
IPv6	IPv6	End-to end IPv6	N/A
IPv4	IPv6	Stateful translation	PLAT
IPv4	IPv4	464XLAT	CLAT/PLAT

8.2 Internet Protocol version 6 (IPv6) only

The goal is to achieve an IPv6-only state where IPv6 connectivity is made possible without any tunnelling or translation and networks can finally remove any dependency on IPv4. This connectivity is illustrated in Figure 5.

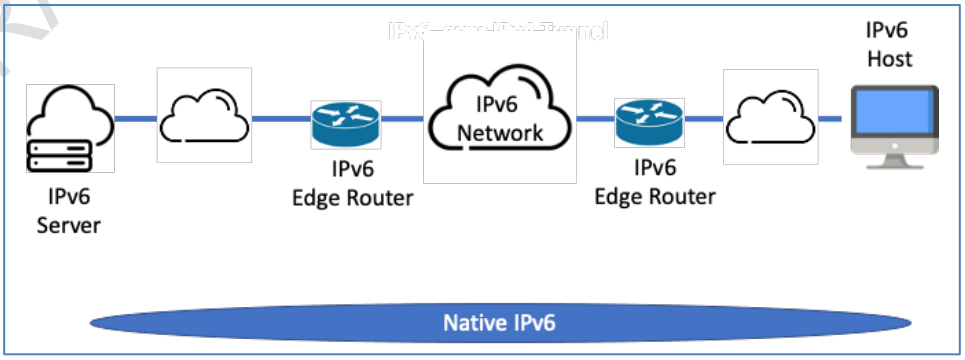

Figure 5. Native IPv6 connectivity

9. Phase 4 - Monitoring

9.1 Monitoring and enforcement

The right strategies shall be adopted and implemented for a smooth transition to IPv6 and it has to be continuously monitored until it is fully deployed and operational. Since 2013, Malaysian Internet Service Providers (ISP) or Network Service Providers (NSP) licensees have been subjected to IPv6 Compliance Audit by Malaysian Communications and Multimedia Commission (MCMC) for both fixed and cellular services to ensure the following:

a) readiness of service;

b) assignment of IPv6 (via dual-stack);

c) DNS and World Wide Web (WWW) reachability;

9.1.1 Regulatory roles

Regulatory push plays a critical role in progressing technological adoption in any country as evident in IPv6 adoption. In countries like Europe, United States of America, China and Vietnam where the government and regulatory impost a directive or a policy on IPv6 adoption, their IPv6 statistics are much higher compared to countries without any such policy.

The same is also for Malaysia with higher IPv6 statistics compared to its neighbours due to similar enforcement by MCMC through Direction No. 2 of 2015, *Commission Direction on Adoption of Internet Protocol version 6 (IPv6) in Malaysia*.

In continuing that spirit and keeping the momentum going, IPv6 compliance audit should be continued by MCMC with certain rejuvenation in consideration of the following:

a) Internet Architecture Board (IAB) recommendation to accelerate IPv6-only deployments.

NOTE: The Internet Engineering Task Force (IETF) as well as other Standards Development Organisations (SDOs) need to ensure that their standards do not assume IPv4. The IAB expects that the IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimise for and depend on IPv6.

b) Self-declaration audit made mandatory to encourage participation without adding overhead.

c) Expansion of coverage, not just to NSP but also Applications Service Provider (ASP), Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) and Mobile Virtual Network Operator (MVNO) which will be facilitated by the method of self-declaration. This could help further to boost the IPv6 adoption for Malaysia.

d) Conversion from physical face-to-face audit exercise to web-based self-declaration in view of improved connectivity facilities, technology and way of working brought by Covid-19 pandemic.

e) Findings from the audit exercise could be used to further improve the deployment of IPv6 in Malaysia.

f) Grace period to be set for readiness of IPv6-only service assignment.

9.1.2 Compliance audit checklist

Recommendation for self-declaration checklist in Annex C is a simplified version of the existing IPv6 Service Compliance Audit by taking into consideration the main objective of the ability of auditee in providing IPv6 service to its customer. The self-declaration check list should be accompanied with a signed declaration and attachment of evidence in softcopy.

9.2 Service experience

The exhaustion of IPv4 address maybe the biggest driver for service providers and content providers to shift to IPv6 especially when introducing new services and applications, in particular those made available on the Internet. However, the adoption of IPv6 to the services should enhance accessibility and consistency of the customer experience without any compromise. The following consideration should be weighed in during the service planning stage:

a) Adoption of IPv6 is transparent to most end-user and should be introduced without causing disruption to the service (by default).

b) The stigma surrounding IPv6 assignment is that IPv6 brings performance degradation in certain internet applications. The Quality of Experience (QoE) over IPv4 versus IPv6 may vary for applications that are sensitive to network performance (i.e. packet loss, jitter, latency) such as gaming, video streaming and Voice over Internet Protocol (VoIP). Thus, the performance for applications on IPv6 should be equal to or more superior than IPv4.

c) Service design consideration should factor in the impact of application behaviour over dual-stack if IPv4 traffic passes through Carrier Grade Network Address Translation (CGN).

d) Network operators should be aware that the host device used by their end users could have differing experience when preferring IPv6 address over IPv4. Further details as in RFC 6724 and RFC 8305.

e) The QoE should be measured as part of compliance checklist by regulators to gather information (crowdsourcing) on differing experiences of users using IPv6 in bid to enrich information and contribute towards the development of IPv6 in this region.

10. Security

IETF documents on operational security consideration for IPv6 are still in ongoing discussion tracks due to new challenges and developments in security controls. For organisations that are planning to start IPv6 deployment or have already started transition to IPv6 via dual-stack, it is important to acknowledge that IPv6 is not more or less secure than IPv4. An oversight on its differences could be a dangerous blind spot for organisations that have adopted or planning towards adoption of IPv6.

10.1 Internet Protocol version 6 (IPv6) security concerns

IPv6 security assessment should be conducted periodically as part of the overall network security audit in any organisation. Table 4 shows consideration specifics to IPv6 that should be included in the assessment and it should be reflective of any changes in the RFC standards..

Table 4. Security assessment

Category		Standard	Title
Basic IPv6 protocol	N/A	RFC 8200	*Internet Protocol, Version 6 (IPv6) Specification*
IPv6 associated protocol	ICMPv6	RFC 4443	*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
	NDP	RFC 4861	*Neighbor Discovery Protocol*
		RFC 6980	*Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*
	MLD	RFC 3810	*Multicast Listener Discovery (MLD) for IPv6*
	DNS	RFC 3596	*DNS Extensions to Support IP Version 6*
	DHCPv6	RFC 8415	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
		RFC 7824	*Privacy Considerations for DHCPv6*
	MTU	RFC 8201	*Path MTU Discovery for IP version 6*
	SLAAC	RFC 4862	*IPv6 Stateless Address Autoconfiguration*
		RFC 7217	*A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)*
Transition	N/A	RFC 4942	*IPv6 Transition/Coexistence Security Considerations*
	N/A	RFC 7123	*Security Implications of IPv6 on IPv4 Networks*
	N/A	RFC 6877	*464XLAT: Combination of Stateful and Stateless Translation*

NOTES:

1. ICMPv6 is Internet Control Message Protocol for IPv6.
2. NDP is Neighbour Discovery Protocol.
3. MLD is Multicast Listener Discovery.
4. DNS is Domain Name System.
5. DHCPv6 is Dynamic Host Configuration Protocol version 6.
6. MTU is Maximum Transmission Unit.
7. SLAAC is StateLess Address Auto Configuration.

11. Recommendation

In conclusion, this Technical Code recommends deployment requirements to complete transition to IPv6 and ultimately reduce dependency on IPv4 address. Organisations need to factor in IPv6 during new infrastructure build and during upgrade of any end-of-life network equipment. The advent of IoT and Fourth Industrial Revolution (IR 4.0) will bring greater potential use for IPv6 and it's adoption will no longer be considered optional.

Annex A
(normative)

Normative references

MCMC MTSFB TC T013, *Internet Protocol version 6 (IPv6) - Equipment Compliance*

Communication and Multimedia Act 1998, Direction No. 2 of 2015, *Commission Direction on Adoption of Internet Protocol version 6 (IPv6) in Malaysia*

RFC 3596, *DNS Extensions to Support IP Version 6*

RFC 3810, *Multicast Listener Discovery (MLD) for IPv6*

RFC 4213, *Basic Transition Mechanisms for IPv6 Hosts and Routers*

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 4942, *IPv6 Transition/Coexistence Security Considerations*

RFC 6724, ***D**efault address selection for Internet Protocol Version 6 (IPv6)*

RFC 6877, *464XLAT: Combination of Stateful and Stateless Translation*

RFC 6980, *Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*

RFC 7059, *A Comparison of IPv6-over-IPv4 Tunnel Mechanisms*

RFC 7123, *Security Implications of IPv6 on IPv4 Networks*

RFC 7217, *A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)*

RFC 7824, *Privacy Considerations for DHCPv6*

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

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

RFC 8305, *Happy Eyeballs Version 2: Better Connectivity Using Concurrency*

RFC 8415, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

Annex B
(informative)

Abbreviation

APNIC	Asia Pacific Network Information Centre
ASP	Applications Service Provider
BSS	Business Support System
CGN	Carrier Grade Network Address Translation
CLAT	Customer-Side Translator
CRM	Customer Relationship Management
DDoS	Distributed Denial of Service
DHCPv6	Dynamic Host Configuration Protocol version 6
DL/UL	Downlink/Uplink
DNS	Domain Name System
ERP	Enterprise Resource Planning
IAB	Internet Architecture Board
ICMPv6	Internet Control Message Protocol for IPv6
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR 4.0	Fourth Industrial Revolution
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit
MCMC	Malaysian Communications and Multimedia Commission
MLD	Multicast Listener Discovery
MNO	Mobile Network Operator
MTU	Maximum Transmission Unit
MVNO	Mobile Virtual Network Operator
NDP	Neighbour Discovery Protocol
NMS	Network Management System
NSP	Network Service Provider
OS	Operating System

OSS	Operations Support System
PLAT	Provider-Side Translator
QoE	Quality of Experience
QoS	Quality of Service
RFC	Request for Comments
RIR	Regional Internet Registry
SDO	Standards Development Organisation
SLAAC	StateLess Address Auto Configuration
VoIP	Voice over Internet Protocol
WWW	World Wide Web

Annex C
(informative)

Self declaration audit checklist

Table B.1. IPv6 service compliance

A	Licensee Information						
1	Service Provider						
2	Type of Service	**Fixed**			**Wireless**		
3	Product Name						
4	Date of Declaration	Dd		Mm		Yy	
5	Region	Central	Northern	Southern	Eastern	Sabah	Sarawak

B	Connectivity			
1	Customer Segment	**Business**		**Consumer**
2	Method of IPv6 Prefix Assignment	**SLAAC**	**DHCPv6**	**Manual**
3	Request for IPv6 Assignment	**Default**		**Upon Request**
4	IPv6 Address Assignment	**Dual-stack**	**Native**	**Others :**
	a. IPv6 Prefix			
	b. IPv4 Prefix			
5	Device Info	**Computer**	**Mobile Phone**	**Others :**
	a. OS Version	*e.g. : macOS Catalina*		
	b. Application Version	*e.g. : Firefox 91.0*		

C	Application Testing	Evidence Required
	HTTP/S	
1	Perform dual-stack website access test to the following sites: 1. http://google.com 2. http://facebook.com 3. http://youtube.com 4. http://www.mampu.gov.my 5. http://www.skmm.gov.my	Demonstrate **successful accessibility** to **any** of the dual-stack websites
2	Perform web based IPv6 accessibility and connectivity tests by accessing the following sites: 1. http://test-ipv6.com 2. http://ipv6-test.com 3. http://ipv6.whatismyv6.com 4. http://ipv6test.google.com	Demonstrate **successful diagnostics** from **any** of the dual-stack websites

Table B.1. IPv6 service compliance *(continued)*

C	Application Testing	Evidence Required
	HTTP/S	
3	Perform dual-stack DNS resolving test to the following domains: 1. google.com 2. facebook.com 3. youtube.com 4. www.mampu.gov.my 5. www.skmm.gov.my	Demonstrate **dual-stack DNS resolution** for **any** of the dual-stack websites
	Video Streaming	
1	Streaming of video content from the following sites: 1. Netflix 2. Youtube 3. Facebook Video 4. Disney HotStar 5. Tonton	Demonstrate **successful streaming** from **any** of the dual-stack streaming video

D	Quality of Service Parameters	
1	Perform ping test to the following domains : 1. google.com 2. facebook.com 3. youtube.com 4. www.mampu.gov.my 5. www.skmm.gov.my	Demonstrate **latency** from to **any** of the dual-stack websites
2	Perform web-based dual-stack speed tests (upload/download) by accessing the following sites: 1. http://www.speedtest.net/ 2. http://ipv6-test.com/speedtest/ 3. http://ipv6-speedtest.net/ 4. http://speedtest.comcast.net/ 5. http://speedtest6.com/	Demonstrate **speed test** from **any** of the dual-stack websites
3	Perform dual-stack website access test to the following sites: 1. http://google.com 2. http://facebook.com 3. http://youtube.com 4. http://www.mampu.gov.my 5. http://www.skmm.gov.my	Demonstrate **page load time** to **any** of the dual-stack websites

Bibliography

[1] MCMC MTSFB TC G005, *Code of Practice for the Deployment of Internet Protocol Version 6 (IPv6)*

[2] MS 2235:2009, *Internet service provider (ISP) and large-scale enterprise IPv6 fixed network implementation and compliance testing - Guidelines*

[3] Resolution 64 (Rev. Hammamet, 2016), *Internet protocol address allocation and facilitating the transition to and deployment of IPv6*

[4] RFC 4213, *Basic Transition Mechanisms for IPv6 Hosts and Routers*

[5] RFC 6241, *IP Version 6 Addressing Architecture*

[6] RFC 6540, *IPv6 support required for all IP-capable nodes*

[7] RFC 6877, *464XLAT: Combination of Stateful and Stateless Translation*

[8] RFC 7059, *A Comparison of IPv6-over-IPv4 Tunnel Mechanisms*

[9] RFC 7381, *Enterprise IPv6 Deployment Guidelines*

[10] RFC 7381, *Enterprise IPv6 Deployment* Guidelines

[11] RFC 8305, *Happy Eyeballs Version 2: Better Connectivity Using Concurrency*

[12] RFC 8504, *IPv6 Node Requirements*

[13] RFC 9099, *Operational Security Considerations for IPv6 Networks*

[14] *Mobile Virtual Network Operators (MVNO) The Redefining Game*, MCMC

[15] IPv6 Forum, IPv6 Ready Logo

Acknowledgement

Members of the Numbering and Electronic Addressing Working Group

Ms Azura Mat Salim (Chairman)	Telekom Malaysia Berhad
Mr Yan Kim Fui (Vice Chairman)	Cisco Systems Malaysia
Ms Norkhadhra Nawawi (Secretariat)	Malaysian Technical Standards Forum Bhd
Ms Nuramirah Abd Ajib/	American Malaysian Chamber of Commerce
Mr Salim Mohamad Ghani	
Mr Sazali Musa	Celcom Axiata Berhad
Mr Hanaffy Geoffrey Ramli	Digi Telecommunication Sdn Bhd
Mr Chai Ko Wei/	Maxis Broadband Sdn Bhd
Mr Goh Gee Han/	
Dr Mun Wai Yuen/	
Mr Teoh Khang Loon/	
Ms Yazma Mat Raschid	
Mr Adil Hidayat Rosli	My6 Initiative Berhad
Mr Ahmad Faizan Pardi	SIRIM QAS International Sdn. Bhd.
Mr Najib Fadil Mohd Bisri	Telekom Malaysia Berhad
Mr Mohd Zahrain Zainol/	webe digital sdn bhd
Ms Siti Najwa Muhammad	

By invitation:

Ms Ng Hsiao Ying	Individual Expert

MALAYSIAN TECHNICAL STANDARDS FORUM BHD

MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia, Jalan Impact
63000 Cyberjaya,
Selangor Darul Ehsan

Tel: (+603) 8320 0300
Fax: (+603) 8322 0115
Website: www.mtsfb.org.my