Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission

GUIDELINES ON IPv6 IMPLEMENTATION AND COMPLIANCE TEST

Notice:

The information contained in this document is intended as a guide only. For this reason it should not be relied on as legal advice or regarded as a substitute for legal advice in individual cases. Parties should still refer to the legislative provisions contained in the law.

Malaysian Communications and Multimedia Commission
Jalan IMPACT Off Persiaran Multimedia
63000 CYBERJAYA
Selangor Darul Ehsan
Tel: +60 3-8688 8000
Fax: +60 3-8688 1000
Website: www.skmm.gov.my

Committee Representation

These guidelines have been developed in collaboration with the Malaysian Technical Standards Forum Bhd (MTSFB). This document is intended to provide a guideline on IPv6 Implementation and Compliance Test for the industry in Malaysia.

The contents of these guidelines were developed by MTSFB's IPv6 Working Group (WG). The working group consists of the representatives from the following organisations (in alphabetical order):

a) .myDomain Registry

b) Celcom Bhd

c) Internet Society Malaysian Chapter

d) MIMOS Bhd

e) National Advanced IPv6 Centre

f) NTT MSC Sdn Bhd

g) Optical Communication Engineering Sdn Bhd

h) Packet One Networks (Malaysia) Sdn Bhd

i) Telekom Malaysia Berhad

These guidelines should be read together with the Communications and Multimedia Act 1998 (CMA), the relevant subsidiary legislations, instruments, codes and guidelines that have been issued by the Malaysian Communications and Multimedia Commission (MCMC) pursuant to the CMA.

Compliance with this Guideline does not itself confer immunity from legal obligations.

TABLE OF CONTENTS

Executive Summary 5
1 Objectives 7
2 Scope 7
3 Key IP Concepts 7
3.1 IP 7
3.2 IP Address 7
3.4 IPv6 8
3.5 IPv6 Header 8
3.6 IPv6 Addresses 8
3.7 IPv6 IETF Documents 9
4 IPv6 Benefits 11
4.1 Technical Benefits 11
4.2 Increased Address Space 11
4.3 Security 11
4.4 Mobility 12
4.5 QoS 12
4.6 Route Aggregations 12
4.7 Neighbour discovery and address auto-configuration 13
4.8 Other Benefits 13
5 IPv6 Implementation Consideration 13
5.1 Considerations for IPv4 to IPv6 Migration 13
5.2 IPv6 addressing scheme 13
5.3 Equipment 14
5.4 Dual Stack 14
5.5 Local Domain (.my) 14
5.6 IPv6 Features 14
5.7 Native IPv6 Support 14
5.8 IPv6 Readiness on Internet Upstream 14
5.9 IPv6 Cost 14
6 IPv6 Implementation Requirements 15
6.1 Basic Requirements 15
6.2 Other Optional Features 15
6.3 Migration Mechanisms 15
6.4 Inter-ISP Connectivity 16
6.5 Internal IGP 16
6.6 Advanced Services 16
6.7 Dial-up or xDSL 16
7 IPv6 Migration Approach 16
7.1 Dual Stack Network 17

7.2 Tunnelling 17
7.3 Translation mechanism 17
8 Regulatory Compliance 18
8.1 Self Declaration 18
8.2 Timeline 19
8.3 Responsibility 19
8.4 Declaration Form 19
8.5 Records 19
8.6 Audit 19
8.7 Notice 20
8.8 Non - Disclosure Agreement 20
8.9 Frequency 20
8.10 Criteria 20
8.11 Security 21
APPENDIX A: Declaration Form 22
APPENDIX B: IPv6 Compliant Test Plan 25
Acknowledgements 33

Executive Summary

This document served as a guideline to all Malaysian Internet Service Providers (ISP), Telcos and other interested parties on IPv6 implementation and compliance test.

Internet Protocol version 6 (IPv6) is a next-generation communications protocol designed to be used on the public Internet and private service provider infrastructure to support the move and development towards a converged system of voice, video, and data communications i.e. Next Generation Network (NGN). The current version used is the Internet Protocol version 4 (IPv4).

IPv4 is a robust and scalable protocol, but it is not immune to the retrospective poor design and planning considerations when viewed from a current socio-economic environment demand perspective. The design of IPv4 is over 25 years old with little or no changes to the protocol and its communications method has little or no foresight as to the potential growth of the Internet.

The transformation of the Internet in the 1990s, from a closed research network to an open commercial network that is perceived to be incapable of supporting the exponential growth and demands experienced, has pushed the Internet Engineering Task Force (IETF) to design a new version of Internet Protocol (IP). The IETF is responsible for producing technical and engineering documents that influence the design, use, and management of the Internet. These documents include protocol standards, best current practices, and related informational documents of various kinds.

While there are no real fundamental and operational differences between the two protocols per se, IPv6 inherently provides the following enhancements over IPv4:

a) extensive IP addresses available;

b) plug and play support (PnP);

c) inherent security (IPSec) features;

d) mandatory quality of service (QoS) standards;

e) mobility support;

f) future-proofing (via header extensions).

The then Ministry of Energy, Water and Communications (MEWC) and MCMC have deployed a national IPv6 implementation targets through the Malaysian Information, Communications and Multimedia Services 886 strategy (MyICMS 886) and have identified the need for Malaysia to deploy IPv6 as the following:

a) a new area to increase its' competitiveness in ICT sector;

b) set itself in par with the advanced nations in the Internet which currently has a dominant share of Internet address space;

c) paving the road to the use of the Next Generation Internet;

d) creating new markets for mobile and cellular application;

e) ability to be globally connected for every person.

Source: *MEWC National IPv6 Technology Forum (17 November 2006)*

Note: *MEWC has been re-organized as Ministry of Energy, Green Technology and Water (MEGTW) and Ministry of Information, Communication and Culture (MICC).*

1 Objectives

The objective of this document is to provide a guideline on IPv6 Implementation and Compliance Test for the industry. The document provides information on:

a) basic IPv6 information;

b) IPv6 implementation options;

c) recommended basic and advanced IPv6 features;

d) IPv6 compliance test plan;

e) transition considerations;

f) IPv6 technology roadmap.

2 Scope

This document covers the following areas:

a) IPv6 implementation options;

b) minimum criteria for IPv6 implementation;

c) recommended self-declaration process;

d) recommended testing procedures;

e) reporting structure;

3 Key IP Concepts

3.1 IP

Internet Protocol (IP) enables a packet of data to traverse multiple networks on the way to its final destination solely based on their addresses.

3.2 IP Address

IP address is a numerical label assigned to each networking device that uses the Internet Protocol for communication. This address is used to uniquely identify a device on a network.

3.3 IPv4

Internet Protocol version 4 (IPv4) uses 32 bits of address. Currently the most widely implemented version of the internet protocol.

3.4 IPv6

Internet Protocol version 6 (IPv6) is the next-generation communications protocol designed to succeed the Internet Protocol version 4 exhaustion. IPv6 uses 128 bits of address.

3.5 IPv6 Header

<table>
<tr><td>Version (4)</td><td>Traffic Class (8)</td><td colspan="2">Flow Label (20)</td></tr>
<tr><td colspan="2">Payload Length (16)</td><td>Next Header (8)</td><td>Hop Limit (8)</td></tr>
<tr><td colspan="4">Source Address (128 bits)</td></tr>
<tr><td colspan="4">Destination Address (128 bits)</td></tr>
</table>

Figure 1: IPv6 Header

The IPv6 header is 40 bytes long and the format consists of Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address and Destination Address.

3.6 IPv6 Addresses

IPv6 addresses are typically composed of two logical parts: a 64-bit network prefix and a 64-bit host part. IPv6 addresses are normally written as eight groups of four hexadecimal digits, where each group is separated by a colon (:).

Addresses are n:n:n:n:n:n:n:n, n = 4 digit hexadecimal integer, 16 x 8 = 128-bit address.

Below are the types of IPv6 addresses;

No.	Address Type	IPv6 notation	Address Representation
1	Loopback	::1/128	::1
2	Multicast	FF00::/8	FF01::101
3	Link Local	FE80::/10	fe80::20f:b0ff:fef1:8b5b
4	Global	Everything else	2001:5c0:1000:a::561

Table 1: IPv6 addresses

3.7 IPv6 IETF Documents

The **IETF** is an open standard organisation that makes the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. By tradition, all IETF documents are published as "Requests for Comments", or **RFC**s.

Note that not all RFCs represent IETF standards -- some are just informational, and some are not even intended to be taken seriously. For more information about the nature of RFCs, see **RFC1796: Not All RFCs are Standards.**

Some of the RFCs that are related to IPv6 are shown in the Table 2 below;

No.	IPv6 Features	RFC
1	Internet Protocol, Version 6 (IPv6) Specification	RFC 2460
2	Neighbour Discovery for IP Version 6 (IPv6)	RFC 2461
3	IPv6 Stateless Address Auto configuration	RFC 2462
4	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	RFC 2463
5	Path MTU Discovery for IP version 6	RFC 1981
6	OSPF For IPv6	RFC 2740
7	Use of BGP-4 Multi-protocol Extensions for IPv6 Inter-Domain Routing	RFC 2545
8	Multi-protocol Extensions for BGP-4	RFC 2858
9	IP Version 6 Addressing Architecture	RFC 4291
10	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	RFC 3315
11	DHCP IPv6 Prefix Delegation	RFC 3633
12	IPv6 Global Unicast Address Format	RFC 3587
13	DNS Extensions to Support IP version 6	RFC 1886
14	RIPng for IPv6	RFC 2080
15	IPv6 Multicast Address Assignments	RFC 2375
16	Security Architecture for the Internet Protocol	RFC 2401
17	IP Authentication Header	RFC 2402
18	The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header	RFC 2404
19	IP Encapsulating Security Payload (ESP)	RFC 2406
20	The Internet Security Domain of Interpretation for ISAKMP	RFC 2407

No.	IPv6 Features	RFC
21	Internet Security Association and Key Management Protocol	RFC 2408
22	Internet Key Exchange (IKE)	RFC 2409
23	Transmission of IPv6 Packets over Ethernet Networks	RFC 2464
24	Transmission of IPv6 Packets over FDDI Networks	RFC 2467
25	IP Version 6 over PPP	RFC 2472
26	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	RFC 2474
27	An Architecture for Differentiated Services Framework	RFC 2475
28	IPv6 over ATM Networks	RFC 2492
29	Transmission of IPv6 Packets over Frame Relay Networks Specification	RFC 2590
30	Assured Forwarding PHB	RFC 2597
31	An Expedited Forwarding PHB	RFC 2598
32	A Single Rate Three Colour Marker	RFC 2697
33	A Two Rate Three Colour Marker	RFC 2698
34	Multicast Listener Discovery (MLD) for IPv6	RFC 2710
35	Network Address Translation-Protocol Translation (NAT-PT)	RFC 2766
36	Transition Mechanisms for IPv6 Hosts and Routers	RFC 2893
37	Connection of IPv6 Domains via IPv4 Clouds	RFC 3056
38	An Anycast Prefix for 6to4 Relay Routers	RFC 3068
39	Generic Routing Encapsulation over CLNS Networks	RFC 3147
40	RADIUS and IPv6	RFC 3162
41	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiated Protocol (SIP) Servers	RFC 3319
42	Default Address Selection for Internet Protocol version 6 (IPv6)	RFC 3484
43	Change of Authorization	RFC 3576
44	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	RFC 3646
45	Stateless DHCP Service for IPv6	RFC 3736
46	Mobility Support in IPv6	RFC 3775
47	Multicast Listener Discovery Version 2 (MLDv2) for IPv6, June 2003	RFC 3810
48	Cisco Systems NetFlow Services Export Version 9	RFC 3954

No.	IPv6 Features	RFC
49	Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address	RFC 3956
50	IPv6 Scoped Address Architecture	RFC 4007
51	Default Router Preferences and More-Specific Routes	RFC 4191
52	Unique Local IPv6 Unicast Addresses	RFC 4193
53	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	RFC 4214
54	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	RFC 4443
55	IPv6 Unicast Address Assignment Considerations	RFC5375

Table 2: IPv6 Documents

4 IPv6 Benefits

These are the key benefits brought forth by the IPv6 in comparison to IPv4:

4.1 Technical Benefits

Some of the technical benefits of IPv6 are:

4.2 Increased Address Space

IPv6 provides 3.4 x 10^{38} = 340 trillion trillion trillion addresses - about 670 quadrillion addresses per square millimetre of the Earth's surface.

4.3 Security

IPv4 also offers IPSec support. However, IPv4's support for IPSec is optional. By contrast, the RFC4301 mandates for IPv6 to use IPSec in all nodes. IPSec consists of a set of cryptographic protocols that provide for securing data communication and key exchange. IPSec uses two wire-level protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP).

The first protocol provides for authentication and data integrity. The second protocol provides for authentication, data integrity, and confidentiality. In IPv6 networks both the AH header and the ESP header are defined as extension headers. Additionally, IPSec provides for a third suite of protocols for protocol negotiation and key exchange management known as the Internet Key Exchange (IKE).

This protocol suite provides the initial functionality needed to establish and negotiating security parameters between endpoints. Additionally, it keeps track of this information to guarantee that communication continues to be secure up to the end.

4.4 Mobility

Mobile IPv6 (MIPv6) is an enhanced protocol supporting roaming for a mobile node, so that it can move from one network to another without losing IP-layer connectivity (as defined in RFC 3775). RFC 3344, *IP Mobility Support for IPv4*, describes Mobile IP concepts and specifications for IPv4. Nevertheless, using Mobile IP with IPv4 has various limitations, such as limited address space, dependence on address resolution protocol (ARP), and challenges with handover when a device moves from one access point to another.

Mobile IPv6 uses IPv6's vast address space and *Neighbour Discovery (*RFC 4861*)* to solve the handover problem at the network layer and maintain connections to applications and services if a device changes its temporary IP address. Mobile IPv6 also introduces new security concerns such as *route optimization (*RFC 4449*)* where data flow between the home agent and mobile node will need to be appropriately secured.

4.5 QoS

IP (for the most part) treats all packets alike, as they are forwarded with best effort treatment and no guarantee for delivery through the network. TCP (Transmission Control Protocol) adds delivery confirmations but has no options to control parameters such as delay or bandwidth allocation. QoS offers enhanced policy-based networking options to prioritize the delivery of information. Existing IPv4 and IPv6 implementations use similar QoS capabilities, such as Differentiated Services and Integrated Services, to identify and prioritize IP-based communications during periods of network congestion.

Within the IPv6 header, two fields can be used for QoS, the *Traffic Class* and *Flow Label* fields. The new Flow Label field and enlarged Traffic Class field in the main IPv6 header allow more efficient and better differentiations of various types of traffic. The new Flow Label field can contain a label identifying or prioritizing a certain packet flow such as voice over IP (VoIP) or videoconferencing, both of which are sensitive to timely delivery. IPv6 QoS is still a work in progress.

4.6 Route Aggregations

IPv6 incorporates a hierarchal addressing structure and has a simplified header allowing for improved routing of information from a source to a destination. The large amount of address space allows organizations with large numbers of connections to obtain blocks of contiguous address space. Contiguous address space allows organizations to aggregate addresses under one prefix for identification on the Internet.

This structured approach to addressing reduces the amount of information Internet routers must maintain and store and promotes faster routing of data. Additionally, it is envisioned that IPv6 addresses will primarily be allocated only from Internet

Service Providers (ISPs) to customers. This will allow for ISPs to summarize route advertisements to minimize the size of the IPv6 Internet routing tables which eventually increases routing efficiency.

4.7 Neighbour discovery and address auto-configuration

Neighbour Discovery (ND) is the mechanism responsible for router and prefix discovery, duplicate address and network un-reachability detection, parameter discovery, and link-layer address resolution. This protocol is entirely network-layer based3. ND operates in tandem with auto-configuration, which is the mechanism used by IPv6 nodes to acquire either stateful or stateless configuration information.

In the stateless mode, all nodes get what they need for global communication, including potential illegal ones. In stateful mode, configuration information can be provided selectively, reducing the possibility for rogue nodes. Both ND and address auto-configuration contribute to make IPv6 more secure than its predecessor. IPv6 provides for TTL values of up to 255; it prevents against outside sourcing of ND packets or duplicate addresses.

4.8 Other Benefits

IPv6 provides the platform to support the services in the areas outlined in MyICMS886.

a) High Speed Broadband;

b) 3G & Beyond;

c) Mobile TV;

d) Digital Multimedia Broadcasting;

e) Digital Home;

f) Short Range Communications (e.g. RFID-based);

g) VoIP/Internet Telephony; and

h) Universal Service Provision.

5 IPv6 Implementation Consideration

5.1 Considerations for IPv4 to IPv6 Migration

5.2 IPv6 addressing scheme

There is no single guideline or formula that exercises the use of IPv6 addresses currently. Organisations shall select the normal practise of the IPv4 addresses assignment to assign those addresses until a proper guideline is made available.

5.3 Equipment

Equipment that are more than 5 years old will potentially have issues supporting IPv6. Major reinvestment is required for replacement. The above short comings should be taken into consideration by organizations when they do the network infrastructure planning in the course of their IPv6 transition.

5.4 Dual Stack

It is imperative to have system supporting dual stack implementation. Connectivity on pure IPv6 will be meaningless as content are primarily hosted on IPv4 network. Dual stack platform allows gradual migration from IPv4 to IPv6.

5.5 Local Domain (.my)

Local domain is crucial and imperative to encourage the domain migration for local content hosts. Therefore, "**.my**" domain registry plays an important role to support the IPv6 implementation for local domain. If this is not addressed, it will hinder the migration plan.

5.6 IPv6 Features

IPv4 and IPv6 are not compatible with each other. So, IPv6 software patches may not compliment the features available in IPv4. As such, people involved in IPv6 network infrastructure planning should do relevant study to decide on the features to be included in their organizations production network.

5.7 Native IPv6 Support

Implementer shall prioritise implementation of IPv6 on a new network since the native protocols are more stable and reliable.

5.8 IPv6 Readiness on Internet Upstream

Not all Internet upstream providers have IPv6 connectivity and their network backbones are IPv6 ready. Clarification need to be sought from the Internet service providers on their IPv6 capability.

5.9 IPv6 Cost

Though IPv6 software patches are made available for free by vendors, minimum hardware upgrade is unavoidable. If proper planning is made, most of the hardware

upgrades cost for IPv6 implementation could be absorbed through the natural upgrade/purchase cycle performed by organizations mostly every 3 years.

6 IPv6 Implementation Requirements

The recommended IPv6 requirements listed below shall be reviewed by the IPv6 WG from time to time to accommodate the development and challenges on IPv6 that may happen over time.

6.1 Basic Requirements

The basic requirements to implement IPv6 network should comprise of the IPv6 requirements as shown in Table 3 below. The minimum requirements should be extended to the other optional requirements depending on the network capabilities.

No.	IPv6 Features	RFC
1	Internet Protocol, Version 6 (IPv6) Specification	RFC 2460
2	Neighbour Discovery for IP Version 6 (IPv6)*	RFC 2461
3	IPv6 Stateless Address Auto configuration*	RFC 2462
4	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	RFC 4443
5	Path MTU Discovery for IP version 6	RFC 1981
6	Use of BGP-4 Multi-protocol Extensions for IPv6 Inter-Domain Routing**	RFC 2545
7	IP Version 6 Addressing Architecture	RFC 4291
8	IPv6 Global Unicast Address Format	RFC 3587
9	DNS Extensions to Support IP version 6	RFC 1886

Table 3: IPv6 requirements

Note : *** Applicable only for ISPs interconnect; essentially it is not mandatory for non-ISPs to adopt that feature if there is no interconnect requirement.*

6.2 Other Optional Features

6.3 Migration Mechanisms

No.	IPv6 Features	RFC
1	Transition Mechanisms for IPv6 Hosts and Routers	RFC 2893
2	Connection of IPv6 Domains via IPv4 Clouds	RFC 3056

Table 4: Migration Mechanisms

6.4 Inter-ISP Connectivity

No.	IPv6 Features	RFC
1	Multi-protocol Extensions for BGP-4	RFC 2858

Table 5: Inter-ISP Connectivity

6.5 Internal IGP

No.	IPv6 Features	RFC
1	OSPF For IPv6	RFC 2740
2	RIPng for IPv6	RFC 2080

Table 6: Internal IGP

Remark: *ISPs can opt for option 1 or 2.*

6.6 Advanced Services

No.	IPv6 Features	RFC
1	IPv6 Multicast Address Assignments	RFC 2375
2	Security Architecture for the Internet Protocol	RFC 2401
3	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	RFC 2474
4	An Architecture for Differentiated Services Framework	RFC 2475
5	Mobility Support in IPv6	RFC 3775

Table 7: Advanced Services

6.7 Dial-up or xDSL

No.	IPv6 Features	RFC
1	IP Version 6 over PPP	RFC 2472
2	RADIUS and IPv6	RFC 3162

Table 8: Dial-up or xDSL

7 IPv6 Migration Approach

Three (3) main migration techniques have been defined by the IETF Next Generation Transition (NGTrans) working group.

7.1 Dual Stack Network

This approach requires hosts and routers to implement both IPv4 and IPv6 protocols. This enables networks to support both IPv4 and IPv6 services and applications during the transition period in which IPv6 services emerge and IPv6 applications become available.

At present, the dual stack approach is a fundamental mechanism for introducing IPv6 in existing IPv4 architectures and will remain heavily used in the near future. The drawback is that an IPv4 and IPv6 addresses must be available for every dual stack machine.

7.2 Tunnelling

Tunnelling enables the interconnection of IP clouds. For instance, separate IPv6 networks can be interconnected through a native IPv4 service by means of a tunnel. IPv6 packets are encapsulated by a border router before transportation across an IPv4 network and de-encapsulated at the border of the receiving IPv6 network. Tunnels can be statically or dynamically configured or implicit (6 to 4, 6 over 4).

The TB (Tunnel Broker) approach has been proposed to automatically manage tunnel requests coming from the users and ease the configuration process. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is a recent technique to avoid tunnel manual configuration. In later stages of transition, tunnels will also be used to interconnect remaining IPv4 clouds through the IPv6 infrastructure.

7.3 Translation mechanism

Translation is necessary when an IPv6 host has to communicate with an IPv4 host. The IP header at least has to be translated but the translation will be more complex if the application processes IP addresses. Such translation inherits most of the problems of IPv4 Network Address Translators.

ALGs (Application-Level Gateways) are required to translate embedded IP addresses, recomputed checksums, etc. SIIT (Stateless IP/ICMP Translation) and NAT-PT (Network Address Translation - Protocol Translation) are the associated translation techniques. A blend of translation and the dual stack model, known as DSTM (Dual Stack Transition Mechanism), has been defined to allow for the case where insufficient IPv4 addresses are available. Similar to the tunnelling techniques, translation can be implemented in border routers and hosts.

This complex set of coexistence and transition techniques can be “mixed and matched” in many ways. An example for Static NAT-PT is given below:

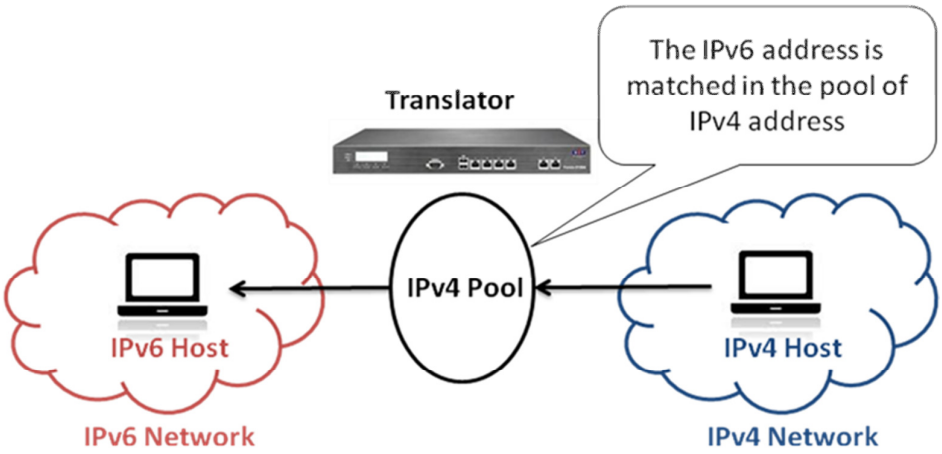


Figure 2: The Translation of IPv4 to IPv6

The IPv6 addresses will be matched to IPv4 addresses thereby allowing IPv4 hosts to send traffic to IPv6 hosts.

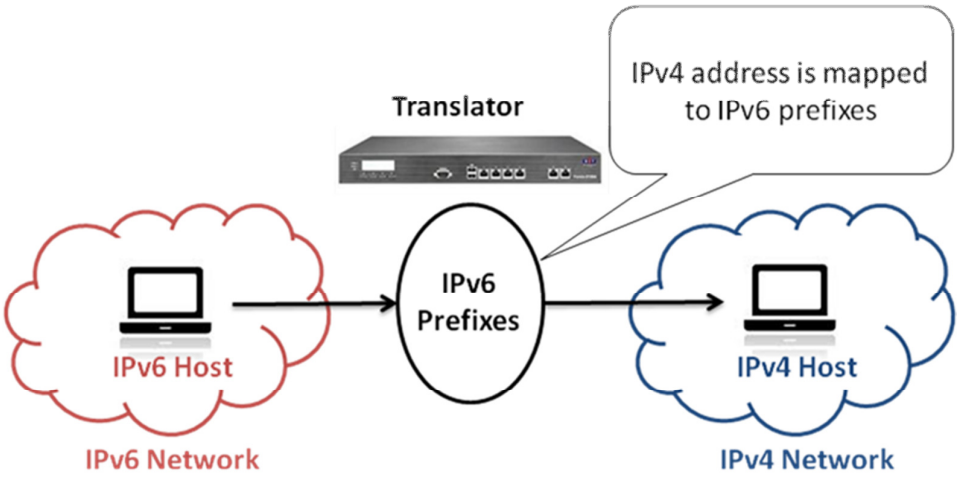


Figure 3: The Translation of IPv6 to IPv4

The IPv4 addresses will be mapped to IPv6 prefixes. This allows IPv6 hosts to send traffic to IPv4 hosts.

8 Regulatory Compliance

8.1 Self Declaration

The best mechanism to check compliant is through self declaration by the organization to the regulator. This is in accordance with the direction towards self-regulation.

The key requirements from the regulator on the compliance:

a) acquire IPv6 addresses from APNIC

b) announce IPv6 global addresses

c) support IPv6 capable DNS

The regulator shall send a letter requesting for the self-declaration to the relevant organizations. The organization shall revert within 14 working days.

8.2 Timeline

The organization must submit the Declaration Form upon request to the regulator on the IPv6 network implementation readiness before the stipulated deadline determined by the regulator.

8.3 Responsibility

The organization is responsible to declare to the regulator on the status of IPv6 network implementation. The declaration must be submitted and undersigned by one (1) key personnel in the organization either the Chief Executive Officer or the Chief Technical Officer or someone who is of equivalent stature.

8.4 Declaration Form

The Declaration Form is as per **Appendix 1.**

8.5 Records

The organization shall keep a set of the followings for auditing and monitoring purposes.

a) IPv6 network (architecture) diagram

b) Test records conducted on all the features implemented for future verification by the regulator

c) Implementation and Maintenance records

8.6 Audit

The Regulator may conduct audit on the organizations that have declared to be IPv6 compliant to verify their readiness.

8.7 Notice

The Regulator shall give thirty (30) working days' notice to the organization through an official letter to the Chief Executive Officer or Chief Technical Officer. The letter should indicate the following information.

a) Details of the appointed person/organization to perform the audit.

   i) Name

   ii) I/C Number

   iii) Letter of appointment

b) The scope of test is as per **Appendix 2**.

c) Proposed date and test duration.

   i) The regulator shall indicate the proposed date and test duration to the organization

   ii) The organisation may request for a different date if the proposed date is inconvenient or due to unforeseen circumstances

d) Requirements.

   i) The regulator shall indicate resources required for the audit such as dedicated PC connection and test gears which are to be provided by the organization/ISP

   ii) The organization is to appoint internal staff to participate in the test

8.8 Non - Disclosure Agreement

The organization may request the appointed person/organization to sign a non-disclosure agreement to protect the confidentiality of information provided.

8.9 Frequency

The regulator shall periodically audit the ISPs for IPv6 compliance.

8.10 Criteria

The person/organization qualified to perform the audit must have the below minimum criteria.

a) 5 years experiences in IP Planning, Implementation and Service Operations

b) 3 years experiences in IPv6 deployment

c) High integrity

d) Not allowed to perform any other activities beyond the test scope defined by the regulator

8.11 Security

The appointed person/organisation to conduct the audit shall not compromise the network security and integrity.

9 Conclusion

IPv6 deployment has been gradually increased over the past of few years and is now in an accelerated mode due to insufficient IPv4 addresses. Transition mechanisms allow existing IPv4 networks to coexist and interoperate with IPv6 networks, systems, and services. These transition mechanisms cover a wide range of technologies and transition scenarios. Organizations should plan their deployment and account for the full lifecycle of equipment from inception to disposal. This document is presented as a guideline to Malaysian Internet Service Provider, Telcos and other interested parties when considering migration to IPv6.

APPENDIX A: Declaration Form

Chairman
Malaysian Communications and Multimedia Commission
Off Persiaran Multimedia
63000 Cyberjaya
Selangor

Date: ……

DECLARATION FOR THE SUBMISSION OF IPv6 COMPLIANCE

<table>
<tr><td>Company Name :</td><td colspan="3"></td></tr>
<tr><td rowspan="12">Network</td><td rowspan="6">☐ ISP</td><td rowspan="4">☐ Fixed</td><td>☐ Core</td></tr>
<tr><td>☐ Edge/Access</td></tr>
<tr><td>☐ Core and Edge/Access</td></tr>
<tr><td>☐ Peering</td></tr>
<tr><td rowspan="3">☐ Mobile</td><td>☐ Core</td></tr>
<tr><td>☐ Edge/Access</td></tr>
<tr><td>☐ Core and Edge/Access</td></tr>
<tr><td rowspan="6">☐ Non-ISP</td><td rowspan="3">☐ Fixed</td><td>☐ Core</td></tr>
<tr><td>☐ Edge/Access</td></tr>
<tr><td>☐ Core and Edge/Access</td></tr>
<tr><td rowspan="3">☐ Mobile</td><td>☐ Core</td></tr>
<tr><td>☐ Edge/Access</td></tr>
<tr><td>☐ Core and Edge/Access</td></tr>
<tr><td>IP Address</td><td colspan="3"></td></tr>
<tr><td>Declaration Date</td><td colspan="3"></td></tr>
</table>

IPv6 Compliant Checklists:

No.	Basic IPv6 Features	RFC	Status *(Yes/No/NA)*
1	Internet Protocol, Version 6 (IPv6) Specification	RFC 2460	
2	Neighbour Discovery for IP Version 6 (IPv6)	RFC 2461	
3	IPv6 Stateless Address Auto configuration	RFC 2462	
4	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	RFC 4443	
5	Path MTU Discovery for IP version 6	RFC 1981	
6	Use of BGP-4 Multi-protocol Extensions for IPv6 Inter-Domain Routing *	RFC 2545	
7	IP Version 6 Addressing Architecture	RFC 4291	
8	IPv6 Global Unicast Address Format	RFC 3587	
9	DNS Extensions to Support IP version 6	RFC 1886	

Note: *NA means Not Applicable*
** Only applicable for ISPs Interconnect*

Remark (If any):

I, _____*(Name)*_____, the undersigned, as the _____*(Designation)*_____ for IPv6 Compliance, confirm and acknowledge that the factual information provided therein is to the best of our knowledge, information and belief, true, accurate and have no material omissions and that any opinion expressed is honestly held.

Signed:

……
Chief Executive Officer/ Chief Technical Officer

APPENDIX B: IPv6 Compliant Test Plan

B.1 Purpose

The purpose of this test plan is to provide test objectives, expected results and test procedures for the ISPs IPv6 Compliance Tests.

B.2 Scope of Acceptance Test Plan

The scope of the testing will cover the scope of test specified in the Guideline on IPv6 Implementation and Compliance Test, section 8.6.

B.3 Definition and Abbreviation

Abbreviation	Meanings
BGP	Border Gateway Protocol
DUT	Device Under Test
ISP	Internet Service Provider
MTU	Maximum Transmission Unit
MPBGP	Multi-Protocol Border Gateway Protocol
NUT	Network Under Test
RFC	Request For Comments

B.4 Basic Requirements for IPv6 Compliance

The Basic Requirements for IPv6 Compliance Test shall be the basis for the test to be conducted:

No.	IPv6 Features	RFC
1	Internet Protocol, Version 6 (IPv6) Specification	RFC 2460
2	Neighbour Discovery for IP Version 6 (IPv6)	RFC 2461
3	IPv6 Stateless Address Auto configuration	RFC 2462
4	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	RFC 4443
5	Path MTU Discovery for IP version 6	RFC 1981
6	Use of BGP-4 Multi-protocol Extensions for IPv6 Inter-Domain Routing	RFC 2545
7	IP Version 6 Addressing Architecture	RFC 4291
8	IPv6 Global Unicast Address Format	RFC 3587
9	DNS Extensions to Support IP version 6	RFC 1886

Table B-1: IPv6 Basic Requirement

The ISPs can choose to deploy the following RFCs to achieve IPv6 connectivity

No.	IPv6 Features	RFC
1	OSPF for IPv6 (OSPFv3)	RFC 5340
2	RIPng for IPv6	RFC 2080
3	Routing IPv6 with IS-IS	RFC 5308
4	Basic Transition Mechanisms for IPv6 Hosts and Routers	RFC4213
5	Scenarios and Analysis for Introducing IPv6 into ISP Networks	RFC4029
6	Routing Aspects Of IPv6 Transition	RFC2185
7	IP Version 6 Addressing Architecture (Obsoletes RFC3513)	RFC4291
8	Requirements for IPv6 Prefix Delegation	RFC3769
9	IPv6 Global Unicast Address Format	RFC3587
10	Unique Local IPv6 Unicast Addresses	RFC4193
11	Deprecating Site Local Addresses	RFC3879
12	IPv6 Stateless Address Auto configuration	RFC4862
13	Default Address Selection for Internet Protocol version 6 (IPv6)	RFC3484
14	Neighbour Discovery for IP version 6 (IPv6)	RFC4861

Table B-2: IPv6 Connectivity Options

B.5 SCOPE OF TESTING

PHASE 1

Objective

ISP to demonstrate that they are capable of setting up IPv6 network in a confined environment.

Scope

No.	Test	Tools
1.	Each Network Under Test (NUT) physically and logically able to be assigned with IPv6 addresses	
2.	IPv6 devices in the NUT able to discover each other's presence	
3.	Network connectivity test is able to be performed by the NUT	• Ping

PHASE 2

Objective

ISP to demonstrate global connectivity with at least 1 peering.

Scope

No.	Test	Tools
1.	Each ISP must perform the IPv6 Forum ISP logo (mandatory) but the choice to insert the IPv6 Logo at their website is optional.	Monitor through the IPv6 ISP Logo Enabled Program website. http://www.ipv6forum.com/ipv6_enabled
2.	Each ISP will demonstrate at least 1 peer for global connectivity and is *strongly recommended to establish local peering over IPv6.*	• Ping • Trace route • Looking Glass • HTTP access to IPv6-ready website

PHASE 3

Objective

ISPs to demonstrate readiness to provide IPv6 connectivity to customer(s) from any segment of its services

Scope

1. Phase 3 Audit offers the flexibility for ISPs to define

a) the segment of service

b) it's customer or end user

c) method of providing IPv6 connectivity to the customer(s) via any of the following:

   i) dual-stack;

   ii) native IPv6 assignment; or

   iii) tunneling.

2. ISPs shall provide a brief explanation on why the items above were selected.

3. Test items to indicate accessibility/reach ability to both IPv4 and IPv6 destinations.

Conditions

a) ISPs include both fixed and mobile operators.

b) Customer CPE/host has to support IPv6.

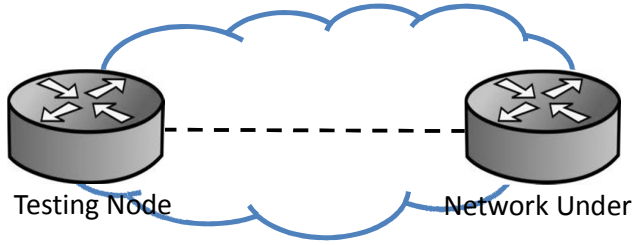
c) At least 2 months of notice is issued to ISPs prior to audit.

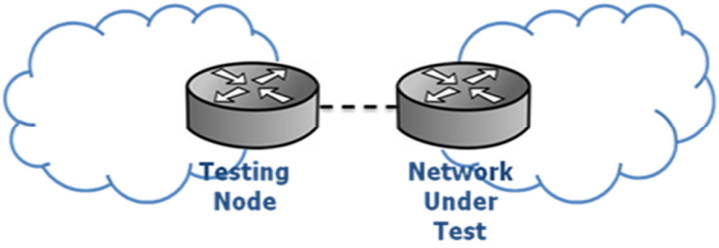
d) Should a site visit is required to the customer(s) premise, a tentative period/duration of visit should be given to ISP/customer at least 2 weeks in advance for necessary arrangements to be made.

e) Recommendation for disclaimer - Upon successful completion of the audit, the ISP has demonstrated its readiness to provide IPv6 connectivity to its customers from the selected segment of service. For further information on the IPv6 service delivery, kindly contact the respective ISP.

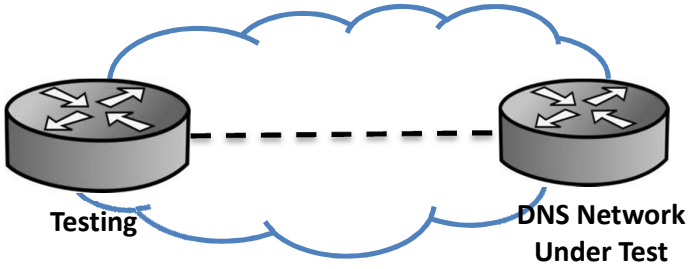
B.6 Test Items & Procedures

Test Item 1: Network Connectivity Tests This test item will cover item no. 1 to 5, 7 and 8 as stipulated in Table B-2.	
Purpose :	1. To ensure the Network Under Test (NUT) physically and logically able to be assigned with the IPv6 address. 2. To ensure IPv6 devices in the NUT able to discover each other's presence (link layer address, neighbour routers and reach ability) using Neighbour Discovery. 3. To ensure the IPv6 NUT able to be configure the testing node with the stateless or stateful mechanism (whichever decided by the ISPs IPv6 planning policy). 4. To ensure the network connectivity test is able to be performed by the NUT. 5. To ensure the NUT able to response to the path MTU discovery send by the testing node
Test Pre-requisite :	All the RFCs of 2460, 2461, 2462, 4443, 4291, 3587 and 1981 are followed as testing pre-requisite for the above.

Test Item 1: Network Connectivity Tests This test item will cover item no. 1 to 5, 7 and 8 as stipulated in Table B-2.	
Test Set-up :	
Test Procedures :	As per ISP's test procedurals (provided the above objectives are met).
Expected Results :	1. The testing node able to obtain address assigned by the NUT (from test objective 1 & 3). 2. The testing node able to ping the neighbour nodes in the same subnet in the NUT (from test objective 2). 3. The testing node able to ping the neighbour nodes in the different subnet in the NUT (from test objective 4). 4. The testing node able to receive variable MTU sizes from 1280 bytes to 9192 bytes (from test objective 5).
Observations & Results :	
Verified By :	**ISP** Name : _____ Designation : _____ Division : _____ Signature : _____ Date : _____ **MCMC** Name : _____ Designation : _____ Division : _____ Signature : _____ Date : _____

Test Item 2: Inter-ISP Inter-Connectivity Tests	
Purpose :	1. To ensure that ISP comply and validated based on the IPv6Forum ISP enabled programme. 2. To establish at least 1 international peering.
Test Pre-requisite :	Recommend ISPs that have not completed Phase 1 but successfully completed Phase 2, will automatically comply with Phase 1 requirements.
Test Set-up :	 Test will be conducted from .my Domain Registry using NTT America IPv6 Looking Glass - https://www.us.ntt.net/support/looking-glass/. For local peering, test should be conducted from the testing network.
Test Procedures :	As per ISP's test procedures (provided the above objectives are met).
Expected Results :	1. The ISP has participated in the IPv6Forum ISP IPv6 enabled program. 2. The testing network able to demonstrate at least 1 international IPv6 peering. 3. The testing node able to ping the nodes located in different ISP's network. 4. The testing node able to trace to a destination in the ISP's network. 5. Able to view IPv6 websites hosted in the ISP's network.
Observations & Results :	

Test Item 2: Inter-ISP Inter-Connectivity Tests	
Verified By :	**ISP** Name : _____ Designation : _____ Division : _____ Signature : _____ Date : _____ **MCMC** Name : _____ Designation : _____ Division : _____ Signature : _____ Date : _____

Test Item 3: DNS Extensions to Support IPv6 This test item will cover item no. 9 as stipulated in Table B-2.	
Purpose :	To verify the testing node is able do AAAA query and obtain reply
Test Pre-requisite :	The RFCs of 1886 is followed as testing pre-requisite for the above.
Test Set-up :	
Test Procedures :	As per ISP's test procedurals (provided the above objectives are met).
Expected Results :	The testing node able to obtain AAAA records from the NUT DNS.
Observations & Results :	
Verified By :	**ISP** Name : _____ Designation : _____ Division : _____ Signature : _____ Date : _____ **MCMC** Name : _____ Designation : _____ Division : _____ Signature : _____ Date : _____

Acknowledgements

Members of the Internet Protocol version 6 Working Group:

1. Gopinath Rao (Chairman) – MIMOS Berhad
2. Ronhazli Adam (Vice-Chairman) – Celcom Axiata Berhad
3. Azura Mat Salim (Secretary) – Telekom Malaysia Berhad
4. Lai Heng Choong – .myDomainRegistry
5. Julian VincentInternet – Society Malaysian Chapter
6. Raha Kumar, M – National Advanced IPv6 Centre
7. Teoh Kiat Jin – NTT MSC Sdn Bhd
8. Simon Teh Chee Hong – NTT MSC Sdn Bhd
9. CK Tan – Optical Communication Engineering Sdn Bhd
10. Lee Seng Hoon – Packet One Networks (Malaysia) Sdn Bhd

