

TECHNICAL CODE

GUIDELINE FOR THE DEPLOYMENT OF INTERNET PROTOCOL VERSION 6 (IPv6)

Developed by



Registered by



Registered date:

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 interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)

MCMC Tower 1
Jalan Impact, Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
<http://www.skmm.gov.my>

OR

Malaysian Technical Standards Forum Bhd (MTSFB)

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

Tel: +60 3 8322 1441/1551
Fax: +60 3 8322 0115
<http://www.mtsfb.org.my>

CONTENTS

	Page
CONTENTS.....	ii
Committee Representation	v
FOREWORD	vi
1. Scope	1
2. Normative references.....	1
3. Abbreviations	1
4. Introduction to IPv6	1
4.1 Limitations of IPv4	2
4.2 IPv6 History	3
4.3 Major Features of IPv6	3
4.3.1 Extended IPv6 Address	3
4.3.2 Autoconfiguration	4
4.3.3 Header Structure.....	4
4.3.4 Extension Headers.....	4
4.3.5 Mandatory Internet Protocol Security (IPsec) Support	5
4.3.6 Mobility	5
4.3.7 Quality of Service (QoS)	5
4.3.8 Route Aggregation	6
4.3.9 Efficient Transmission.....	6
4.4 IPv4 and IPv6 Threat Comparison	6
4.5 Motivations for IPv6 Deployment.....	7
5. IPv6 Addressing and Address Assignment.....	9
5.1 IPv6 Addressing.....	9
5.1.1 Simplifying IPv6 Addresses	11
5.1.2 IPv6 Address Types.....	12
5.1.3 IPv6 Address Scope	12
5.2 IPv6 Address Allocation.....	14
5.2.1 IPv6 Address Assignment.....	14
5.2.2 Obtaining Global IPv6 Addresses.....	16
5.2.2.1 Obtaining IP addresses and Autonomous System (AS) number from APNIC ...	17
6. Challenges of Technology, Resources and Organization.....	18
6.1 Technology	19
6.1.1 Tools	19
6.1.1.1 Network Management System (NMS)	19
6.1.1.2 IP Address Management (IPAM)	19
6.1.2 Devices and Application availability	20
6.1.3 Standard.....	20
6.2 Resources.....	20
6.2.1 Training & Expertise.....	20
6.2.2 Project Management.....	20
6.2.3 Timeline.....	20
6.2.4 Device Refreshment	21
6.3 Organization	21
6.3.1 Guideline	21
6.3.2 Justifying benefit	21

MCMC MTSFB TC TXXX:2015

6.3.3 Cost.....	22
7. IPv6 Deployment Strategy	22
7.1 Transition Mechanism.....	22
7.2 IPv4/IPv6 Dual Stack Environment.....	23
7.2.1 Deployment of Dual Stack Environment.....	23
7.2.2 Addressing in Dual Stack Environment	24
7.2.3 Security Implication of a Dual Stack Environment.....	24
7.3 Tunneling	25
7.3.1 Manually Configured Tunneling	26
7.3.2 GRE Tunneling	26
7.3.3 Automatic GRE Tunneling	26
7.3.4 6to4 Tunneling	26
7.3.5 ISATAP	26
7.3.6 Tunnel Brokers.....	27
7.4 Translation	27
7.5 IPv6 Deployment	27
7.5.1 Building the team	28
7.5.2 Goals, Requirements and Scope.....	30
7.5.3 Initiation Phase	32
7.5.4 Acquisition/Development Phase	34
7.5.5 Implementation	37
7.5.6 Operation and Maintenance.....	38
7.5.7 Disposition	39
8. Technology Education	39
8.1 Training Need / Knowledge Acquisition.....	40
8.1.1 Training Domains.....	40
8.1.2 Training Assessments.....	40
8.1.2.1 Certification compliance.....	40
8.1.3 Information Sharing.....	41
8.1.4 Resources.....	41
9. Summary	41

Figures

1. IPv6 Header Format (size in bits).....	4
2. IPv6 Address Format.....	10
3. 32-Bit Network Prefix.....	11
4. 64-Bit Network Prefix.....	11
5. IPv6 Address Assignment Scheme	15
6. Enterprise IPv6 Adoption.....	19
7. ISATAP Tunneling mechanism.....	27
8. IPv6 End-to-End Solution	32

Tables

1. Link-local address.....	13
2. IPv4-compatible IPv6 Address	13
3. IPv4-mapped IPv6 Address.....	13
4. Summary of IPv6 Tunneling Mechanism.....	25
5. Sample Project Team, Responsibilities and Workload.....	29

Annexes

A Abbreviations.....42
B Sample ISP Requirements Checklist44
C IETF Request for Comments (RFC).....45
Acknowledgements

MCMC MTSFB TC TXXX:2015

Committee Representation

Internet Protocol version 6 Working Group (IPv6 WG) under the Malaysian Technical Standards Forum Bhd (MTSFB), which developed this Technical Code, consists of representatives from the following organizations:

Asian Broadcasting Networks (M) Sdn Bhd (ABNxcess)

Celcom Axiata Berhad

Cisco Systems Malaysia

DiGi Telecommunications Sdn Bhd

Huawei Technologies

Jaring Communications Sdn Bhd

Maxis Broadband Sdn Bhd

MIMOS Berhad

My6 Initiative Berhad

Packet One Networks (Malaysia) Sdn Bhd

REDtone IoT Sdn Bhd

Telekom Malaysia Berhad

TIME dotCom Bhd

U Mobile Sdn Bhd

FOREWORD

This technical code for the Guideline For The Deployment of Internet Protocol Version 6 (IPv6) ('Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd ('MTSFB') via its Internet Protocol version 6 Working Group (IPv6 WG).

Migrating to IPv6 is about more than just address space. An organization must also begin to plan for proper transition to use IPv6. The transition to IPv6 gives an organization an opportunity to fix problems in its current environment. IPv6 addressing will allow more opportunities to aggregate addressing and simplify routing and access control rules if requirements are collected early.

This Technical Code was developed to assist organization or individuals to properly deploy IPv6 in their network. It provides basic information about IPv6, challenges in deploying IPv6 and the plan for deploying IPv6. Users can use this document together with other available resources to deploy IPv6 services in their network.

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

MCMC MTSFB TC TXXX:2015

GUIDELINE FOR THE DEPLOYMENT OF INTERNET PROTOCOL VERSION 6 (IPv6)

1. Scope

This Technical Code provides the basic understanding of IPv6 and guidance to organizations that are planning to deploy IPv6 technologies or are simply seeking a better understanding of IPv6.

The scope encompasses the IPv6 protocol and related specifications as well as general guidance on IPv6 deployment and integration planning in the following areas:

- a) Basic information about IPv6;
- b) IPv6 addressing information;
- c) Challenges of technology, resources and organizations;
- d) IPv6 deployment; and
- e) Technology education.

This Technical Code is intended primarily for network engineers and administrators who are responsible for planning, building, and operating IP networks.

2. Normative references

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

Draft-ietf-v6ops-dc-ipv6-01, *IPv6 Operational Guidelines for Datacenters*

Draft-ietf-opsec-v6-05, *Operational Security Considerations for IPv6 Networks*

Global IPv6 Strategies, From Business Analysis to Operational Planning, Cisco Press, 2008, Patrick Grossetete, Ciprian P. Popoviciu and Fred Wettling

Guidelines for the Secure Deployment of IPv6, National Institute of Standards and Technology (NIST), Special Publication 800-119, December 2010, Sheila Frankel, Richard Graveman, John Pearce and Mark Rooks

IETF Request For Comments (RFC)

IPv6 Essentials, 2nd Edition, O'Reilly Media, May 2006, Silvia Hagen

3. Abbreviations

For the purposes of this Technical Code, the following abbreviation applies. See Annex A.

4. Introduction to IPv6

Internet Protocol version 6 (IPv6) is a new network layer protocol that was introduced as an enhancement to Internet Protocol version 4 (IPv4), the protocol in use since 1980s. There are numerous upgrades in IPv6. Most significantly, in comparison with IPv4, IPv6 has increased its network address

size from 32 to 128 bits. This provides more than enough addresses to satisfy the global demand for unique IP addresses for networking devices. It is a protocol designed to handle the growth rate of the internet and to cope with the demanding requirements of services, mobility, and end-to-end security.

This section provides an overview of IPv6 as a foundation for later sections. The section starts with the early history of IPv6 and the limitations of IPv4, followed by descriptions of the major features of the IPv6 specifications. This is followed by a threat comparison between IPv4 and IPv6 and concludes with motivations for deploying IPv6.

4.1 Limitations of IPv4

IPv4 (RFC 791, *Internet Protocol*) was designed over 30 years ago for a relatively small number of users. At that time, it seemed unlikely that personal computing technology would become as widespread as it is today. The rapid, universal adoption and growth of personal computing technologies, including IP networking, were unforeseen in 1981. At that time, the internet was used almost exclusively by scholars and researchers, and IPv4's 4.3 billion theoretically available addresses were considered to be more than sufficient.

As a result of growing internet use, IPv4's address capacity could not meet the demand. In practice, the supply of available IPv4 addresses has been limited since the early 1990s. Previously, an organization could apply for and receive an order of magnitude more IPv4 addresses than it could actually justify. However, as a result of regulatory advances, IP address allocations are now bound by strict policies that include formal justification to a Regional Internet Registry (RIR). During the 1990s, address allocation policies, along with address reuse and restriction technologies, were put into place to conserve IPv4 addresses.

Technologies widely adopted in response to the constrained supply of IPv4 addresses are network address translation (NAT) as specified in RFC 3022 and classless inter-domain routing (CIDR) as specified in RFC 4632. NAT essentially makes private IPv4 addresses (also known as non-routable addresses) at least partially functional on the global internet. Despite their adaptation to other uses, private IPv4 addresses were designed for testing and other non-production purposes and never intended to be usable on the internet. Nevertheless, a NAT-capable router positioned at an organization's boundary has the ability to connect an entire network of privately addressed nodes within the organization to the internet via a single routable IP address.

This technology saves IPv4 address space because nodes bearing private addresses are essentially "on" the internet but do not have globally unique IP addresses. Nevertheless, this address conservation technology can actually defeat certain aspects of the design intent of IPv4:

- a) network layer end-to-end security;
- b) peer-to-peer (host-to-host connectivity); and
- c) interoperability.

A host using private addressing behind a NAT device cannot have a full peer-to-peer relationship with another host via the internet or backbone enterprise network using globally unique addressing. This is because NAT does not allow communication sessions to be initiated from globally addressed nodes to the privately addressed nodes.

NAT traversal technologies are available to work around some of these barriers. They typically work in one of the two ways:

- a) by maintaining stateful address lookup tables and redirecting inbound traffic to appropriate private addresses; or
- b) by employing application layer gateways that listen for specific port numbers and redirect traffic according to pre-configured parameters.

MCMC MTSFB TC TXXX:2015

Neither of these approaches to NAT traversal lends itself to scalability or guarantees compatibility with all forms of NAT, not to mention the efforts put into each of these work-arounds. In addition, neither approach lends itself to dynamic configuration when, for example, hosts move or networks are renumbered.

Another limitation of IPv4 is that its design favoured interoperability over security and did not contain features that protected the confidentiality, integrity or availability of communications. For example, IPv4 could not cryptographically protect data from eavesdropping or manipulation and IPv4 did not provide a method for endpoints to authenticate each other. Over time, the open nature of IPv4 was increasingly a target of exploitation. The multi-path nature of the Internet, which was designed for high availability, also allows multiple attack vectors for a variety of threats. As a response, new technologies were added to IPv4 to provide needed security functionality.

4.2 IPv6 History

Efforts to develop a successor to IPv4 started in the early 1990s within the Internet Engineering Task Force (IETF). The objective was to solve the address space limitations as well as provide additional functionality. The IETF started the Internet Protocol Next Generation (IPng) work in 1993 to investigate different proposals and to make recommendations for further actions. The IETF recommended IPv6 in 1994 (the name Internet Protocol version 5 (IPv5) had previously been allocated to an experimental stream protocol) as specified in RFC 1752, *The Recommendation for IP Next Generation Protocol*. Several proposals followed; the Internet Engineering Steering Group approved the IPv6 recommendation and drafted a Proposed Standard on November 17, 1994. RFC 1883, *Internet Protocol, Version 6 (IPv6) Specification*, was published in 1995. The core set of IPv6 protocols became an IETF Draft Standard on August 10, 1998. This included RFC 2460, which replaced RFC 1883.

4.3 Major Features of IPv6

IPv6 has many new or improved features that make it significantly different from its predecessor. These features include extended address space, autoconfiguration, header structure, extension headers, IPsec, mobility, quality of service, route aggregation and efficient transmission.

This section discusses these features and compares specific aspects of IPv4 and IPv6 to help establish an understanding of the protocols' similarities and differences.

4.3.1 Extended IPv6 Address

Each IPv4 address is typically 32 bits long and is written as four decimal numbers representing 8-bit octets and separated by decimal points or periods.

An example address is 172.30.128.97.

Each IPv6 address is 128 bits long as defined in RFC 4291 and is written as eight 16-bit fields in colon-delimited hexadecimal notation.

An example is fe80:43e3:9095:02e5:0216:cbff:feb2:7474.

This new 128-bit address space provides an enormous number of unique addresses, 2^{128} (or 3.4×10^{38}) addresses, compared with IPv4's 2^{32} (or 4.3×10^9) addresses. That is enough for many trillions of addresses to be assigned to every human being on the planet.

Moreover, these address bits are divided between the network prefix and the host identifier portions of the address. The network prefix designates the network upon which the host bearing the address resides. The host identifier identifies the node or interface within the network upon which it resides. The network prefix may change while the host identifier can remain static. The static host identifier allows a device to maintain a consistent identity despite its location in a network. This enormous number of addresses allows for end-to-end communication between devices with globally unique IP addresses

and can better support the delivery of peer-to-peer services with data-rich content such as voice and video. Section 5 describes IPv6 addressing in detail.

4.3.2 Autoconfiguration

Essentially, plug-and-play networking defined in RFC 4862, *IPv6 Stateless Address Autoconfiguration*, is one of the most interesting and potentially valuable addressing features in IPv6. This feature allows devices on an IPv6 network to configure themselves independently using a stateless protocol.

In IPv4, hosts are configured manually or with host configuration protocols like Dynamic Host Configuration Protocol (DHCP); with IPv6, autoconfiguration takes this a step further by defining a method for some devices to configure their IP addresses and other parameters without the need for a server. Moreover, it also defines a method, renumbering, whereby the time and effort required to renumber a network by replacing an old prefix with a new prefix are vastly reduced.

4.3.3 Header Structure

The IPv6 header is much simpler than the IPv4 header and has a fixed length of 40 bytes, defined in RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*.

Even though this header is almost twice as long as the minimum IPv4 header, much of the header is taken up by two 16-byte IPv6 addresses, leaving only 8 bytes for other header information. This allows for improved fast processing of packets and protocol flexibility.

IPv6 datagrams use a structure that always includes a 40-byte base header and, optionally, one or more extension headers. This base header is like the header of IPv4 datagrams, though it has a different format.

Five IPv4 header fields have been removed: IP header length, identification, flags, fragment offset, and header checksum. The IPv6 header fields are as follows: version (IP version 6), traffic class (replacing IPv4's type of service field), flow label (a new field for Quality of Service (QoS) management), payload length (length of data following the fixed part of the IPv6 header), next header (replacing IPv4's protocol field), hop limit (number of hops, replacing IPv4's time to live field), and source and destination addresses.

The IPv6 header format is illustrated in Figure 1. The payload can be up to 64KB in size in standard mode, or larger with a jumbo payload option.

Version (4)	Traffic Class (8)	Flow Label (20)	
Payload Length (16)		Next Header (8)	Hop Limit (8)
Source Address (128)			
Destination Address (128)			

Figure 1. IPv6 Header Format (size in bits)

4.3.4 Extension Headers

An IPv4 header can be extended from 20 bytes to a maximum of 60 bytes, but this option is rarely used because it impedes performance and is often administratively prohibited for security reasons.

IPv6 has a new method to handle options, which allows substantially improved processing and avoids some of the security problems that IPv4 options generated.

MCMC MTSFB TC TXXX:2015

IPv6 RFC 2460 defines six (6) extension headers:

- a) hop-by-hop option header;
- b) routing header;
- c) fragment header;
- d) destination options header;
- e) authentication header (AH); and
- f) encapsulating security payload (ESP) header.

Each extension header is identified by the Next Header field in the preceding header.

4.3.5 Mandatory Internet Protocol Security (IPsec) Support

IPsec is a suite of protocols for securing Internet Protocol (IP) communications by authenticating the sender and providing integrity protection plus optionally confidentiality for the transmitted data. This is accomplished through the use of two (2) extension headers:

- a) the Encapsulating Security Payload (ESP); and
- b) the Authentication Header (AH).

The negotiation and management of IPsec security protections and the associated secret keys is handled by the Internet Key Exchange (IKE) protocol. IPsec is a mandatory part of an IPv6 implementation; however, its use is not required. IPsec is also specified for securing particular IPv6 protocols (e.g., Mobile IPv6 and Open Shortest Path First version 3 (OSPFv3)).

4.3.6 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, *Mobility Support in IPv6*.

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, defined in RFC 4861, *Neighbour Discovery for IPv6 version 6 (IPv6)*, 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, defined in RFC 4449, *Securing Mobile IPv6 Route Optimization Using a Static Shared Key*, where data flow between the home agent and mobile node will need to be appropriately secured.

4.3.7 Quality of Service (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. Transmission Control Protocol (TCP) 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 (2) fields can be used for QoS:

- a) Traffic Class; and
- b) Flow Label fields.

The new Flow Label field and enlarged Traffic Class field in the main IPv6 header allow more efficient and finer grained differentiation 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 and security should be given increased consideration in this stage of development.

4.3.8 Route Aggregation

IPv6 incorporates a hierarchical 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.

4.3.9 Efficient Transmission

IPv6 packet fragmentation control occurs at the IPv6 source host, not at an intermediate IPv6 router. With IPv4, a router can fragment a packet when the Maximum Transmission Unit (MTU) of the next link is smaller than the packet it has to send. The router does this by slicing a packet to fit into the smaller MTU and sends it out as a set of fragments. The destination host collects the fragments and reassembles them. All fragments must arrive for the higher level protocol to get the packet. Therefore, when one fragment is missing or an error occurs, the entire transmission has to be redone.

In IPv6, a host uses a procedure called Path Maximum Transmission Unit (PMTU) Discovery to learn the path MTU size and eliminate the need for routers to perform fragmentation. The IPv6 Fragment Extension Header is used when an IPv6 host wants to fragment a packet, so fragmentation occurs at the source host, not the router, which allows efficient transmission.

4.4 IPv4 and IPv6 Threat Comparison

The deployment of IPv6 can lead to new challenges with respect to the types of threats facing an organization. This section provides a high-level overview as to how threats differ from an IPv4 environment to an IPv6 environment and combined IPv4-IPv6 environment.

The following sections provide additional details to these threats as required. It should be noted that many IPv6 threat discussions rely on IPsec to provide protection against attack. Due to issues with key management and overall configuration complexity (including applications), it is possible that IPsec will not be deployed much more than it is with IPv4 today for initial IPv6 use.

Network reconnaissance is typically the first step taken by an attacker to identify assets for exploitation, defined in RFC 5157, *IPv6 Implications for Network Scanning*. Reconnaissance attacks in an IPv6 environment differ dramatically from current IPv4 environments. Due to the size of IPv6 subnets (2^{64} in a typical IPv6 environment compared to 2^8 in a typical IPv4 environment), traditional IPv4 scanning techniques that would normally take seconds could take years on a properly designed IPv6 network. This does not mean that reconnaissance attacks will go away in an IPv6 environment; it is more likely that the tactics used for network reconnaissance will be modified. Attackers will still be able to use passive techniques, such as Domain Name System (DNS) name server resolution; to identify victim networks for more targeted exploitation. Additionally, if an attacker is able to obtain access to one

MCMC MTSFB TC TXXX:2015

system on an IPv6 subnet, the attacker will be able to leverage IPv6 neighbour discovery to identify hosts on the local subnet for exploitation. Neighbour discovery-based attacks will also replace counterparts on IPv4 such as ARP spoofing.

Prevention of unauthorized access to IPv6 networks will likely be more difficult in the early years of IPv6 deployments. IPv6 adds more components to be filtered than IPv4, such as extension headers, multicast addressing, and increased use of ICMP. These extended capabilities of IPv6, as well as the possibility of an IPv6 host having a number of global IPv6 addresses, potentially provides an environment that will make network-level access easier for attackers due to improper deployment of IPv6 access controls. Moreover, security related tools and accepted best practices have been slow to accommodate IPv6. Either these items do not exist or have not been stress tested in an IPv6 environment. Nevertheless, global aggregation of IPv6 addresses by ISPs should allow enhanced anti-spoofing filtering across the internet where implemented.

Attacks that focus on exploitation above the IP layer, such as application-based attacks and viruses, will not see a difference in the types of threats faced in an IPv6 environment. Most likely, some worms will use modified IPv6 reconnaissance techniques for exploitation. Additionally, because many IPv4 broadcast capabilities have been replaced with IPv6 multicast functionality, broadcast amplification attacks will no longer exist in an IPv6 environment.

From this comparison of IPv4 and IPv6 threats, one can surmise that IPv6 will not inherently be either more or less secure than IPv4. While organizations are in the process of deploying IPv6, the lack of robust IPv6 security controls and a lack of overall understanding of IPv6 by security staff may allow attackers to exploit IPv6 assets or leverage IPv6 access to further exploit IPv4 assets. There is a very likely possibility that many IPv6 services will rely on tunneling IPv6 traffic in IPv4 for infrastructures that do support the protocol, which will also increase the complexity for security staff. Additionally, since IPv6 systems and capabilities are not yet widely used in production environments, there is a distinct possibility that the number of vulnerabilities in software from implementing IPv6 capabilities could rise, as IPv6 networks are increasingly deployed.

Based on of the threat comparison between IPv4 and IPv6, the following actions are recommended to mitigate IPv6 threats during the deployment process:

- a) Develop a granular ICMPv6 filtering policy for the enterprise. Ensure that ICMPv6 messages that are essential to IPv6 operation are allowed, but others are blocked;
- b) Use IPsec to authenticate and provide confidentiality to assets that can be tied to a scalable trust model (an example is access to Human Resources assets by internal employees that make use of an organization's Public Key Infrastructure (PKI) to establish trust);
- c) Identify capabilities and weaknesses of network protection devices in an IPv6 environment;
- d) Enable controls that might not have been used in IPv4 due to a lower threat level during initial deployment (implementing default deny access control policies, implementing routing protocol security, etc); and
- e) Pay close attention to the security aspects of transition mechanisms such as tunneling protocols.

4.5 Motivations for IPv6 Deployment

Early address allocation policies were relatively relaxed and large quantities of IPv4 addresses were assigned upon request, even when those allocations were not thoroughly justified. This resulted in a high concentration of IPv4 address allocations in the United States, with more than half of all routable IPv4 addresses assigned to U.S.-based organizations. Some large U.S.-based Internet backbone service providers have more IPv4 addresses than all of the nations that comprise the Asian region of the world.

These circumstances have left most of the world, especially Asia, with little choice other than to adopt the IPv6 specification if they are to become pervasive participants in IP technologies or the global

internet at large. Nations such as Japan have built IPv6-capable internet infrastructures to support their growing demand for internet connectivity. Further, the advanced state of wireless telecommunications in Asia produced an environment where globally unique IP addresses are required to enable the features of advanced wireless technologies. In essence, every mobile device becomes a mobile personal computing platform, and each of those devices requires true end-to-end connectivity to realize its full potential.

All organizations making use of IP networking should study and consider IPv6's feature set when designing and managing their networks. Even with no intent to replace IPv4, the IPv6 security controls discussed later in this Technical Code should be planned and deployed to detect unauthorized use of IPv6. Fundamental knowledge of IPv6:

- a) what it is;
- b) what its attributes are; and
- c) how it operates

are critical to any organization.

As the IPv6 protocol becomes increasingly ubiquitous, all enterprise and internet-connected networks need to be prepared for specific threats and vulnerabilities that the new protocol will bring. For example, an IPv4-only network segment may contain several newly installed hosts that are both IPv4 and IPv6-capable, as well as hosts that have IPv6 enabled by default. This circumstance can come about simply as a result of the normal systems life cycles. Additionally, IPv6 could be enabled on a host by an attacker to circumvent security controls that may not be IPv6-aware; these hosts can then be leveraged to create covert or backdoor channels. Taken further, IPv6 traffic could be encapsulated within IPv4 packets using readily available tools and services and exchanged with malicious hosts via the Internet.

Interoperability of geographically dispersed internet-connected nodes may become a profit motivation for some organizations to deploy IPv6. For instance, content providers are making more multimedia features available via a diverse set of customer platforms. Mobile phones, handheld personal computers, notebook computers, desktop personal computers, and home multimedia and gaming centres are all IPv4-capable today. Delivering multimedia content to those platforms is increasingly viable given the availability of broadband network bandwidths.

Nevertheless, IPv4 clearly cannot address all of these devices without using an address conservation technology like NAT and NAT by its nature denies true end-to-end IP connectivity. Multimedia service offerings and ultimately the market for those offerings are likely always to be constrained by IPv4, while IPv6 may prove to be an enabling technology.

If an organization is not constrained by IPv4 address availability or the disruption that NAT causes to true end-to-end connectivity between nodes, it should still plan for a world in which IPv6 will eventually be ubiquitous. All major vendors of IT products are shipping IPv6-capable products. Wholesale replacement of computing platforms and network infrastructure as a deployment requirement is less likely now than only five years ago, since many operating systems and networking products contain a native IPv6 protocol stack.

Also, tunneling IPv6 over the existing IPv4 internet is possible today by using free, readily available tunnel clients. An end user may download client software, obtain a routable IPv6 address and begin tunneling IPv6 over IPv4 networks with few technical or administrative barriers. Many open source IP networking tools are IPv6-capable, as are many consumer-oriented wireless access points. Many consumers of personal computing and home networking equipment are IPv6-capable, even if they do not use the features.

Because of the increasing availability and use of IPv6, as well as many years of coexistence between IPv6 and IPv4, management and technical experts within any organization should understand IPv6 technology - its background, basis, and capabilities, and how they can mitigate risks associated with

MCMC MTSFB TC TXXX:2015

running dual stack IPv4 and IPv6 networks. In the context of this Technical Code, dual stack means that nodes are running both IPv4 and IPv6 protocols concurrently.

5. IPv6 Addressing and Address Assignment

One of the main components for IPv6 deployment is the process of obtaining IPv6 addresses, planning and deploying the addresses. The following basic IPv6 definitions are important for any IPv6 discussion:

- a) Address: An IPv6-layer identifier for an interface or a set of interfaces;
- b) Node: Device on the network that sends and receives IPv6 packets;
- c) Deprecated address: An address, assigned to an interface, which is discouraged, but not forbidden (e.g., site-local addresses such as FEC0::/10). A deprecated address should no longer be used as a source address in new communications, but packets sent from or to deprecated addresses are delivered as expected;
- d) Router: A node that sends and receives packets, and also accepts packets and forwards them on behalf of other nodes;
- e) Host: A node that may send and receive packets but does not forward packets for other nodes;
- f) Link: A communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IPv6. Examples are Ethernets (simple or bridged); Point-to-Point Protocol (PPP); X.25, Frame Relay, or Asynchronous Transfer Mode (ATM) networks; and layer three (or higher) tunnels, such as tunnels over IPv4 or IPv6 itself;
- g) Link MTU: The maximum transmission unit (MTU), i.e., maximum packet size in octets, which can be conveyed over a link;
- h) Path MTU: The minimum link MTU of all the links in a path between a source node and a destination node;
- i) Upper Layer: A protocol layer immediately above IPv6. Examples are transport protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), control protocols such as Internet Message Control Protocol (ICMP), routing protocols such as Open Shortest Path First (OSPF) and internet or lower-layer protocols being tunnelled over (i.e. encapsulated in) IPv6 such as Internetwork Packet Exchange (IPX), AppleTalk or IPv6 itself;
- j) Interface: The point at which a node connects to a link. Unicast IPv6 addresses are always associated with interfaces;
- k) Packet: An IPv6 header plus payload; and
- l) Neighbours: Nodes attached to the same link.

5.1 IPv6 Addressing

The RFC 4291, *IPv6 Addressing Architecture*, describes IPv6 addresses are 128 bits long and are written in what is called colon-delimited hexadecimal notation. An IPv6 address is comprised of eight distinct numbers representing 16 bits each and written in base -16 (hexadecimal or hex) notation. The valid hex digits are 0 through 9 and A through F and together with the colon separator are the only characters that can be used for writing an IPv6 address.

An example of an IPv6 address is:

2001:0db8:9095:02e5:0216:cbff:feb2:7474¹

IPv6 addresses are divided among the network prefix, the subnet identifier and the host identifier portions of the address. The network prefix is the high-order bits of an IP address, used to identify a specific network and in some cases, a specific type of address.

¹ The address contains eight distinct four-place hex values, separated by colons. Each of these values represents 16 bits, for a total of 128 bits in the entire address.

The subnet identifier (ID) identifies a link within a site. The subnet ID is assigned by the local administrator of the site; a single site can have multiple subnet IDs. This is used as a designator for the network upon which the host bearing the address is resident.

The host identifier (host ID) of the address is a unique identifier for the node within the network upon which it resides. It is identified with a specific interface of the host. Figure 2 depicts the IPv6 address format with the network prefix, subnet identifier and host identifier.

RFC 4291 also describes the notation for prefixes. The network prefix is analogous, but not equivalent to the subnet mask in IPv4.

IPv4 addresses are written in Classless Inter-domain Routing (CIDR) notation with a subnet mask that contains "1"s in the bit positions that identify the network ID. There is no subnet mask in IPv6, although the slash notation used to identify the network address bits is similar to IPv4's subnet mask notation. The IPv6 notation appends the prefix length and is written as a number of bits with a slash, which leads to the following format:

IPv6 address/prefix length

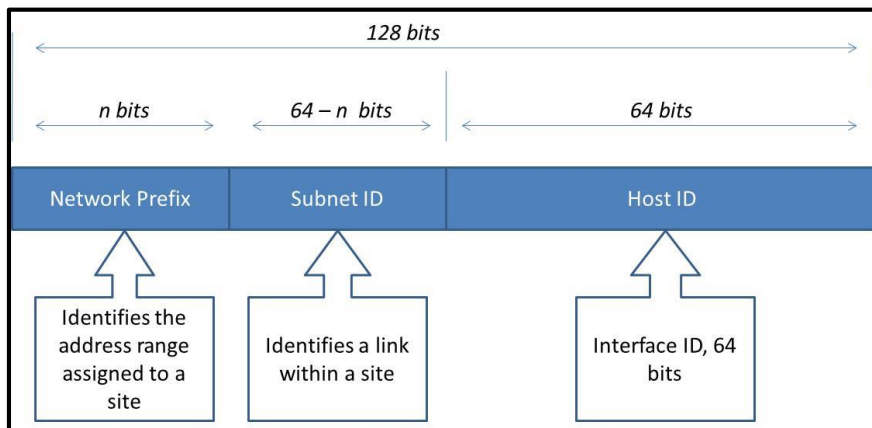


Figure 2. IPv6 Address Format

The prefix length specifies how many of the address's left-most bits comprise the network prefix. An example address with a 32-bit network prefix is:

2001:0db8:9095:02e5:0216:cbff:feb2:7474/32

Quantities of IPv6 addresses are assigned by the international registry services and Internet service providers (ISP) based upon the size of the entity receiving the addresses. Large, top-tier networks may receive address allocations with a network prefix of 32 bits as long as the need is justified. In this case, the first two groupings of hex values, separated by colons, comprise the network prefix for the assignee of the addresses. The remaining 96 bits are available to the local administrator primarily for reallocation of the subnet ID and the host ID.

The subnet ID identifies a link within a site, which can have multiple subnet IDs. The host ID within a network must be unique and identifies an interface on a subnet for the organization, similar to an assigned IPv4 address. Figure 3 depicts an IPv6 address with 32 bits allocated to the network prefix.

MCMC MTSFB TC TXXX:2015

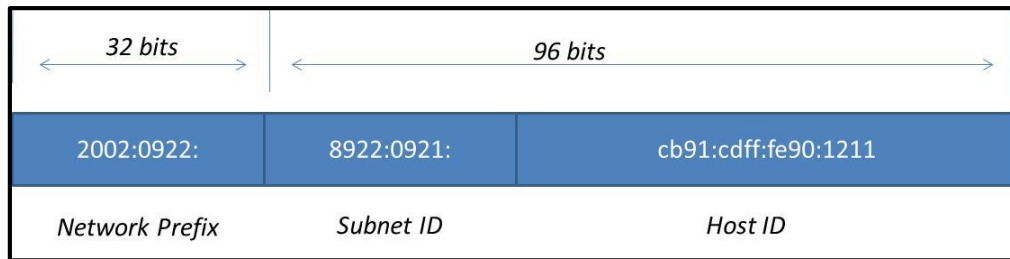


Figure 3. 32-Bit Network Prefix

Government, educational, commercial and other networks typically receive address allocations from top-tier providers (ISPs) with a network prefix of 48 bits (/48), leaving 80 bits for the subnet identifier and host identifier.

Subnets within an organization often have network prefixes of 64 bits (/64), leaving 64 bits for allocation to hosts' interfaces. The host ID should use a 64-bit interface identifier that follows EUI-64 (Extended Unique Identifier) format when a global network prefix is used (001 to 111), except in the case when multicast addresses (1111 1111) are used 10. Figure 4 depicts an IPv6 address with 64 bits allocated to the network prefix.

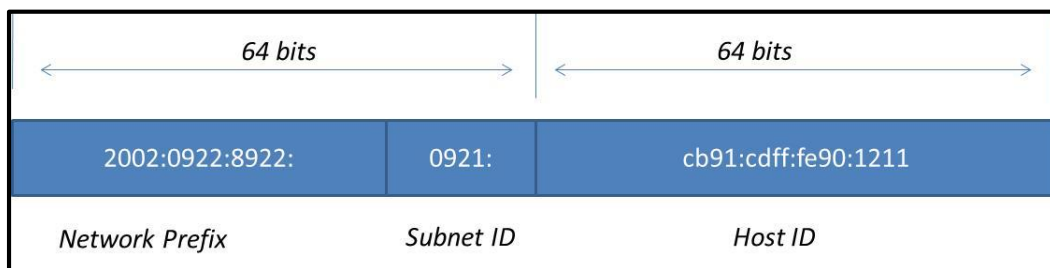


Figure 4. 64-Bit Network Prefix

5.1.1 Simplifying IPv6 Addresses

Due to their length, IPv6 addresses are difficult to remember. Administrators of IPv4 networks typically can recall multiple IPv4 network and host addresses; remembering multiple IPv6 network and host addresses is more challenging. The notation for IPv6 addresses may be compressed and simplified under specific circumstances.

One to three zeroes that appear as the leading digits in any colon-delimited hexadecimal grouping may be dropped. This simplifies the address and makes it easier to read and to write. For example:

2001:0db8:0aba:02e5:0000:0ee9:0000:0444/48 becomes
2001:db8:aba:2e5:0:ee9:0:444/48

It is important to note that trailing zeroes may not be dropped because they have intrinsic place value in the address format.

Further efficiency is gained by combining all-zero portions of the address. Any colon-delimited portion of an address containing all zeros may be compressed so that nothing appears between the leading and trailing colons. For example:

2001:0db8:0055:0000:cd23:0000:0000:0205/48 becomes
2001:db8:55:0:cd23::205/48

In this example, the sixth and seventh 16-bit groupings contain all zeroes; they were compressed by eliminating the zeroes completely, as well as the colon that divided the two groupings. Nevertheless, compressing an address by removing one or more consecutive colons between groups of zeroes may only be done once per address. The fourth 16 bit-grouping in the example also contains all zeroes, but in the condensed form of the address, it is represented with a single zero. A choice had to be made as to which group of zeroes was to be compressed. The example address could be written:

2001:db8:55::cd23:0:0:205/48, but this is not as efficient as **2001:db8:55:0:cd23::205/48**

It is important to note that both of the addresses in the preceding paragraph are properly formatted, but the latter address is shorter. Compression is just a convention for writing addresses, it does not affect how an address is used, and it makes no difference whether compression falls within the network prefix, host identifier, or across both portions of the address.

5.1.2 IPv6 Address Types

IPv6 uses the notion of address types for different situations. These different address types are defined below:

- a) **Unicast Addresses**
Addresses that identify one interface on a single node; a packet with a unicast destination address is delivered to that interface.
- b) **Multicast Addresses**
RFC 4291 defines a multicast address as, “An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.” Although multicast addresses are common in both IPv4 and IPv6, in IPv6 multicasting has new applications. The single most important aspect of multicast addressing under IPv6 is that it enables fundamental IPv6 functionality, including neighbour discovery (ND) and router discovery. Multicast addresses begin with FF00::/8. They are intended for efficient one-to-many and many-to-many communication. The IPv6 standards prohibit sending packets from a multicast address; multicast addresses are valid only as destinations.
- c) **Anycast Addresses**
Addresses that can identify several interfaces on one or more nodes; a packet with an anycast destination address is delivered to one of the interfaces bearing the address, usually the closest one as determined by routing protocols. Anycast addressing was introduced as an add-on for IPv4, but it was designed as a basic component of IPv6.

The subnet prefix in an anycast address is the prefix that identifies a specific link. Anycast addresses are intended for efficiently providing services that any one of a number of nodes can perform (e.g. a Home Agent for a Mobile IP node). Anycast addresses may not be used as source addresses and, as of the writing of this guide, may only be assigned to routers. It should be noted that there are no defined mechanisms for security or registration for anycast, nor is there a way to verify that a response to a packet sent to an anycast address was sent by an interface authorized to do so. This leaves open the possibility of impersonating anycast servers.

- d) **Broadcast Addresses**
Broadcast addressing is a common attribute of IPv4, but is not defined or implemented in IPv6. Multicast addressing in IPv6 meets the requirements that broadcast addressing formerly fulfilled.

5.1.3 IPv6 Address Scope

The shortage of IPv4 addresses led to the designation of non-routable addresses in RFC 1918 and the widespread use of Network Address Translation (NAT) to share globally routable addresses (with certain limits placed on the hosts using so-called RFC 1918 addresses). IPv6 has no such shortage, so

MCMC MTSFB TC TXXX:2015

the use of NAT is unnecessary; nevertheless, the usefulness of addresses with limited scope was identified and maintained in IPv6. IPv6 addresses with different scopes were defined.

In the original design for IPv6, link local, site local and global addresses were defined; later, it was realized that site local addresses were not well enough defined to be useful. Site local addresses were abandoned and replaced with unique local addresses. Older implementations of IPv6 may still use site local addresses, so IPv6 firewalls need to recognize and handle site local addresses correctly.

The IPv6 standards define several scopes for meaningful IPv6 addresses:

- a) Interface-local
This applies only to a single interface; the loopback address has this scope.
- b) Link-local
This applies to a particular Local Area Network (LAN) or network link; every IPv6 interface on a LAN must have an address with this scope. Link-local addresses start with FE80::/10. Packets with link-local destination addresses are not routable and must not be forwarded off the local link. Link-local addresses are used for administrative purposes such as neighbor and router discovery. Table 1 shows the details of link local address.

Table 1. Link-local address

10 bits	54 bits	64 bits
1111 1110 10	0000 0000	Interface ID
FE80/10	0000 0000	Interface ID

- c) Site-local
This scope was intended to apply to all IPv6 networks or a single logical entity such as the network within an organization. Addresses with this scope start with FEC0::/10. They were intended not to be globally routable but potentially routed between subnets within an organization. Site local addresses have been deprecated and replaced with unique local addresses.
- d) Unique local unicast
This scope is meant for a site, campus or enterprise's internal addressing. It replaces the deprecated site-local concept. Unique local addresses (ULAs) may be routable within an enterprise. Use of unique local addresses is not yet widespread; see RFC 4193, *Unique Local IPv6 Unicast Addresses*, for more information.
- e) Global
The global scope applies to the entire internet. These are globally unique addresses that are routable across all publicly connected networks.
- f) Embedded IPv4 Unicast
The IPv6 specification has the ability to leverage existing IPv4 addressing schemes. The transition to IPv6 will be gradual, so two special types of addresses have been defined for backward compatibility with IPv4: IPv4-compatible IPv6 addresses (rarely used and deprecated in RFC 4291) and IPv4-mapped IPv6 addresses. Both allow the protocol to derive addresses by embedding IPv4 addresses in the body of an IPv6 address. An IPv4-mapped IPv6 address is used to represent the addresses of IPv4-only nodes as an IPv6 address, which allows an IPv6 node to use this address to send a packet to an IPv4-only node.

Table 2. IPv4-compatible IPv6 Address

80 bits	16 bits	32 bits
0000 0000	0000	IPv4 Address

Table 3. IPv4-mapped IPv6 Address

80 bits	16 bits	32 bits
0000 0000	FFFF	IPv4 Address

The two IPv4 embedded address types are similar. The only difference is the sixth group of 16 bits. IPv4-compatible addresses set these to 0; IPv4-mapped addresses set these to 1.

A more generalized form of IPv4-embedded IPv6 addresses has been defined in RFC 6052, *IPv6 Addressing of IPv4/IPv6 Translators* to aid the process of automated translation from one type of address to the other. Two (2) new variants of IPv4-embedded IPv6 addresses are:

- i. IPv4-converted IPv6 addresses: IPv6 addresses used to represent IPv4 nodes in an IPv6 network
- ii. IPv4-translatable IPv6 addresses: IPv6 addresses assigned to IPv6 nodes for use with stateless transition

It is quite likely that additional special-use variants will be defined in the future.

g) Other address or Special Address types.

IPv6 makes use of addresses other than those shown above. The unspecified address consists of all zeros (0:0:0:0:0:0:0 or simply ::) and may be the source address of a node soliciting its own IP address from an address assignment authority (such as a DHCPv6 [DHCP for IPv6] server). IPv6-compliant routers never forward a packet with an unspecified address. The loopback address is used by a node to send a packet to itself. The loopback address, 0:0:0:0:0:0:0:1 (or simply: 1), is defined as being interface-local. IPv6-compliant hosts and routers never forward packets with a loopback destination.

An essential design consideration for IPv6 is to simplify routing in enterprise and global networks. One of the intents of the IPv6 address schema is to facilitate hierarchical routing. Hierarchical routing in turn accelerates the end-to-end routing function and routing table convergence and maintenance are vastly simplified.

A typical IPv6 interface is configured to receive packets sent to several addresses. In addition to its link local and global unicast addresses, it may have a unique local address. It can also receive multicast messages sent to the all hosts and solicited node multicast addresses, as well as possibly to other multicast addresses. Finally, because of renumbering, multiple instances of some of these addresses may be active at once.

5.2 IPv6 Address Allocation

IPv6 addresses have a flexible structure for address assignments. This enables registries, ISPs, network designers and others to assign address ranges to organizations and networks based on different criteria, such as size of networks and estimated growth rate. Often, an initial assignment does not scale well if a small network becomes larger than expected and hence needs more addresses. The assignment authority may not be able to allocate contiguous addresses if they were already assigned to another network.

5.2.1 IPv6 Address Assignment

IPv6 network prefix assignment is the first step in network deployment. The Best Common Practice is described in RFC 4291, *Internet Protocol Version 6 (IPv6) Addressing Architecture*, which is leftmost addressing scheme.

However, there are other methods such rightmost and centermost helps provide for flexibility and efficient aggregation of an assigned IPv6 block, as described in RFC 3531, *A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block*. If done without foresight, boundaries between sub-allocations become difficult to move and future increases in the use of address space cannot be kept contiguous.

MCMC MTSFB TC TXXX:2015

The easiest but least flexible solution is to make block address assignment in order from the beginning of the organization's allocated IPv6 block. For example, if an organization is assigned the prefix **2001:0db8:9095::/48**, prefixes can be distributed in simple sequential order:

2001:0db8:9095:0001::/64
2001:0db8:9095:0002::/64
2001:0db8:9095:0003::/64

This is the simplest way to distribute address assignments, but it lacks consideration for future needs and does not take into account grouping networks by site for clean routing aggregation. Additionally, this method makes it impossible to make an existing network assignment larger and keep its address space contiguous.

RFC 3531 proposes a method to manage the assignment of bits of an IPv6 address block or range. First, the scheme defines parts of the IP address as p1, p2, p3, ...pN in order, so that an IP address is composed of these parts contiguously. Boundaries between each part are based on the prefix assigned by the next level authority. Part (p1) is the leftmost part probably assigned to a registry, Part (p2) can be allocated to a large ISP or national registry. Part (p3) can be allocated to a large customer or a smaller provider, etc. Each part can be of different length.

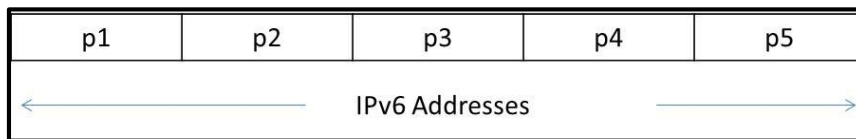


Figure 5. IPv6 Address Assignment Scheme

The algorithm for allocating addresses is as follows:

- a) (p1) for the left-most part, assign addresses using the leftmost bits first;
- b) (pN) for the rightmost part, assign addresses using the rightmost bits first; and
- c) for all other parts (center parts), predefine an arbitrary boundary (prefix) and then assign addresses using center bits of the part being assigned first.

This algorithm increases the assigned bits in such way that it keeps unassigned bits near the boundaries between the parts. This means that the boundary between any two parts can be changed forward or backward, later on, up to the assigned bits.

A brief example based on RFC 3531 uses a provider called Provider 1. This provider has been assigned the **3ffe:0b00/24** prefix and wants to assign prefixes to its connected networks. It expects in the foreseeable future a maximum of 256 customers consuming 8 bits. One of these customers, named C2, expects a maximum of 1024 customers' assignments under it; consuming 10 other bits (see RFC 3531 for greater detail). The assignment will be as follows, not showing the first 24 leftmost bits (**3ffe:0b00/24** or 0011 1111 1111 1110 0000 1011):

Provider 1 assigns address space to its customers using leftmost bits:

1000 0000: assigned to customer 1 (C1)
0100 0000: assigned to customer 2 (C2)
1100 0000: assigned to customer 3 (C3)
0010 0000: assigned to customer 4 (C4)

C2 assigns address space to its customers (C2C1, C2C2, ...) using centermost bits:


0000 10000: assigned to C2C1

MCMC MTSFB TC TXXX:2015

0001 00000: assigned to C2C2
 0001 10000: assigned to C2C3

Customer of C2 uses centermost bits for maximum flexibility and then the last aggregators (which should be networks within a site) will be assigned using rightmost bits.

Putting all bits together for C2C3:

	P1	C2	C2C3
Hex	3ffe:0b00	40	0C
Binary	0011 1111 1111 1110 0000 1011	0100 0000	0000 1100 00
 <p>← → ← → Growing bits</p>			

By using this method, Provider 1 will be able to expand the number of customers and the customers will be able to modify their first assumptions about the size of their own customers, until the reserved bits are assigned.

Predicting future network requirements will always be a challenge with ever changing business needs and unforeseen technological advances. Nonetheless, a strategy to account for organizational needs, possible growth areas and consideration to address assignment will provide as much downstream flexibility as possible.

5.2.2 Obtaining Global IPv6 Addresses

The Internet Corporation for Assigned Names and Numbers (ICANN) and Internet Assigned Numbers Authority (IANA) have delegated most IPv6 address allocation to the five (5) Regional Internet Registries (RIR):

- a) African Network Information Centre (AfriNIC) is the RIR for Africa and the Indian Ocean, <http://www.afrinic.net/>
- b) Asia Pacific Network Information Centre (APNIC) is RIR for Asia Pacific Region - Australia, Oceania and most of Asia, <http://www.apnic.net/> or <http://www.apnic.net/policy/ipv6-address-policy>
- c) Réseaux IP Européens Network Coordination Centre (RIPE NCC) is the RIR for Europe, the Middle East and parts of Central Asia, <http://www.ripe.net/> or <http://www.ripe.net/rs/index.html>
- d) Latin America and Caribbean Network Information Centre (LACNIC) is the RIR for the Latin American and Caribbean regions, <http://www.lacnic.net/> or <http://lacnic.net/en/bt-IPv6.html>
- e) American Registry for Internet Numbers (ARIN) is the RIR for Canada, the United States and many Caribbean and North Atlantic islands, <http://www.arin.net/> or https://www.arin.net/resources/request/ipv6_initial_assign.html

ISPs find information about their regional registries at these websites. Organizations and end users get their address allocations from their ISPs. Normally a RIR allocates a /32 ('slash 32') address to qualified ISPs, which are called Local Internet Registries (LIR) and the ISP allocates /48 ('slash 48') addresses to its customers.

Section III Sub-Section 10 of Numbering and Electronic Addressing Plan (NEAP) Amendment Notice No. 1 of 2015 set out rules of electronic addressing in Malaysia.

MCMC MTSFB TC TXXX:2015

5.2.2.1 Obtaining IP addresses and Autonomous System (AS) number from APNIC

An organization should first become a member of APNIC and then complete the appropriate request form to obtain IP addresses.

5.2.2.1.1 Criteria for initial LIR delegation

Organizations seeking their first IPv4 allocation must meet the minimum criteria. Organizations must:

- a) Have used a /24 ('slash 24') from their upstream provider or can demonstrate an immediate need for a /24;
- b) Have complied with applicable policies in managing all address space previously allocated to it; and
- c) Be able to demonstrate a detailed plan to use a /23 within a year.

5.2.2.1.2 Criteria for small multihoming delegations

- a) An organization is eligible if it is currently multihomed with provider-based addresses, or demonstrates a plan to multihome within one month and agrees to renumber out of previously assigned address space.
- b) Organizations requesting a delegation under these terms must demonstrate that they are able to use 25% of the requested addresses immediately and 50% within one year.

5.2.2.1.3 Criteria for Internet Exchange Points

- a) Internet Exchange Points (IXP) are eligible to receive a delegation from APNIC to be used exclusively to connect the IXP participant devices to the Exchange Point.
- b) Global routability of the delegation is left to the discretion of the IXP and its participants.

5.2.2.1.4 Criteria for critical infrastructure

The following critical infrastructure networks, if operating in the Asia Pacific region, are eligible to receive a portable assignment:

- a) Domain registry infrastructure
 - i. Root domain name system (DNS) server
 - ii. Global top level domain (gTLD) DNS
 - iii. Country code TLD (ccTLD) DNS server
- b) Address registry infrastructure
 - i. Internet Assigned Numbers Authority (IANA)
 - ii. Regional Internet Registry (RIRs)
 - iii. National Internet Registry (NIRs)

From one point of view, the case for Provider Independent (PI) assignments can allow for a small number of large organizations to avoid a significant expense due to address renumbering. In addition, organizations may not want to be locked in to a specific Internet provider. On the other hand, the main concerns regarding PI assignment include two (2) major issues:

- a) The possibility of a large increase in the size of the IPv6 default-free routing table; these tables generally point only to top-level domains of aggregated routes. PI assignments do not fit into the normal aggregation and will increase the size of these tables; and
- b) The fear is that early adopters, similarly to IPv4, would have an unfair advantage vis à vis those who adopted later.

IPv6 address allocation is designed to allow routing prefix aggregation. IPv6 network addresses may be aggregated in the same sense that IPv4 CIDR addresses are. IPv6 address allocation is based on the hierarchy mentioned previously and allocated blocks of addresses are widely dispersed with top-tier allocations having network prefixes of 32 bits. This leaves 96 bits' worth of addresses that can all be aggregated through a single route advertisement on the internet backbone.

Consider routing prefix aggregation for a large backbone service provider. The service provider, hypothetically, receives a block of address space with a 32-bit network prefix. In turn, the provider allocates this address space to customers. Those customers could be multiple regional network service providers or large enterprises that receive blocks of addresses with 48-bit network prefixes from that single large backbone service provider. Subnets within those enterprises and smaller regional service providers may have address space with 64-bit network prefixes.

This arrangement may easily result in tens of millions of nodes attached to millions of subnets, all of which are aggregated and reachable via the global Internet through one route on the Internet's backbone routers.

IPv6 address allocation is a work in progress. Organizations should familiarize themselves with assignment and reporting requirements that differ from those for IPv4. RFC 3177, *IAB/IESG Recommendations on IPv6 Address Allocations to Sites*, documents an ongoing effort to provide the latest information for the internet community regarding current practices, status, and clarifications for IPv6 address allocations.

Information on obtaining IP addresses is available at the APNIC website.

6. Challenges of Technology, Resources and Organization

IPv6 deployment is an enterprise-wide problem, covering not just networks and servers, but also desktops, applications, security and other endpoints as shown in Figure 6. The basic network infrastructure is the first priority, including IP addressing and routing protocols. Network services are next. Most of these functions are available in IPv6 implementations today.

The challenge is mostly on configuration and testing. However, some network services, especially security, rely heavily on IPv4 packet header information and require modifications to provide the same level of service in IPv6.

Desktops, laptops, and servers can use a dual-stack approach, supporting simultaneous connectivity with both IP versions. Traditional devices, such as printers, may be accessible only through IPv4, whereas newer devices, such as small sensors and controllers, may use only IPv6. The dual-stack approach integrates both types of devices into the network.

Most of the technology challenges are a matter of resources. It takes time to learn the configuration and operation details for the additional protocol. The Operations Support staff will require additional training. The team needs to upgrade or replace some network devices because of product gaps and other protocol support concerns. Commercial IPv6 offerings may not be available everywhere, requiring temporary tunneling. Remote office deployment can be very time-consuming. And, like any project, detailed budgets and headcount numbers are required for approval.

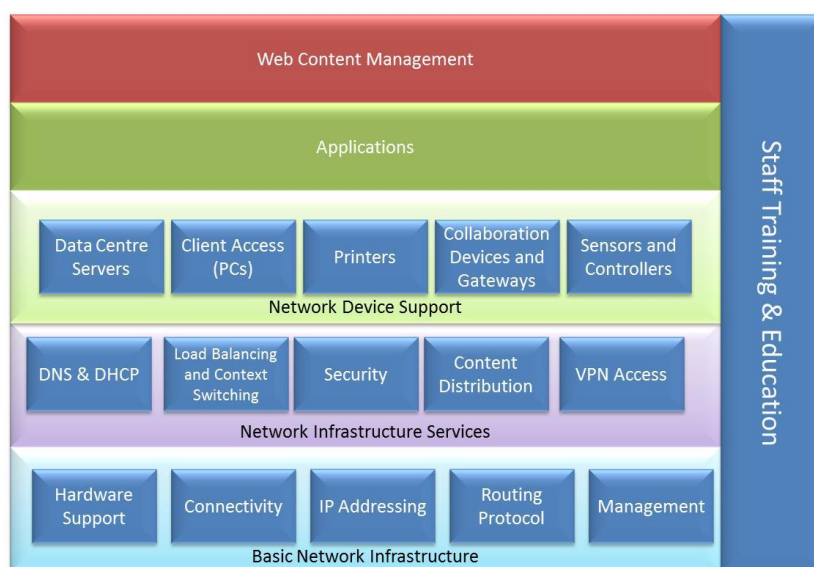


Figure 6. Enterprise IPv6 Adoption

6.1 Technology

6.1.1 Tools

Some tools can help to ensure the smooth operation and management of a network. Monitoring tools to be used can be determined after auditing and validating the network. Some of the tools such as Network Management System (NMS) and IP Address Management (IPAM) are important to manage IPv6 network. These two tools are explained briefly in the following sections.

6.1.1.1 Network Management System (NMS)

NMS provides information of network inside an organization. The system also helps organizations to monitor, control, analyse and manage the network. The standard practice of NMS uses SNMP protocol to manage the element and services. NMS assessment needs to be done prior to IPv6 deployment to support IPv6. Areas to be considered:

- a) IPv6 Applications;
- b) Network Protocol (SNMP, TFTP, NTP, Syslog, Telnet, SSH, etc.) over IPv6; and
- c) DNS/DHCP server, Network Collector.

In a dual- stack network, both IPv4 and IPv6 environment must be managed with the best optimization to decrease the cost of operation.

6.1.1.2 IP Address Management (IPAM)

Developing an IPv6 addressing plan can seem like nothing more than a massive complication. It's challenging for system administrator to manage large number of IPv6 addresses manually. It's also impossible to track, manage and plan using manual method without proper system tools.

IPAM is a solution to assist in managing list of active IP addresses in a network. IPAM can also dissect the packets transmitted and categorize into media access control address, DNS name, DNS aliases, MX records, Dynamic vs Static IP addresses. An obvious extension to IPAM is the ability to push IP address information out to the DNS and DHCP server to make information usable across the network. Other IPv6 related tools are available on 6Now website.

6.1.2 Devices and Application availability

Often an individual or company will choose a device based on its need to run a particular application. Application availability is an important factor when choosing devices. Security is another major concern. Some organizations prohibit the use of devices that don't support encrypted storage.

The best approach for deciding which devices your organization will use involves establishing a set of requirements to which the devices must adhere and then seeking out devices that meet those criteria.

For enterprise, it is recommended to minimize the number of different types of devices that are being used in the organization. The greater the variety of devices that are in use, the higher your operational costs will be.

6.1.3 Standard

There are many devices in the market that are not IPv6 compliant. Some of these devices are IPv6 capable but with functionalities disabled. These devices are unable to execute IPv6 services even though it is stated as IPv6 capable. So, it is important that devices are certified to be IPv6 compliant according to *MCMC MTSFB TC TXXX:2015 – Specification for Internet Protocol version 6 (IPv6) Compliant Products*.

6.2 Resources

One of the critical components in implementing IPv6 is resource. Existing personnel must have adequate knowledge to support IPv6 deployment. For this, organisations have to properly plan their resources for IPv6 to avoid any disaster that can disrupt the daily operation.

6.2.1 Training & Expertise

Training is a critical part of deploying IPv6. An intensive IPv6 training shall be required to ensure users and technical working group understand the requirement and implementation before migration to IPv6 networks.

Appropriate trainings have to be provided to individuals who will be supporting IPv6 deployment and management. More information is given in the technology education section.

6.2.2 Project Management

It is essential that preparations start with determining the interactions among various groups' involvement within the operations, engineering and management layers. This includes defining workflows, planning, design and shared responsibility and timeline of IPv6 deployment.

6.2.3 Timeline

To complete the IPv6 transition process, industry players must work together to support the new protocol on an accelerated timeline. The IETF, equipment vendors, application developers, network operators and end users have roles to play in ensuring the successful widespread deployment of IPv6.

As ISP particularly play a key role in the global adoption of IPv6, they have to ensure that on existing core and edge network devices, infrastructure service such as the domain name system, firewalls, security and management systems are ready to make IPv6 connectivity available to user.

Other organizations like web companies need to offer their sites and applications over IPv6, operating system vendors may need to implement specific software updates, and hardware and home gateway manufacturers may need to update firmware. This will encourage the timely deployment of IPv6.

MCMC MTSFB TC TXXX:2015

6.2.4 Device Refreshment

It is normal that existing devices have to be refreshed from time to time depending on the availability of updates and also other factors. New programs have to be created for companies to upgrade or replace existing devices so that they can provide IPv6 services without delay. Some of the programs to consider are:

- a) Program to subsidize to replace/upgrade all non-IPv6 ready devices; and
- b) Promotion of upgrading existing system.

Besides that, proper plans have to be in place so that the non-IPv6 ready devices, such as printers, cameras and others will be replaced. This will avoid any disruption of services in the future.

6.3 Organization

It is important for organizations to support IPv6 sooner than later so that they are not left behind in this technology. However, many organizations have been lackadaisical in this matter. This is due to the cost involved and the lack of business case. Therefore it may require beyond the organization's initiative to push for realization.

To avoid the late acceptance and deployment of IPv6 compared with other countries, Malaysia has taken proactive measures by issuing a mandate to ensure that the whole industry is aligned in making more significance in their deliverables. With this mandate, ISPs are required to provide IPv6 services by the deadline.

6.3.1 Guideline

The organizations should establish guidelines and policies for IPv6 deployment that consist of planning, design, and implementation and migration plan for IPv6 deployment.

6.3.2 Justifying benefit

This section discusses the costs and benefits of adopting IPv6. Here are the specific reasons and benefits of implementing IPv6:

- a) Prevent cost increase: Companies will need to spend more to cope with scarcity of IPv4 addresses, whether it's in a workaround buying the networking gear or trying to buy more IPv4 addresses. The fact is, it is more expensive if an organization doesn't plan for it.
- b) Prevent service disruption: Business that do not commit to IPv6 transition and do not start to take the proper steps to initiate this process now, will risk accessibility problems of their websites and other internet-connected locations and services.
- c) Growth of global business depends on it: IPv4 addresses are fast depleting and many organizations have to use IPv6 addresses to continuously support their services. To ensure that ISPs provide IPv6 services to customers, Government has mandated ISPs to provide IPv6 services by Q1 2015.
- d) Avoid diminishing experience for customers and access to supply chain: If the IPv6 transition happens as expected, most users would not notice any change in their Internet use. But those who are still operating IPv4 may notice service disruptions.
- e) Ready to deploy today: Deployment of IPv6 started since 20 years ago. Initial work on the next generation of Internet protocol began in 1992 and more than thousand websites around the world including Google, Facebook and Yahoo have enabled IPv6. Most of companies, website, ISP and vendors have committed to make IPv6 permanent or by "default" for their products and services.

- f) Your competitors are doing it: Major Internet Service Provider, home networking equipment manufacturer and Web companies around the world are coming together to enable IPv6 for their product and services, which will result in significant increase in Internet traffic using IPv6.

6.3.3 Cost

One of the major challenges is the cost of IPv6 deployment. It is not directly related to organizational size but depend on existing organizational network infrastructure including servers, core/access routers, firewalls, billing systems, and standard and customised software programs on the type of organization. Planning the deployment enables each organization to determine costs and select a deployment scenario that enables IPv6 services at the lowest cost possible. Below are the ten (10) essential planning steps.

- Step 1: Identifying how IPv6 affects operations
- Step 2: Establishing goals, a critical path and timelines
- Step 3: Inventorying IT equipment and build a deployment plan
- Step 4: Identifying software and services and develop an upgrade plan
- Step 5: Creating an IPv6 training strategy and plan
- Step 6: Developing an addressing plan and corresponding network architecture
- Step 7: Obtaining an IPv6 prefix
- Step 8: Developing an IPv6 threats and countermeasures security policy
- Step 9: Developing an IPv6 procurement strategy and policy
- Step 10: Drafting an exception strategy (systems that don't need to be modified)

7. IPv6 Deployment Strategy

7.1 Transition Mechanism

IPv6 is not backward compatible with IPv4. IPv4 systems cannot use IPv6 services or communicate with IPv6 hosts. The transition from IPv4 to IPv6 is expected to take a significant amount of time. As long as systems require interoperability between IPv4 and IPv6, transition mechanisms are needed.

In the transition environment, three (3) different types of hosts exist:

- a) IPv4 only;
- b) IPv6 only; and
- c) Dual stack IPv4/IPv6.

While dual stack is the recommended approach, there may be circumstances that require an organization to operate and communicate with single-stack systems.

Transition mechanisms support interoperability between IPv4 and IPv6 hosts. Multiple transition mechanisms may be deployed with any IPv6 transition. Transition mechanism chosen depends on the client capabilities, the particular transition strategy chosen, time frame and the transition stages. Transition mechanisms fall into three (3) categories:

- a) Dual stack;
- b) Tunneling; and
- c) Translation.

MCMC MTSFB TC TXXX:2015

A typical transition will transform an organization's network from an all IPv4 environment to one where there are isolated IPv6 hosts or small islands of IPv6 hosts. The term island often appears in RFCs and refers to a small collection of like protocol hosts (either IPv4 or IPv6).

These examples demonstrate how an organization could use the different transition mechanisms during this process:

- a) Early in a transition, IPv4 tunnels will connect to IPv6 islands. Translation and dual stack mechanisms will allow IPv6 hosts to use IPv4 resources. Wherever possible, the use of translation mechanisms should be avoided because of the complexities and incompatibilities associated with the translation of multiple protocols.
- b) As the transition progresses from IPv4 dominant to IPv6 dominant, the organization will configure the network core to either IPv6 or a dual stack. This will allow the organization to dispense with some of the tunnel mechanisms installed in the earlier stage of IPv6 transition. Translation mechanisms will be required to allow IPv4 hosts to use new IPv6 services.
- c) In the last phase of the migration, most equipment and services will support IPv6. Only isolated islands of IPv4 legacy services will remain. IPv4 traffic will tunnel over IPv6 and translation services will allow IPv6 clients to access legacy services.

7.2 IPv4/IPv6 Dual Stack Environment

In the dual stack method of IPv4 to IPv6 transition, each host is both IPv4 and IPv6 aware. Dual stack hosts run both IPv4 and IPv6 protocols and allocate addresses for both protocols. RFC 4213, *Basic IPv6 Transition Mechanisms*, further explains the dual stack method. Dual stack is ideal in an environment where the organization has an existing IPv4 network, albeit an extensive one and would like to introduce IPv6 in a rapid deployment.

The purpose of a dual stack method is to minimize the number of tunnels used in a transition. Organizations use dual stack when the majority of an organization's equipment is dual stack capable and they want a rapid deployment.

7.2.1 Deployment of Dual Stack Environment

When considering a deployment of a dual stack environment, one must consider the following issues:

- a) Shared infrastructure;
- b) Need for more resources;
- c) Application protocol preference; and
- d) Sustaining IPv4 address usage.

The IPv4 and IPv6 infrastructures are different. Dual stack devices require routing and switching infrastructures that are protocol aware. RFC 4554, *Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks*, describes how 802.1q tags can be used to divide a network logically into IPv4 routing and IPv6 routing domains.

Dual stack environments use more resources than a single protocol environment. The following are examples of how a dual stack environment uses more resources:

- a) Routers need to:
 - i. Maintain forwarding tables for both IPv4 and IPv6;
 - ii. Run routing protocols for both protocols;
 - iii. Implement packet filtering for both protocols;

- iv. Provide for congestion control for both protocols;
 - v. Handle special cases (IPv4 Router Alerts and IPv6 Hop-by-Hop Options) for both; and
 - vi. Forward packets for both protocols.
- b) Hosts must devote resources to both protocol stacks (for example, processing, memory, and network infrastructure traffic).
 - c) Administrative and security staff must maintain concurrent environments as well.
 - d) As long dual-stack environment exist, network administrator have to sustain IPv4 address assignment.

Within a dual stack environment, some applications are IPv4 only, some are IPv6 only and some applications may be IPv4/IPv6. The host must use the correct protocol to access each. The administrator using DNS record order or translation mechanisms can influence protocol selection.

Applications are written to query only A, only AAAA, or both A and AAAA records for name resolution. The administrator can influence the service called by ordering the records returned by DNS, giving precedence to the preferred service. Except for IP addressing, DNS is the same protocol for both IPv4 and IPv6.

For example, to allow an IPv4 host to locate a service, create a DNS A record and to allow an IPv6 host to locate a service, create a DNS AAAA record. Order the DNS records so that dual stack hosts are resolved to the preferred service. When configuring DNS in a transition environment, administrators should set the preference for IPv6.

7.2.2 Addressing in Dual Stack Environment

Each protocol stack is responsible for configuring its own addresses. The administrator can configure static addresses or configure the host to receive dynamic addressing. If DHCP is used, then each protocol stack must access a DHCP server for address allocation. DHCP has different protocols for IPv4 and IPv6. Each protocol must access its own DHCP server.

7.2.3 Security Implication of a Dual Stack Environment

A dual stack strategy is useful in making a transition between protocols, but the approach exposes every dual stack node to the vulnerabilities of both protocols, plus any new vulnerabilities resulting from unintended interactions between them.

RFC 4852, *IPv6 Enterprise Network Analysis - IP Layer 3 Focus*, contains sound general advice on securing dual stack systems. RFC 4942, *IPv6 Transition/Coexistence Security Considerations*, includes many specific details:

- a) Organizations need to implement a consistent security policy for both IPv4 and IPv6 (including firewalls and packet filters);
- b) Organizations should account for new IPv6 functionality. This functionality may include mobility, stateless address autoconfiguration, neighbour discovery, privacy addresses and end-to-end encryption with IPsec;
- c) Because both protocols are running, unexpected tunneling between the hosts may occur. The result may violate security policies;
- d) Organizations must upgrade intrusion detection or intrusion prevention systems, firewalls, monitoring, logging and auditing to provide IPv6 protection equivalent to what was available for IPv4. If tunnelled packets are allowed to enter the network, the firewall or IDS/IPS system must be able to perform deep packet inspection; and

MCMC MTSFB TC TXXX:2015

- e) The performance of security systems may degrade when handling IPv6 (when using the same resources compared to IPv4).

Good security practice dictates disabling unneeded services. Network administrators deploying IPv6 dual stack should configure nodes (hosts, servers, routers, etc.) to treat the IPv6 protocol as preferred and phase out remaining instances of the IPv4 protocol in a timely manner. When a given IPv4/IPv6 node no longer needs IPv4 services, administrators should disable the IPv4 protocol. Employing both protocols is useful during the early phases of IPv6 deployment, but the practice becomes a security risk because of increased complexity.

Administrators also need to watch for an unintended dual stack transition due to IPv6 being enabled prematurely. Security organizations should monitor for IPv6 traffic. Organizations should also audit router and neighbour solicitations to detect the insertion of rogue routers and devices on the network.

Security and network administrators should have an incident response plan in place for responding to violations of the configuration and security policies.

7.3 Tunneling

Tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure or IP core network. By using overlay tunnels, user can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. Tunnels can be configured between border routers or between a border router and a host; however, both tunnel endpoints must support dual stack protocol (IPv4 and IPv6 protocol stacks). Following are types of tunneling mechanisms:

- Generic routing encapsulation (GRE);
- IPv4-compatible;
- 6to4; and
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).

Table 4. Summary of IPv6 Tunneling Mechanism

Tunneling Type	Tunnel Configuration Parameter			
	Tunnel Mode	Tunnel Source	Tunnel Destination	Interface Prefix or Address
Manual	ipv6ip	An IPv6 address, or a reference to an interface on which IPv4 is configured	An IPv4 address	An IPv6 address
GRE/IPv4	gre ip		An IPv4 address	An IPv6 address
IPv4-Compatible	ipv6ip auto-tunnel		Not required. These are all point-to-multipoint tunneling types. The IPv4 destination address is calculated on a per-packet basis from IPv6 destination	Not required. The interface address is generated as ::tunnel-source/96
6to4	ipv6ip 6to4		An IPv6 address. The prefix must embed the tunnel source IPv4 address	
ISATAP	ipv6ip isatap		An IPv6 address prefix in modified eui-64 format. The IPv6 address is generated from the prefix and the tunnel source of IPv4.	

7.3.1 Manually Configured Tunneling

A manually configured tunnel is equivalent to a permanent link between two IPv6 domains over an IPv4 backbone.

An IPv6 address is manually configured on a tunnel interface and manually configured IPv4 addresses are assigned to the tunnel source and the tunnel destination. The host or router at each end of a configured tunnel must support dual stack (IPv4 and IPv6 protocol stacks). Manually configured tunnels can be configured between border routers or between a border router and a host.

7.3.2 GRE Tunneling

When GRE IPv6 tunnels are configured, IPv6 addresses are assigned to the tunnel source and the tunnel destination. The tunnel interface can have either IPv4 or IPv6 addresses assigned. The host or router at each end of a configured tunnel must support dual stack (IPv4 and IPv6 protocol stacks).

7.3.3 Automatic GRE Tunneling

Automatic tunneling is a technique by which the routing infrastructure automatically determines the tunnel end point. With automatic tunnels, one tunnel endpoint can find the other end without pre-configuration. One way for IPv6 over IPv4 tunnels to accomplish this is by embedding IPv4 addresses in IPv6 addresses. Automatic tunneling is suitable to be used in the early stages of IPv6 transition. Some of the automatic tunneling mechanisms are discussed in the subsequent sections:

- a) 6to4 Tunneling (RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds*) – router to router;
- b) ISATAP – intra-site tunnels; and
- c) Tunnel Broker – using a server for automatic tunneling.

7.3.4 6to4 Tunneling

RFC 3056 recommends automatic 6to4 tunnel. 6to4 is an internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 backbone without the need to physically configure explicit tunnels.

Basically, 6to4 performs three (3) functions:

- a) Assigns a block of IPv6 address space to any host or network that has a global IPv4 address;
- b) Encapsulates IPv6 packets inside IPv4 packets for transmission over an IPv4 network using 6in4; and
- c) Traffic route between 6to4 and "native" IPv6 networks.

7.3.5 ISATAP

ISATAP uses the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link-local IPv6 address.

ISATAP is designed for transporting IPv6 packets within a site where a native IPv6 infrastructure is not yet available; for example, when sparse IPv6 hosts are deployed for testing. ISATAP tunnels allow individual IPv4 or IPv6 dual-stack hosts within a site to communicate with other such hosts on the same virtual link, basically creating an IPv6 network using the IPv4 infrastructure.

Although the ISATAP tunneling mechanism is similar to other automatic tunneling mechanisms, such as IPv6 6to4 tunneling, ISATAP is designed for transporting IPv6 packets within a site, not between sites. More information regarding this method is available in RFC5214, *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*.

MCMC MTSFB TC TXXX:2015

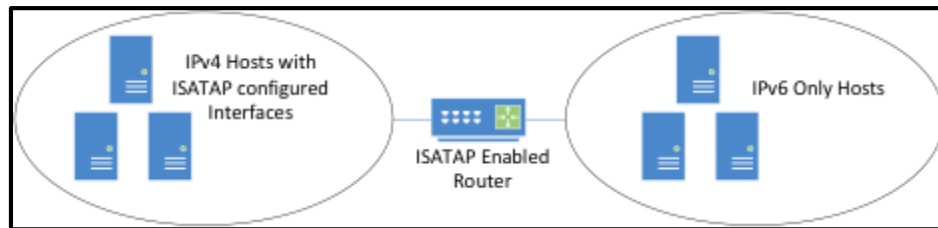


Figure 7. ISATAP Tunneling mechanism

7.3.6 Tunnel Brokers

A tunnel broker is a service that provides a network tunnel. These tunnels can provide encapsulated connectivity over existing infrastructure to another infrastructure.

IPv6 tunnel brokers provide dual stack IPv4/IPv6 nodes on IPv4 networks with a way to obtain IPv6 connectivity without the administrative support of a large site running, for example, 6to4. Tunnel broker is intended for small sites or individual hosts. The IPv6 tunnel broker method requires the deployment of a tunnel broker server. More information on IPv6 tunnel brokers is available in RFC 3053, *IPv6 Tunnel Broker*.

7.4 Translation

The concept of address translation is also not a new concept to most network engineers; this is because Network Address Translation (NAT) is implemented between different IPv4 networks in almost every residential household. The concept behind this type of NAT and the newer technologies that support address translation between IPv4 and IPv6 networks is similar. IPv6 translation technologies differ from IPv6 tunneling technologies; this is because the translation technologies enable IPv4-only devices to speak to IPv6-only devices, which is not possible with any of the tunneling methods.

However, IPv4/IPv6 translation and IPv4-only translation entail a certain amount of complexity. In some situations, a secondary technology is required to step in and provide additional services for the connection to work such as when an IPv6-only device attempts to communicate with a device on the public IPv4 Internet and only has IPv4 DNS record (A).

The first method to be introduced to provide IPv6 translation services was Network Address Translation - Protocol Translation (NAT-PT). NAT-PT defined a mechanism to not only translate between IPv4 to IPv6 addresses but also a built-in ability to provide protocol translation services for Internet Control Message Protocol (ICMP), File Transfer Protocol (FTP) and Domain Name System (DNS). The component that was responsible for these translation services is called the Application Layer Gateway (ALG).

The ALG piece of the NAT-PT method raised a number of issues. With additional testing and real-life experience, a new method was introduced that separated the address translation functionality and the application layer translation functionalities: NAT64 and DNS64.

DNS64 can synthesize IPv6 address resource records (AAAA) from IPv4 resource records (A); it does this by encoding the returned IPv4 address into an IPv6 address format.

7.5 IPv6 Deployment

The IPv6 deployment should include the following stages:

- a) Building the Team;
- b) Setting Goals, Requirements and Scope;
- c) Initiation Phase / Analysis;

- d) Acquisition/Development Phase;
- e) Implementation Phase;
- f) Operations/Maintenance Phase; and
- g) Disposition Phase.

The framework calls for a phased approach or a gradual transition from IPv4 to IPv6. The use of a phased implementation will enable an organization to implement IPv6 with as little disruption to the current environment as possible. Existing users should be unaware of the new protocol until they require its use. The phased approach will minimize the effect on day-to-day operations. There are two main approaches to transition deployment:

- a) Pervasive IPv6 deployment; and
- b) Sparse IPv6 deployment.

In a pervasive approach, the organization enables dual (IPv4/IPv6) stack equipment rapidly throughout the entire enterprise. This scenario is appropriate when an organization has mostly new equipment that supports both IPv4 and IPv6. After the organization validates core services and translation mechanisms are functioning properly, it is suggested that IPv4 can be disabled on all equipment, leaving an IPv6 dominant network.

Edge to core describes a sparse IPv6 deployment. In this approach, organizations enable groups or islands of IPv6 equipment in an IPv4 dominant network. After most of the edge devices transition to IPv6, the network core transitions to either dual stack or IPv6 only. A sparse IPv6 deployment requires supporting both IPv4 and IPv6 traffic throughout the duration of the deployment life cycle. This approach makes extensive use of IPv4/IPv6 and IPv6/IPv4 tunneling. This scenario is appropriate when an organization has a large installed base of older equipment or services that cannot transition to IPv6.

Software or applications may be more important than equipment when selecting a transition approach. Upgrades for hardware and embedded operating systems can be quicker than custom or off the shelf applications. The hardware vendors have been working towards IPv6 support for longer than application software vendors have. Many vendors may not be able or willing to upgrade software to support IPv6 and many organizations do not have the expertise in house to upgrade the code base. The more legacy applications and custom code an organization supports (either developed in house or highly customized off the shelf software) the greater the risk that the software will not support IPv6. Transition planners must address software in the approach to IPv6 transition.

The two (2) main differences between an IPv6 pervasive deployment and an IPv6 sparse deployment are:

- a) The IPv6 pervasive deployment has a shorter lifecycle than an IPv6 sparse deployment.
- b) An IPv6 sparse deployment will take longer and make use of tunneling mechanisms.

Both deployment scenarios (IPv6 pervasive deployment and IPv6 sparse deployment) are covered by the same general deployment plan. All phases of the lifecycle are the same regardless of approach.

7.5.1 Building the team

Because the network reaches into every aspect of business, organizational concerns become the biggest challenge in IPv6 deployment. This type of project does not fall solely within the IT domain; thus, IT cannot unilaterally implement a solution. The interconnected and always-on nature of the business means that a bottom-up approach is insufficient. Many different groups have to work together for an IPv6 project to be successful, executive support and leadership is critical for success. As a result, the team needs to be cross-functional and the pilot implementation cannot rely on the resources of a single department.

MCMC MTSFB TC TXXX:2015

In large organization, the team should consist of corporate IT, local network and desktop support teams, and information security. An example of sample project team, responsibilities and workload is given in Table 5.

Table 5. Sample Project Team, Responsibilities and Workload

Key Area	Unit	Role	Nomination Planner/ Engineer/ Consultant Name (Resources name)	Estimated FTE (Full Time Equivalent) = 1 person full time
Project Management	PM Office	Timeline		0.8
		Project Manager (End to End project review technical, commercial and product/marketing)		0.8
		Policy		1
		Update to regulatory		1
	Steering Committee	Driver		2
		Governance		1
Technical	Planning and Development	Network Team (Core, Access)		5
		System Administrator (server and database team)		5
		Charging and Billing		5
		Application (VAS) and Content provider		4
		Web Portal (Application and Syslog)		1
	Implementation	Proof Of Concept (POC)		5
		Production rollout		5
	Operation	OSS, BAU integration, Services and network support		2
Commercials	Finance	PO Process (dedicate for IPv6 project)		2
	Procurement	To source IPv6 Vendors.		1
Product and Marketing	End-user Customer Consultant /	Training/Education of IPv6		1
	Devices	Certificate of IPv6 compliance, device configuration		1
	Product and Application	Product specialist		2

MCMC MTSFB TC TXXX:2015

Key Area	Unit	Role	Nomination Planner/ Engineer/ Consultant Name (Resources name)	Estimated FTE (Full Time Equivalent) = 1 person full time
	Marketing and Sales	Introducing IPv6 Services to customers		2
		Benefit of IPv6		1

Project Management is the key area for the success of IPv6 implementation. Following are the scope of work under Project Management:

- a) Require to setup a project team which consists of various departments such as regulatory, PMO (project management office), network department, IT department, marketing/product, device management team, etc.
- b) The project manager will drive the team from impact analysis, design, POC until the completion of the production rollout within the target timeline.
- c) Apart from the design & implementation, the project team will also come out with the new policy and process for IPv6 implementation as well as for future IPv6 address assignment.
- d) Steering committee will govern the project progress and address the project issue escalation.

7.5.2 Goals, Requirements and Scope

One of the first steps in the deployment of IPv6 is to define the goals, requirements and scope. The team should consider on where and how IPv6 integration might happen, creating a wide range of options, including voice services, wireless devices, building automation and data centres.

Implementation across the network infrastructure and a defined set of desktops provided the foundation for services and applications to use when they are ready. An example of goals for deployment could be:

- a) Provide a publicly accessible IPv6 Internet presence;
- b) Facilitate IPv6-enabled user access in the network; and
- c) Build toward end-to-end IPv6 in the network using dual stacks.

Supporting both IPv4 and IPv6 devices with a common infrastructure is the goal, providing a consistent user experience without users needing to be aware of which protocol they are using. Over the longer term, IPv4 will fade away, but this process could take many years. In the meantime, the team must identify the fundamental project requirements:

- a) Integration must not affect any existing services and applications.
- b) There must be no reduction in the corporate security posture.
- c) Reuse existing infrastructure, capabilities, content, and application environments whenever possible.
- d) Deployment covers a broad range of applications and devices and must be prioritized across all IT functions.

The following goals can be used:

MCMC MTSFB TC TXXX:2015

- a) Mobile data growth has led to IPv4 address exhaustion. Furthermore 4G LTE requires always on connection for voice over IP service. The ultimate solution is to migrate to IPv6.
- b) As the applications and devices are moving towards IPv6 enabled, public accessibility to IPv6 internet is essential.
- c) As more and more applications are migrating to IPv6, it is necessary to provide user access to these applications on enterprise network in future.
- d) Unlike IPv4, IPv6 come with the security feature to enhance the network robustness to protect the network from the attack of the hackers.
- e) IPv6 has QoS feature which allows the service providers to offer differential services.
- f) With the implementation of IPv6, it allows the interconnection to IPv6 only network.

Requirements:

- a) Implementation shall be transparent to the existing products, services and applications. There shall be seamless experience to the users.
- b) No compromise on corporate security. There shall be no impact to the security measure during the deployment.
- c) Shall reuse existing IPv6 capable infrastructure, capabilities, content, and application. As much as possible, minimizing or avoiding (whichever possible) the change of the existing infrastructure. Software patch and update is highly recommended.
- d) Managing the priority for applications & devices across all IT functions. During the deployment, there might be a long list of applications and devices for IPv6 implementation. Prioritizing the application and devices according to the criticality and severity is important. The deployment starts with the very high critical and high severity of the applications and devices following up by the less critical ones.

The IPv6 network infrastructure is generally consist of user end, access network, network core, transport core and other branches or ISP connection/internet. Figure 8 shows the scope of deployment, i.e IPv6 End-to-End Solution.

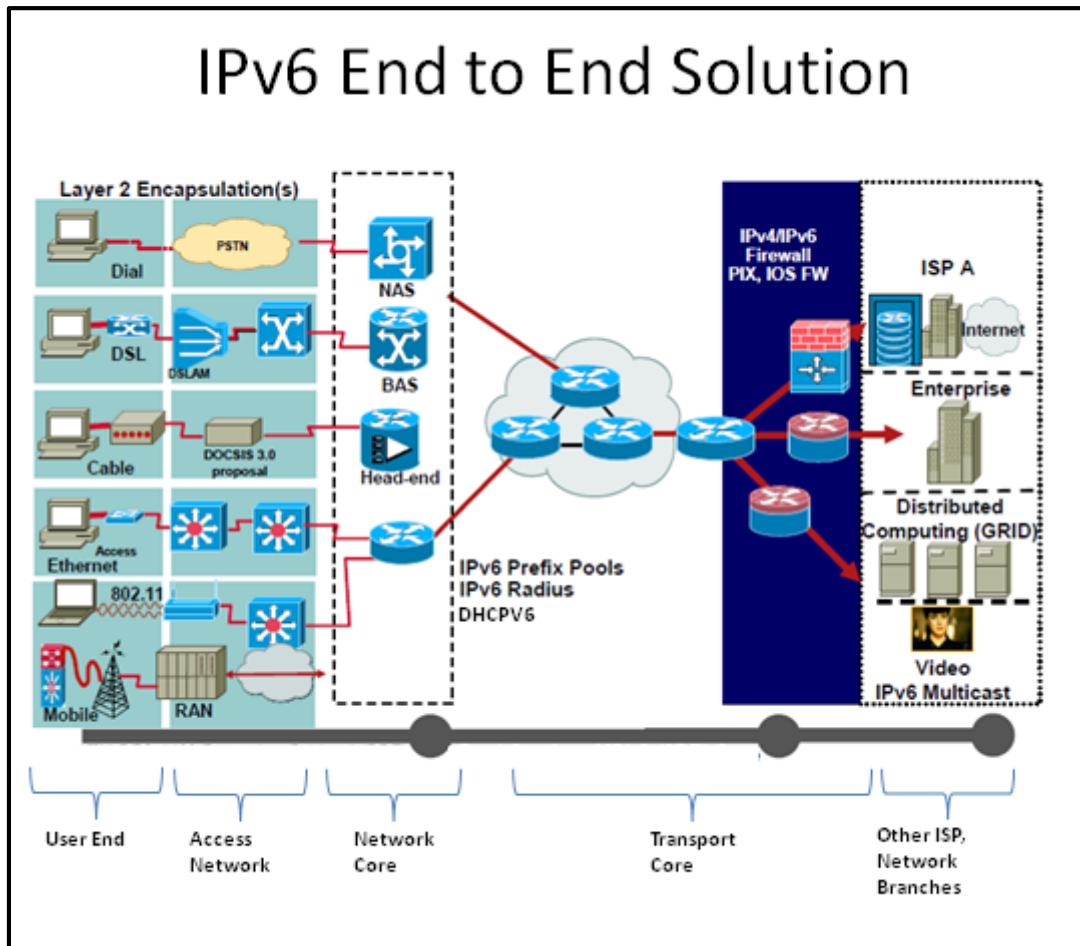


Figure 8. IPv6 End-to-End Solution

7.5.3 Initiation Phase

The next step in the plan is to extend the existing IT department's methodologies and processes to include a framework of IPv6 solution services, aiming to standardize each deployment to the maximum extent possible. The team should plan to build or modify its network management and deployment tools to handle IPv6 addresses. Specific tools can be used to generate the appropriate addresses, subnets, and VLANs for each router, using a consistent numbering scheme.

An important part of the implementation and best practice for large or complex deployments is a controlled lab environment. Building the lab allowed the team to test and evaluate the effect of dual-stack operations on the network. The team could look for adverse side effects IPv6 might have on the existing IPv4 network and applications. Using the lab, the team can identify all the aspects that are crucial for deployment such as required time, people and budget.

The initiation phase is concerned with requirements gathering. It is important for an organization to understand its current environment before deploying IPv6. By understanding the current environment, the correct transition approach can be selected and an organization can ensure that it maintains security parity between its IPv4 and IPv6 environment.

An organization must also begin to plan for new IPv6 features. The transition to IPv6 gives an organization an opportunity to fix problems in its current environment. IPv6 addressing will allow more opportunities to aggregate addressing and simplify routing and access control rules if requirements are collected early.

MCMC MTSFB TC TXXX:2015

One of the key tasks in the initiation phase is to conduct an extensive inventory of the IP equipment and services. RFC 4057, *IPv6 Enterprise Network Scenarios*, covers the types of questions that an organization needs to answer to plan a successful IPv6 transition. Different scenarios break out these questions, because each type of organization will have unique transition requirements.

All organizations have the same similarities which are IPv4 assets that require transition to IPv6. In an effort to understand the transition requirements, an organization must perform an asset discovery. While it is feasible that asset discovery could populate a configuration management database (CMDB), the primary purpose of asset discovery in an IPv6 transition plan is to gather transition requirements.

Transition requirements determine which assets will transition to IPv6, the order assets will transition, the transition methods selected and the security controls implemented. The type of information that can help determine if an asset or service will transition to IPv6, require some other coexistence mechanism, or be replaced include system security categorization, operating system and applications, lifecycle replacement and dependencies.

Most organizations have a large installed base of legacy equipment and applications. Many legacy systems cannot support IPv6. IPv6 is widely supported by network equipment vendors, and desktop systems and productivity applications generally support IPv6. Firewall and IDS implementations also are beginning to have good support for IPv6. Where organizations have difficulties supporting IPv6 is with management applications, embedded systems, and legacy applications. Legacy applications that implement network protocols or process network addresses were not written to support IP-Agnostic² addressing (IPv4/IPv6). There were no requirements for IPv6 address handling. These applications' code assumes 32-bit addressing. The application code logic and storage allocations work with IPv4 addressing. It will take a long time to update legacy applications to support IPv6. Applications that cannot support IPv6 require the evaluation and selection of co-existence mechanisms. Organizations should plan that a significant number of legacy applications will not natively support IPv6 and include requirements to support accessing IPv4 only applications and services by IPv4 and IPv6 clients.

The information captured in this inventory should populate the organization's IPv6 configuration management database and be maintained by configuration management. Configuration management data will not be perfect and will become out of date with the production environment. An organization must decide the acceptable level of accuracy needed to make good decisions and build processes to maintain the inventory data within the established parameters.

The following decisions need to be made for each piece of equipment:

- a) Will the equipment be replaced to support IPv6?
- b) Can a service be upgraded to support IPv6?
- c) Will a translation mechanism be necessary?

The asset inventory is the main input into the organization's decision process concerning the deployment scenario. If the inventory demonstrates mostly new equipment, an IPv6 pervasive scenario is available as a deployment option. On the other hand, if the inventory demonstrates mostly older equipment that cannot readily support IPv6, then an IPv6 sparse deployment scenario is the more likely choice.

Organizations should consider the life cycle replacement of equipment in conjunction with the IPv6 rollout schedule. When possible, the IPv6 rollout schedule should align with the lifecycle replacement to reduce costs of the overall transition. Organizations that do not align schedules should plan for additional costs.

² IP-Agnostic means that the application should be able to function well when:

- IPv4 and IPv6 are installed
- IPv4 is the only network layer protocol installed
- IPv6 is the only network layer protocol installed

Other requirements to be considered are:

- a) Security;
- b) Routing;
- c) Network Management;
- d) Host Configuration;
- e) Address Planning;
- f) Application Support and Development;
- g) Performance and Bandwidth;
- h) Hardware and software; and
- i) Checklist Document – Annex B.

7.5.4 Acquisition/Development Phase

The acquisition and development phase is concerned with taking the requirements gathered during the initiation phase and developing the IPv6 enterprise architecture. When developing the IPv6 environment, the current enterprise architecture should be considered. The acquisition/development phase will work with three (3) different architectures:

- a) the “as is” IPv4 based enterprise architecture;
- b) the “to be” IPv6; and
- c) the transitional architecture that bridges the “as is” and “to be”.

During the development phase, an organization should plan for an IPv6 evaluation pilot. The goals of an IPv6 pilot are to test IPv6 configuration and design assumptions against existing equipment, test and evaluate new IPv6 equipment and begin training staff. The pilot is the time to test the IPv6 numbering plan and other design assumptions. It is easier and less expensive to correct design deficiencies earlier in the transition lifecycle. As the requirements are evaluated against the existing equipment, inventory gaps may be discovered. It should be expected that some equipment will not make the transition; either it does not support IPv6 or does not meet performance expectations. The pilot should be used to evaluate new equipment and its ability to coexist in the “to be” and transition architectures. The pilot is a great opportunity to allow technical staff to develop their IPv6 skills. A pilot affords the opportunity to combine classroom training with a hands-on environment.

IPv4 and IPv6 are different protocols; they behave differently on similarly configured equipment. The IPv6 pilot should include testing to validate the performance of IPv6 in the environment and to develop strategies to mitigate any problems. IPv6 generally performs worse on equipment that was designed for IPv4. This is mainly the result of IPv6 header manipulation in software instead of hardware. Other factors besides header size can degrade performance, including extension headers, large packet sizes, and differences in fragmentation characteristics. This performance difference can vary.

The pilot should establish the baseline performance of IPv4 only, IPv6 only and dual stack equipment and services. The baseline performance will allow the enterprise architects to understand the different performance characteristics and to design capacity into the “to be” and transition architectures. When possible the testing should use production configuration to reduce the variation between the production and the test environment.

When establishing a baseline for security equipment, performance and coverage measures must be established. Security equipment evaluates traffic, which introduces latency into the network and reduces network throughput. IPv6 security equipment tends to have fewer known heuristics available for identifying potentially suspicious traffic than equivalent IPv4 equipment, which reduces the level of traffic coverage and potentially increases risk. Testing should be performed after establishing equivalent levels of coverage between IPv4 and IPv6. All security controls should be tested to include access

MCMC MTSFB TC TXXX:2015

control list, firewall rules and IDPS signatures. The goal should be to design an IPv6 environment that is as secure as or more secure than the IPv4 environment.

Another area the pilot should address is the validation of tunnel performance. A mixed IPv4/IPv6 environment uses tunnels to connect the islands of similar protocol equipment. The performance of these tunnels affects the user experience, availability and scalability of the network. Each transition mechanism has different performance characteristics. Before the pilot begins, the enterprise architecture team should select the appropriate mechanism based on functionality, performance and the capabilities of the communicating peers. The testing of tunnels requires a realistic environment.

The final area the pilot should address is baseline transition mechanisms. Translation is performed in software and incurs a performance penalty.

In addition to developing the “to be” and transition enterprise architectures and running the IPv6 pilot, the other activities of the acquisition and development phase include:

- a) Developing a risk assessment;
- b) Developing a sequencing plan for IPv6 implementation;
- c) Developing IPv6 related policies and enforcement mechanisms;
- d) Developing training material for stakeholders; and
- e) Developing and implementing a test plan for IPv6 compatibility/interoperability.

IPv6 Enterprise Architecture introduces new risks into the current environment. These risks can be the result of many different factors, including reduced security coverage, new IPv6 features, lack of IPv6 experience, degraded performance, and dual operations. A formal risk assessment must be performed with a risk mitigation strategy to address the identified risks. The risk assessment drives several other deliverables, including the security plan and certification and accreditation.

The transition to IPv6 offers a clean slate in implementing ingress and egress firewall rules. Organizations should have few IPv6 source or destination addresses that traverse the perimeter. Organizations, at this point, should be able to implement a deny all, permit by exception IPv6 firewall policy. In the future, as new external connections are required, either in bound or out bound, they can be documented and allowed by exception.

As the transition enterprise architecture is developed, a transition plan must also be developed. The transition plan details which equipment and servers are to be transitioned and in which order. The transition plan, which includes a coexistence plan, drives the project plan. The coexistence plan documents the type of transition mechanism used to connect islands of like protocol hosts and will also document the translation mechanisms for enterprise services.

Existing policies must be reviewed to determine whether they provide adequate coverage for IPv6. New policies should be developed to address IPv6 specific areas or areas where IPv6 has a significant impact. Senior leadership should support the new policies and sign off on them. Once policies are established, standards, procedures, and guidelines can be developed to provide guidance for equipment configuration and operation. The procurement policies should be amended early in the transition to require that all new equipment introduced to the environment support IPv6. This requirement should include both equipment that is lifecycle replacement and equipment introducing new capabilities. In many cases, existing policies can simply be amended.

IPv6 affects a broad range of support and operations personnel. During the acquisition and development phase, individual jobs should be evaluated and training material should be developed or identified. IPv6 skills are not ready available in the job candidate pool and organizations should expect to increase training budgets for IPv6 training for existing staff and new hires.

Proving the connectivity and interoperability of the enterprise architecture is a key factor in the success of the IPv6 transition. To ensure a successful transition, organizations must develop measures and test procedures for key services, applications, and capabilities. These measures and procedures collectively are the test plan. After a service, application or capability is migrated, the test plan validates that the IPv6 equivalent provides service equal to or better than the IPv4 service.

At the conclusion of the acquisition and development phase, an organization should have produced the following artifacts:

- a) Enterprise Architecture;
- b) Address Allocation Plan;
- c) Address Management Plan;
- d) Routing Plan;
- e) Training Plan;
- f) Security Plan; and
- g) Coexistence Plan.

The first design decision is to determine the organization's IPv6 address allocation. The size of the address space required to support the deployment depends on the number of devices and how many networks those devices require.

At this point, the organization should request an IPv6 address allocation from their RIR.

The organization also needs to create an address management plan. The address management plan documents the following:

- a) How devices allocate an address (for example, clients could use autoconfiguration or DHCPv6);
- b) Which nodes will have fixed IP addresses; and
- c) How to update DNS with address ranges.

The training plan documents the training requirements across the organization as related to the IPv6 deployment. Typically, core engineers, help desk support, application developers, the security team and system administrators will need training. The training plan includes both the types of training and length of training required. Training should allow IT operations to support IPv6 in production along with their current job specifications. Poor security practices, misconfiguration and operator error are some of the leading causes of system compromise and loss of availability. Increasing staff knowledge about security and the computing environment will increase security and availability.

The goal of the security plan is to ensure that the IPv6 environment has the same level of security or better than the existing IPv4 environment. It should document how an organization plans to maintain security parity during the IPv6 deployment. The security plan should address the following areas:

- a) Equipment configuration;
- b) Perimeter defence (firewall, ACL, IDPS);
- c) Content filtering;
- d) Mail filtering;
- e) Patch management;
- f) Vulnerability management (scanning);
- g) Certification and accreditation of the new systems;
- h) AAA (authentication, authorization, and accounting);
- i) Rogue detection; and

MCMC MTSFB TC TXXX:2015

- j) Infrastructure protocol security.

The coexistence plans documents which mechanisms support IPv6/IPv4 internetworking. The coexistence plan details how IPv6 clients will access legacy IPv4 services (i.e. deployment of which translation mechanisms) and how existing IPv4 clients will access IPv6 services. By planning the coexistence mechanism in advance, an organization is able to leverage economy of scale and select technology that can be a repeatable solution. This reduces the amount of required training and increases operator familiarity with the mechanisms.

7.5.5 Implementation

The implementation phase involves the secure installation and configuration of IPv6 equipment and transition mechanisms. The deployment stage differs depending on which deployment scenario is used (IPv6 pervasive deployment or IPv6 sparse deployment). In both scenarios, the actual IPv6 roll out involves a phased deployment. The first three steps are the same regardless of deployment scenario.

The steps for the IPv6 pervasive deployment are as follows:

- a) Enabling perimeter firewall IPv6 policies and IPv6 access control lists and configuring devices in accordance with security plan, standards, and procedures.
- b) Deploying external IPv6 connectivity with exterior IPv6 routing.
- c) Deploying basic IPv6 services (DNSv6, DHCPv6, Remote Access, NTPv6).
- d) Deploying IPv6 interior routing.
- e) Enabling management monitoring (SNMPv6, service monitoring, IDPS, authentication, statistical monitoring, and netflow).
- f) Synchronisation of core, distribution, access network equipment and syslog server to NTPv6 / PTPv6 according to agreed stratum.
- g) Enable public facing services (web service, email, ftp).
- h) Enabling IPv6 hosts.
- i) Deploying translation mechanisms, if required.

The steps for the IPv6 sparse deployment are as follows:

- a) Enabling perimeter firewall IPv6 policies and IPv6 access control lists and configuring devices in accordance with security plan, standards, and procedures.
- b) Deploying external IPv6 connectivity with exterior IPv6 routing.
- c) Deploying basic IPv6 services (DNSv6, DHCPv6, Remote Access, NTPv6).
- d) Enabling dual protocols on core routers (this step can be performed at this point or after completing Step (e)).
- e) For each IPv6 Island, enable IPv6 on hosts.
- f) Enabling management monitoring (SNMP, service monitoring, IDPS, authentication, statistical monitoring, and netflow).
- g) Deploying translation mechanisms, if required.

With Step (e) above, the process is iterative until all hosts are either dual stack or IPv6 enabled.

Organizations should have a change control committee that enforces the change control process. The security manager should be a member of the change control committee. An IPv6 transition should follow established change control processes. Once a system is transitioned, it should be accredited and certified using inspection and acceptance testing. The measures and test procedures developed during the acquisition and development phase are used to certify that the transition equipment performs in the environment as intended.

Organizations must validate IPv6 migrated equipment by inspecting the configuration and running test procedures before transitioning devices to production. Device configurations must comply with established security and operations standards. Device configuration settings can be validated using either manual inspection or automated inspection tools. When possible, the use of automated compliance management solutions will increase the accuracy and consistency of configuration compliance.

Transitioned equipment must integrate and interoperate with other production and migrated equipment and systems. Integration validates that equipment is able to communicate with other systems and equipment and correctly exchange data. Checklists should be consulted that list the services with which a transitioned device must interoperate. Some examples include routing neighbours, DNSv6, DHCPv6, NTPv6, SNMP trap servers, syslog servers, mail servers and application gateways.

Transitioned equipment must perform at the levels established in the test plan. Performance testing may be validated using live traffic or load generators. Failure to comply with test plans could result in a loss of availability when the equipment is placed into production.

IPv6 migration efforts require the certification and accreditation of systems. The migration to IPv6 (either IPv6 or dual stack) has the potential to significantly change the existing security posture. While the same security controls required for IPv4 are also required for IPv6, existing controls require reworking and reconfiguration to support IPv6 and new security controls are required to mitigate new IPv6 vulnerabilities. Organizations should plan on certifying and accrediting systems that have been migrated to IPv6 and systems that interact with IPv6 systems. Organizations should evaluate their certification support tools, techniques and procedures to ensure that these support IPv6. Organizations should ensure auditors performing the certification function are knowledgeable about IPv6 security and have the tools to look for IPv6 traffic and vulnerabilities. If two separate environments are supported (IPv4 and IPv6), then a system accreditor may require two separate certifications and accreditations; with a dual stack environment only a single certification and accreditation may be required. The goal should be to achieve security as good as or better than the IPv4 network.

7.5.6 Operation and Maintenance

The operations phase often begins concurrently with the implementation phase. During operations, the focus is the secure operation of a dual stack or mixed IPv6/IPv4 environment. One of the most difficult challenges facing the operations staff in a mixed IPv6/IPv4 environment is keeping the two environments synchronized.

When operations makes changes to security controls such as firewall rule sets, access control lists and IDS signatures, they must ensure the change occurs on both the IPv4 and IPv6 networks. Rules and signatures must be translated between IPv4 and IPv6 syntax and deployed as a single coordinated process. If strict change control is not followed, the two environments will have non-overlapping protections.

In a dual stack environment, the physical topologies of the equipment are the same, but the logical topologies can be very different. Configuration changes can have unpredictable or unforeseen consequences. Configuration management controls should be structured to prevent configuration changes on IPv4 or IPv6 networks that affect the other network. Organizations should manage and monitor their IPv4, IPv6 and dual stack environment as a single environment.

Monitoring the use of the internet connectivity should be done for IPv6 as it is done for IPv4. This includes the use of IPFIX, as describe in RFC7012, *Information Model for IP Flow Information Export (IPFIX)*, to report abnormal traffic patterns (such as port scanning, SYN flooding and related IP source addresses) from monitoring tools and evaluating data read from SNMP MIBs [RFC4293] (some of which also enable the detection of abnormal bandwidth utilization) and syslogs (finding server and system errors). Where NetFlow is used, Version 9 is required for IPv6 support. Monitoring systems should be able to examine IPv6 traffic, use IPv6 for connectivity and record IPv6 addresses, and any log parsing tools and reporting need to support IPv6. Some of this data can be sensitive (including personally

MCMC MTSFB TC TXXX:2015

identifiable information) and care in securing it should be taken, with periodic purges. Integrity protection on logs and sources of log data is also important to detect unusual behaviour (misconfigurations or attacks). Logs may be used in investigations, which depend on trustworthy data sources (tamper resistant).

In addition, monitoring of external services (such as websites) should be made address specific, so that people are notified when either the IPv4 or IPv6 version of a site fails.

Some of the key aspects of IPv6 operational considerations are as follows.

- a) Addressing: There are many considerations, recommendation and best practices related on IPv6 addressing operational topics which are documented in a variety of IETF documents e.g. RFC7381, RFC4193, RFC4192, RFC5887 and draft-ietf-v6ops-dc-ipv6-01.
- b) Management Systems and Applications: Organization may use Internet Protocol address management (IPAM) software, provisioning systems and other variety of software to document and operate. It is important that these systems are prepared and possibly modified to support IPv6 in their data models (see Section 6.1.1).
- c) Monitoring and Logging: Monitoring and logging are critical operations in any network environment and they should be carried at the same level for IPv6 and IPv4. It is important to consider that the collection of information from network devices is orthogonal to the information collected. For example it is possible to collect data from IPv6 MIBs using IPv4 transport. Similarly it is possible to collect IPv6 data generated by Netflow9/IPFIX agents in IPv4 transport. In this way the important issue to address is that agents (i.e. network devices) are able to collect data specific to IPv6.
- d) Security Considerations: A thorough collection of operational security aspects for IPv6 network is available in *ietf-opsec-v6*. Most of them are applicable in the environment we consider in this Technical Code.

7.5.7 Disposition

A migration from IPv4 to IPv6 results in displacement or retirement of equipment. Some equipment does not support IPv6 and is retired, while other equipment is transferred to IPv4 islands or to other organizations. Organizations must plan for the secure disposition of this obsolete equipment, ensuring that no confidential data is released. Organizations place themselves at great risk for exposing confidential information when disposing of obsolete equipment.

A key decision concerning sanitization is whether the equipment is planned for reuse or retirement. Often, equipment is reused to conserve an organization's resources. Equipment should be sanitized before it is reused or retired. Most organizations have policies, regulations or standards that require the proper disposition of obsolete equipment. It is important that these processes be followed.

Failure to follow proper disposition procedures could result in the disclosure of confidential information. Organizations store and process information such as personal records of employees, personal records of clients, credit card numbers, social security numbers, medical information, trade secrets, classified data, system passwords, system configuration, network documentation and many other examples of data that must be kept confidential. Network equipment can expose administrative accounts, passwords, authentication credentials, certificates, pre-shared keys and community strings.

8. Technology Education

The proper planning of the IPv6 integration project, the development and implementation of complete related policies, and the seamless deployment of the technology depend on the staff's familiarity with IPv6. All planning steps presented so far in this chapter cannot be successfully implemented without a good understanding of the various aspects of the technology. The scope of the project cannot be clearly

defined without the strategy team understanding the protocol characteristics and its potential. Assessment cannot be effectively performed without understanding the IPv6 features that must be supported by various elements of the environment. Entrance/acceptance and security policies cannot be updated without an understanding of the standardization state of the protocol and its features. The successful deployment of the protocol requires an operations team that is familiar with managing and troubleshooting IPv6. For these reasons, initiating IPv6 training very early and scaling it to match the project evolution is essential to its success.

8.1 Training Need / Knowledge Acquisition

8.1.1 Training Domains

The diverse population involved in the various aspects of the IPv6 integration requires diverse forms of targeted training. The right amount and level of education needed for each technical or business function must be delivered in a timely and cost-effective way:

- a) IPv6 technology: The most common form of training available today focuses on describing the protocol operation through a side-by-side comparison with IPv4.
- b) IPv6 deployment: This type of training focuses less on the protocol description and more on its integration in real networks. It has to address the specific interests of each environment: enterprise (branch office, campus, data centre) versus service provider (core, broadband, wireless). It also focuses on the operational aspects of IPv6 infrastructures.
- c) IPv6 security: The unique aspects of IPv6 security must be well understood by the IT operations staff well in advance of a deployment. The security policies must be adjusted to deal with the new protocol and its use by various user and device types. New security paradigms might emerge with IPv6.
- d) Networking equipment: These are traditional vendor classes that describe the specifics of equipment configuration and operation.
- e) Operating system and applications: New versions of OSs or applications that include IPv6 require additional training for system managers and software developers.
- f) Software development: This type of training focuses on the IPv6 features that can be leveraged when developing new applications.
- g) End users: Although this type of training is for the most part IP version agnostic, it familiarizes users with new applications that run over IPv6. This training is important in ensuring the smooth adoption of applications and services deployed over IPv6.

8.1.2 Training Assessments

Everyone does not need the same skill set or training at the same time. Just-in-time training is based on technology being a required skill set, technology being developed/deployed and location. The focus of the assessment should be to enable people for success at the right time.

8.1.2.1 Certification compliance

Certification program ensures the technical competence of IPv6 professionals through a tangible measurement of skills and knowledge. Exams go beyond training by providing an objective measurement of a professional's knowledge and skills. Certificate programs establish standards for IPv6 courses and play important role developing a qualified workforce. Some of the certification programs that are available that can be considered are:

MCMC MTSFB TC TXXX:2015

- a) Fundamental IPv6;
- b) IPv6 Certified Engineer;
- c) IPv6 Certified Security Engineer; and
- d) IPv6 System Administrator.

8.1.3 Information Sharing

A local data-sharing portal for organizations may be established to obtain all relevant information pertaining to IPv6. This includes case studies, experiences from other organizations, overcoming challenges and others information.

8.1.4 Resources

There are multiple sources of information regarding IPv6, each catering to one of the categories mentioned above. Some resources are free to those who are interested in a self-study approach or are just starting to get familiar with IPv6.

Integrators or consulting groups, such as Command Information, often have IPv6 training, consulting practices and “jump-start” services that can be very valuable in helping an organization achieve a solid level of competence in IPv6.

Vendors are another source of IPv6 training that is both generic and specific to its implementation in their product line.

Following are some of the references to obtain resources related to IPv6:

- a) Internet Engineering Task Force (IETF), www.ietf.org – This organization provides all the technical specification (request for comment) for various technologies including IPv6. There are many working groups specifically working on IPv6.
- b) Asia Pacific Network Information Centre (APNIC), www.apnic.net – This is an open, membership-based, not-for-profit organization providing internet addressing services to the Asia Pacific. The site has comprehensive information available from getting IPv6 addresses to deploying it.
- c) IPv6 Observatory, <http://www.ipv6observatory.eu/>.
- d) 6Now, <http://ipv6now.com.au/>.

9. Summary

It is important that early, comprehensive planning is essential for cost-effective and seamless implementation of IPv6. Even though there are many resources available that presents technical aspects of IPv6 with great length, this document compiles some of these technical aspects of IPv6 with the intention to provide a guideline for individuals and organizations who want to know about IPv6 and its implementation.

Annex A (Normative)

Abbreviations

3G	Third Generation
ACL	Access Control List
AFRINIC	Africa and the Indian Information Centre
AH	Authentication Header
ALG	Application Layer Gateway
APNIC	Asia Pacific Network Information Centre
ARP	Address Resolution Protocol
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol Version 6
DNS	Domain Name System
DNSv6	Domain Name System version 6
EUI	Extended Unique Identifier
FTP	File Transfer Protocol
GRE	Generic routing encapsulation
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICMP	Internet Message Control Protocol
ICMPv6	Internet Message Control Protocol Version 6
ID	Identifier
IDPS	Intrusion Detection and Prevention System
IDS	Integrated Delivery Systems
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPAM	IP Address Management
IPFIX	Internet Protocol Flow Information Export
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISPs	Internet Service Providers
IT	Information Technology
IXP	Internet Exchange Points
LACNIC	Latin America and the Caribbean Network Information Centre
LAN	Local Area Network
LIR	Local Internet Registries
LTE	Long Term Evolution
MIBs	Management Information Base
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NMS	Network Management System
NTP	Network Time Protocol
NTPv6	Network Time Protocol version 6

OPsec	Operations Security
PI	Provider Independent
PPP	Point-to-Point Protocol
PT	Protocol Translation
PTPv6	Point-to-Point version 6
QOS	Quality of Service
RFC	Request for Comments
RIR	Regional Internet Registry
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol (TFTP)
TLD	Top Level Domain
VLANs	Virtual Local Area Network

Annex B
(Normative)

Sample ISP Requirements Checklist

	Mandatory	Optional	Require 1. Software upgrades 2. Hardware upgrades 3. New hardware	Recommendation/ N/A
User End:				
UE (Phone, Device, CPE)	√			
Terminal	√			
Access Layer:				
Fixed,		√		
Mobile(3G, LTE),		√		
Wifi	√			
IP Core Network:				
Routers,	√			
Switches,	√			
Firewalls	√			
Core Network:				
NGN,	√			
Servers & Application	√			
Database,		√		
DNS	√			
NTP	√			
DHCP	√			
Packet Core	√			
Charging, billing and provisioning	√			
Network Monitoring and Management		√		
International and Domestic Gateway:				
Transit	√			
Peering	√			
IP Security:				
IPSec Tunneling	√			

Annex C
(Normative)

IETF Request for Comments (RFC)

No	RFC	List of RFC
1	RFC 1752	The Recommendation for the IP Next Generation Protocol
2	RFC 1981	Path MTU Discovery for IPv6
3	RFC 1883	Internet Protocol, Version 6 (IPv6) Specification
4	RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
5	RFC 3022	Traditional IP Network Address Translator (Traditional NAT)
6	RFC 3053	IPv6 Tunnel Broker
7	RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
8	RFC 3177	IAB/IESG Recommendations on IPv6 Address Allocations to Sites
9	RFC 3344	IP Mobility Support for IPv4
10	RFC 3531	A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block
11	RFC 3775	Mobility Support in IPv6
12	RFC 4057	IPv6 Enterprise Network Scenarios
13	RFC 4192	Procedures for Renumbering an IPv6 Network without a Flag Day
14	RFC 4193	Unique Local IPv6 Unicast Address
15	RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
16	RFC 4291	IPv6 Addressing Architecture
17	RFC 4293	Management Information Base for the Internet Protocol (IP)
18	RFC 4449	Securing Mobile IPv6 Route Optimization Using a Static Shared Key
19	RFC 4554	Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks
20	RFC 4632	Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
21	RFC 4852	IPv6 Enterprise Network Analysis – IP Layer 3 Focus
22	RFC 4861	Neighbour Discovery for IPv6 version 6 (IPv6)
23	RFC 4862	IPv6 Stateless Address Autoconfiguration
24	RFC 4942	IPv6 Transition/Coexistence Security Considerations
25	RFC 5157	IPv6 Implications for Network Scanning
26	RFC 5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
27	RFC 5887	Renumbering Still Needs Work
28	RFC 6052	IPv6 Addressing of IPv4/IPv6 Translators
29	RFC 7012	Information Model for IP Flow Information Export (IPFIX)
30	RFC 7381	Enterprise IPv6 Deployment

MCMC MTSFB TC TXXX:2015

Acknowledgements

Members of the IPv6 Working Group

Dr. Gopinath Rao Sinniah (Chairman)	REDtone IoT Sdn Bhd
Mr. Zaharin Mohd Nadzri (Vice Chairman)	Celcom Axiata Berhad
Ms. Azura Mat Salim (Secretary)	Telekom Malaysia Berhad
Mr. Azmi Salim	Asian Broadcasting Networks (M) Sdn Bhd (ABNxcess)
Mr. Wan Salman Yahya	Celcom Axiata Berhad
Mr. Yan Kim Fui	Cisco Systems Malaysia
Mr. Fami Abdul Hamid	DiGi Telecommunications Sdn Bhd
Mr. Wenke (Kevin)	Huawei Technologies
Mr. Nasrul Hafiz Shaharudin	Jaring Communications Sdn Bhd
Mr. Zulkarnain Zainal	Maxis Broadband Sdn. Bhd
Mr. Adil Hidayat	My6 Initiative Berhad
Ms. Cheok Meng Hui /	Packet One Networks (Malaysia) Sdn Bhd
Mr. Khor Wei Li	
Mr. Junaedy bin Jamaludin	Telekom Malaysia Berhad
Mr. Victor Ong Wai Kit	TIME dotCom Bhd
Ms. Tee Leh Pheng	UMobile Sdn Bhd