UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)
JABATAN PERDANA MENTERI
ARAS 6, BLOK B2
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN
62502 PUTRAJAYA

Telefon : 03-88723000
Faks : 03-88883721
Laman Web : www.mampu.gov.my

MAMPU.BDPICT -7/22 (23)

04 Januari 2010

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Badan Berkanun Persekutuan
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Tempatan

YBhg./YB Tan Sri/Datuk/Dato'/Tuan/Puan,

GARIS PANDUAN TRANSISI PROTOKOL INTERNET VERSI 6 (IPV6) SEKTOR AWAM

Dengan hormatnya saya merujuk perkara di atas.

2. Untuk makluman YBhg./YB Tan Sri/Datuk/Dato'/Tuan/Puan, dunia hari ini sedang membuat persediaan untuk peralihan penggunaan Protokol Internet versi 4 (IPv4) kepada Protokol Internet versi 6 (IPv6) dalam jaringan internet global. Sehubungan dengan itu, agensi Sektor Awam hendaklah memastikan kesediaan untuk beralih kepada teknologi yang menggunakan IPv6 dalam rangkaian masing-masing bagi memastikan kesinambungan penyampaian perkhidmatan menerusi rangkaian internet.

3. Semua Ketua Jabatan adalah dipohon untuk mengambil tindakan berikut:

(a) Memastikan perolehan semua perkakasan baru atau peningkatan perkakasan sedia ada menepati ciri IPv6 (IPv6 *compliance*); dan
(b) Memastikan pembangunan sistem aplikasi baru atau peningkatan aplikasi sedia ada dinaiktarafkan supaya menepati ciri IPv6 (IPv6 *compliance*).

4. Maklumat lanjut mengenai panduan pelaksanaan peralihan IPv6 boleh diperolehi dari **"Garis Panduan Transisi IPv6 Sektor Awam"** seperti yang dilampirkan. Garis panduan ini bertujuan untuk menerangkan kaedah transisi IPv6 secara umum sebagai panduan bagi setiap agensi Sektor Awam dalam pelaksanaan peralihan IPv4 kepada IPv6. Sehubungan dengan itu, YBhg./YB Tan Sri/Datuk/Dato'/Tuan/Puan adalah dipohon untuk mengambil tindakan sewajarnya agar garis panduan ini dipatuhi, dilaksanakan dan dipantau sepenuhnya dengan berkesan.

Sekian, terima kasih.

"BERSAMA MELAKSANA TRANSFORMASI'

"BERKHIDMAT UNTUK NEGARA"

Saya yang menurut perintah,

(DATUK NORMAH BINTI MD. YUSOF)

s.k.

YBhg. Tan Sri Mohd Sidek Hj Hassan
Ketua Setiausaha Negara
Pejabat Ketua Setiausaha Negara
Aras 4, Blok Timur
Bangunan Perdana Putra
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA

(Lampiran kepada

Surat Arahan Ketua Pengarah MAMPU)

Rujukan MAMPU : MAMPU.BDPICT.700-2/22 (23)

Garis Panduan

Transisi IPv6 Sektor Awam

Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)

Jabatan Perdana Menteri

Kandungan

Lampiran

Senarai Rajah

Ringkasan Eksekutif

Ringkasan Eksekutif

Internet memainkan peranan penting dalam menjalankan perniagaan dan proses komunikasi harian. Protokol Internet versi 4 (IPv4) merupakan protokol yang digunakan secara meluas untuk memudahkan komunikasi antara makmal penyelidikan dan bahagian-bahagian kecil di universiti dan agensi-agensi Sektor Awam. Walau bagaimanapun, protokol yang berusia 30 tahun tidak direka khas untuk penggunaan telefon bimbit, Pembantu Peribadi Digital (PDA) dan Identifikasi berdasarkan Radio Frekuensi (RFID) di mana alamat 32-bit IPv4 yang terhad adalah penghalang kepada pertambahan capaian ke peranti dan aplikasi internet yang baru. Alamat IPv4 dari segi teori terhad kepada 4.3 bilion alamat di mana kurang daripada populasi penduduk dunia, dan tidak mengambil kira pertambahan penduduk dan pertumbuhan Internet. Kemunculan Protokol Internet versi 6 (IPv6) adalah satu keperluan kepada perkembangan Internet dan pembangunan aplikasi melalui sambungan Internet mudah alih. IPv6 adalah satu penyelesaian jangka panjang dalam menangani kekurangan IPv4.

Terdapat beberapa isu yang perlu dikenal pasti dan diketengahkan semasa proses transisi IPv6 di agensi-agensi Sektor Awam. Perkara pertama yang perlu diberi perhatian semasa melaksanakan transisi kepada IPv6 adalah pelaksanaan ini tidak akan menyebabkan sebarang gangguan terhadap rangkaian dan operasi harian agensi. Kedua, keselamatan juga merupakan perkara penting dalam komunikasi rangkaian Sektor Awam di mana keselamatan rangkaian harus dititik beratkan semasa proses transisi. Perkara lain yang perlu dipertimbangkan semasa transisi ialah kos yang diperlukan, keperluan, impak keselamatan, risiko dan isu-isu lain. Bagi mengetengahkan kekangan dan menyediakan maklumat berkaitan proses transisi IPv6, satu (1) garis panduan perlu disediakan bagi tujuan ini.

Agensi Sektor Awam harus bersedia dengan infrastuktur yang menyokong teknologi IPv6 bagi memastikan kesinambungan rangkaian agensi masing-masing. Pelbagai

pertimbangan perlu diambil kira apabila memperkenalkan suatu teknologi kepada infrastruktur sesebuah agensi. Oleh itu proses transisi harus dilakukan secara berhati-hati dan terkawal, memahami dan mengenal pasti faedah-faedah serta cabaran dalam setiap teknik-teknik pelaksanaan IPv6. Dokumen ini menyatakan faedah dan cabaran serta memberikan kaedah pelaksanaan terbaik yang dapat digunakan untuk membolehkan agensi merancang proses transisi IPv6 bagi infrastruktur *Information and Communication Technology* (ICT) di agensi masing-masing.

Bab 1

Pengenalan

Bab 1: Pengenalan

1. Latar belakang

1.1 Malaysia menyedari bahawa IPv6 mampu memberikan sumbangan yang besar bagi memenuhi visi negara untuk menjadi hub ICT dan Multimedia. Selaras itu, bagi memastikan Malaysia tidak ketinggalan dalam pelaksanaan IPv6, Kementerian Tenaga, Air dan Komunikasi menubuhkan Majlis IPv6 Kebangsaan pada 2004 untuk menerajui dan merancang pelaksanaan IPv6 di Malaysia. Majlis IPv6 Kebangsaan Malaysia telah bermesyuarat pada 28 Disember 2004 dan menetapkan sasaran untuk menjadikan Malaysia sebuah negara tersedia IPv6 (IPv6 *ready*) pada akhir tahun 2010.

1.2 Di samping itu, IPv6 merupakan salah satu elemen strategi *blueprint* MyICMS 886 (*Malaysia Information, Communication and Multimedia Services* 886) dan juga merupakan salah satu bidang fokus dalam Rancangan Malaysia Kesembilan.

1.3 Selain memenuhi mandat Kerajaan untuk transisi IPv6, ianya juga memberi faedah dalam aspek teknikal dan komersial. Sebagai contoh, IPv6 dapat menghapuskan penggunaan *Network Address Translator* (NAT) dalam infrastruktur rangkaian organisasi bagi memudahkan operasi ICT. Ciri-ciri *encryption* dan *authentication* yang terdapat dalam IPv6 amat penting dan berguna dalam infrastruktur ICT Sektor Awam. Agensi juga dapat menggunakan sepenuhnya faedah IPv6 dalam mengukuhkan keselamatan rangkaian dan memudahkan pengurusan infrastruktur.

1.4 Garis panduan ini bertujuan untuk menyediakan panduan serta rujukan bagi membantu agensi bagi melaksanakan proses transisi IPv6. Menerusi

garis panduan ini, perancangan proses transisi dapat dibuat bagi mengenal pasti isu seperti peruntukan kewangan, keperluan transisi, impak keselamatan, risiko yang terlibat, teknik pelaksanaan dan isu-isu lain. Dalam erti kata lain, satu pelan transisi yang lengkap akan dapat memberikan maklumat bagi keseluruhan proses untuk mengurangkan kesilapan dan kelewatan semasa proses transisi.

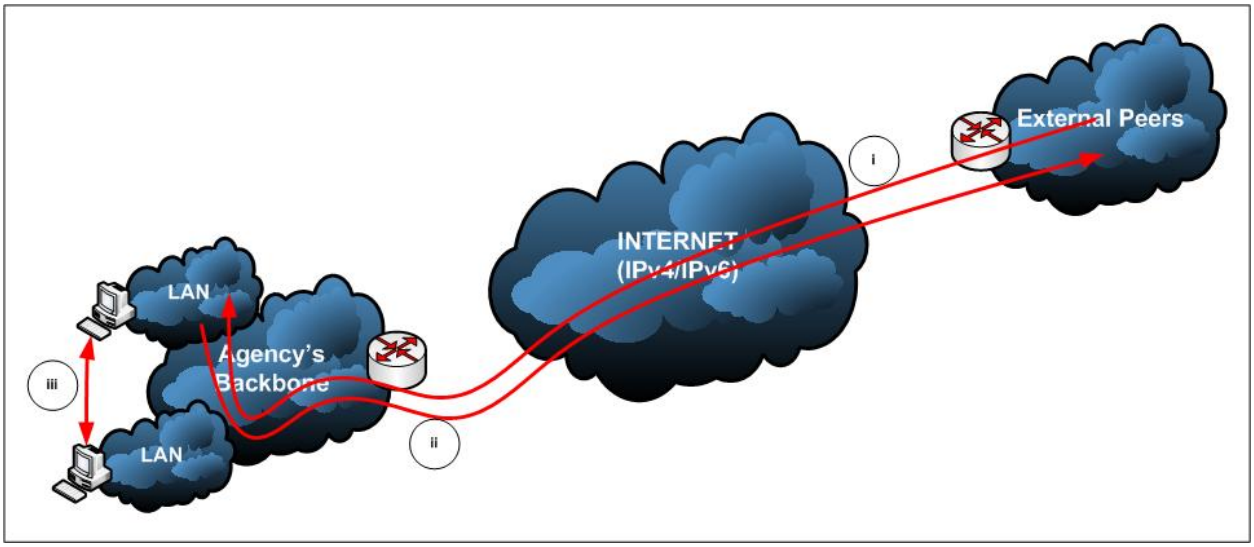
1.5 Rangkaian agensi adalah tersedia IPv6 sekiranya rangkaian persekitaran IPv4 sedia ada dapat melaksanakan perkara-perkara berikut:

(a) Menerima data IPv6 dari Internet dan jaringan luaran melalui rangkaian tulang belakang *(network backbone)* kepada *Local Area Network* (LAN);

(b) Menghantar data IPv6 melalui rangkaian tulang belakang (*network backbone*) keluar ke Internet dan jaringan luar dan sebaliknya; dan

(c) Menghantar data IPv6 daripada LAN terus ke rangkaian tulang belakang *(network backbone*) ke LAN yang lain (atau nod pada LAN yang sama).

Rajah 1-1 Keperluan Sambungan IPv6



2. Objektif

2.1 Tujuan utama dokumen ini adalah untuk menerangkan kaedah transisi IPv6 secara umum sebagai panduan bagi agensi Sektor Awam di Malaysia.

2.2 Objektif garis panduan transisi ini adalah seperti berikut:

(a) Menerangkan kaedah penggunaan teknologi IPv4 dan IPv6 secara bersama;

(b) Menerangkan teknik atau kombinasi teknik-teknik yang terlibat dalam melaksanakan transisi IPv6;

(c) Mengenal pasti risiko keselamatan rangkaian semasa proses transisi;

(d) Menyatakan isu yang bakal dihadapi atau *stress factor* (peruntukan kewangan, kemahiran personel dan dasar) semasa proses transisi; dan

(e) Memastikan pelaksanaan IPv6 memberi kesan paling minimum terhadap operasi rangkaian sedia ada.

2.3 Setiap agensi adalah bertanggungjawab untuk membangunkan pelan transisi yang merangkumi perkara-perkara berikut:

(a) Menyediakan analisis terperinci bagi pengurusan dan penilaian risiko;

(b) Memastikan perancangan transisi dibuat secara berskala;

(c) Menyatakan anggaran peruntukan kewangan yang diperlukan bagi melaksanakan proses transisi IPv6;

(d) Mengenal pasti aplikasi, perisian atau perkakasan yang perlu diganti atau dinaiktarafkan;

(e) Mengenal pasti kesan transisi IPv6 pada perkakasan, perisian dan aplikasi sedia ada; dan

(f) Membuat agihan keperluan sumber untuk pelan transisi.

2.4 Agensi perlu melengkapkan senarai semak seperti di dalam **Lampiran E** dan **Lampiran F**. Satu (1) salinan senarai semak perlu dikemukakan kepada Kumpulan Kerja IPv6 (Maklumat lanjut mengenai Kumpulan Kerja IPv6 seperti dijelaskan dalam Bab 3) untuk semakan.

3. Organisasi Dokumen

3.1 Dokumen ini mengandungi empat (4) bab iaitu Pengenalan, Pendahuluan Berkaitan IPv6, Struktur Tadbir Urus Pelaksanaan IPv6, dan Pelaksanaan IPv6.

3.2 Dalam Bab Satu (1) **Pengenalan** menerangkan latar belakang dan objektif dalam pelaksanaan transisi IPv6 di Sektor Awam.

3.3 Bab Dua (2) **Pendahuluan berkaitan IPv6** menerangkan latar belakang dan kemunculan IPv6, penjelasan ciri, faedah-faedah dan cabaran dalam memperkenalkan IPv6 ke dalam persekitaran rangkaian.

3.4 Bab Tiga (3) **Struktur Tadbir Urus Pelaksanaan IPv6** menerangkan struktur tadbir urus yang menyokong proses transisi IPv4 kepada IPv6.

3.5 Bab Empat (4) **Pelaksanaan IPv6** menerangkan fasa-fasa yang terlibat dalam melaksanakan transisi IPv4 ke IPv6 ke jaringan agensi Sektor Awam.

Bab 2

Pendahuluan berkaitan IPv6

Bab 2: Pendahuluan Berkaitan IPv6

4. Kajian terhadap IPv6

4.1 Penggunaan Internet sebagai satu teknologi asas untuk kegiatan komersial dan sosial lebih meluas sejak penciptaan **laman sesawang** *(World Wide Web)* pada awal tahun 90-an. Selepas itu, Internet telah berkembang dengan pesatnya dalam jangka masa lima (5) tahun, bagi skala yang lebih besar daripada apa yang digambarkan oleh pereka Internet 20 tahun yang lalu.

4.2 IPv4 telah dibangunkan dalam tahun 1970 dan menyediakan asas untuk Internet pada masa kini. Selari dengan pertambahan jumlah fungsi dan pengguna Internet, IPv6 telah muncul sebagai protokol generasi berikutnya bagi Internet dalam memenuhi keperluan semasa.

4.3 Ruang alamat IPv4 sedia ada adalah tidak mencukupi dalam memenuhi penggunaan Internet yang meluas dalam penggunaan peranti *Internet-enable* tanpa wayar, peralatan industri dan peralatan elektronik yang digunakan di rumah, pengangkutan yang mempunyai sambungan Internet, perkhidmatan telefoni bersepadu, pengkomputeran teragih dan permainan komputer. Ruang alamat IPv4 adalah sebesar 2^{32} (4,294,967,296) alamat unik manakala ruang alamat IPv6 adalah 2^{128} (*octillions*) alamat unik.

4.4 Disebabkan ruang alamat global IPv4 yang tidak mencukupi, IPv4 telah diperluaskan dengan menggunakan teknik-teknik tertentu seperti NAT.

Walaupun teknik ini dapat meningkatkan ruang alamat IPv4 namun ia gagal memenuhi keperluan semasa. Selain daripada menambah alamat IP, IPv6 juga mempunyai kelebihan lain seperti keselamatan *end-to-end* dan *Quality of Service* (QOS) yang tidak terdapat dalam rangkaian yang menggunakan NAT.

4.5 Transisi rangkaian Internet global daripada IPv4 ke IPv6 mengambil masa selama beberapa tahun. Dalam tempoh transisi ini, organisasi mula mengaplikasikan IPv6 dalam infrastruktur rangkaian sedia ada di samping menggunakan IPv6 bersama IPv4.

4.6 Tiada kaedah khusus yang boleh digunakan dalam transisi dan strategi pelaksanaan IPv6. Untuk itu proses transisi kepada IPv6 haruslah dilakukan secara berperingkat yang memberikan masa untuk melakukan penyesuaian seterusnya untuk membolehkan IPv4 dan IPv6 digunakan serentak. Maklumat lanjut berhubung kaedah transisi IPv4 ke IPv6 boleh didapati di dalam **Lampiran B.**

5. Ciri-ciri dan Faedah IPv6

5.1 IPv6 telah direka berdasarkan ciri-ciri IPv4 dan menyediakan perkhidmatan dan keupayaan baru. Evolusi protokol IPv6 adalah hasil cadangan dan usaha *Internet Engineering Task Force* (IETF). Beberapa ciri dan faedah IPv6 adalah seperti berikut:

(a) Format *header* Yang Baru

Header IPv6 telah direkabentuk bagi meminimumkan pemprosesan *header*. IPv6 adalah lebih efisien apabila diproses oleh *router*. Walaubagaimanapun, *header* IPv4 dan IPv6 adalah tidak *interoperable*. Hos atau *router* perlu menyokong kedua-dua protokol IPv4 dan IPv6 untuk membolehkannya mengenali dan memproses format *header* protokol-protokol tersebut. Walaupun jumlah bit alamat IPv6 adalah empat (4) kali lebih besar daripada alamat IPv4, *header* IPv6 hanya dua (2) kali lebih besar daripada *header* IPv4. Sila rujuk **Lampiran A** untuk perbezaan IPv4 dan IPv6.

(b) Ruang Alamat yang Lebih Besar

Saiz alamat IPv6 adalah 128 bit (16 bait) menghasilkan alamat IP yang banyak serta mencukupi. Dengan itu, penggunaan NAT tidak lagi diperlukan.

(c) Konfigurasi alamat *Stateless* dan *Stateful*

IPv6 mempunyai keupayaan pengalamatan *stateful* (seperti pemberian alamat menggunakan pelayan DHCPv6[1]) dan pengalamatan *Stateless*[2] (seperti pemberian alamat dalam ketiadaan pelayan DHCPv6), yang bertujuan untuk memudahkan konfigurasi pengalamatan IP. Dengan penggunaan konfigurasi

[1] RFC315 – Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

[2] RFC2462 – IPv6 Stateless Address Auto configuration

alamat *stateless*, setiap hos secara automatik akan dapat melakukan konfigurasi untuk alamat sendiri dengan menggunakan alamat IP *link-local*[3] yang akan membolehkan mereka berkomunikasi antara satu sama lain walaupun dengan ketiadaan *router* dan tanpa konfigurasi manual.

(d) Pengenalan *Neighbour Discovery Protocol* (NDP)

***Neighbour Discovery Protocol* (NDP)** dalam IPv6 adalah siri mesej *Internet Control Message Protocol* untuk IPv6 (ICMPv6[4]) iaitu mesej yang digunakan untuk menguruskan interaksi antara nod-nod jiran (nod yang berada pada jalinan rangkaian sama). NDP menggantikan *Address Resolution Protocol* (ARP), ICMP untuk IPv4 (ICMPv4) *Router Discovery* dan ICMPv4 *Redirect massages.*

(e) IPv6 mempunyai fungsi *routing* yang lebih cekap

IPv6 adalah versi generasi baru IPv4 yang mempunyai saiz *header* yang tetap iaitu 40 bait, ini akan membolehkan *router* memproses paket dengan lebih cepat. Selain itu, jenis pengalamatan berperingkat dan perumusan struktur alamat global IPv6 akan mengurangkan jumlah laluan rangkaian yang perlu diproses oleh *router*.

[3] Link-local addresses only refer only to a particular physical link (physical network). Routers will not forward datagram's using link-local addresses at all, not even within the organization

[4] RFC2463 – *Internet Control Message Protocol (ICMPv6)* untuk spesifikasi IPv6

(f) IPv6 Menyokong Ciri Keselamatan dan Mobiliti

IPv6 telah direka bentuk bagi menyokong keselamatan *IPsec* (*Authentication Header* dan *Encapsulated Security Payload header)* dan IPv6 mudah alih. Rekabentuk ini akan memastikan IPv6 dapat memenuhi keperluan pengguna internet secara berterusan. Manfaat penggunaan *IPsec* akan dapat dilihat daripada keupayaannya untuk melindungi paket sepanjang proses penghantaran dalam rangkaian internet.

Bab 3

Strukur Tadbir Urus Pelaksanaan IPv6

Bab 3: Struktur Tadbir Urus Pelaksanaan IPv6

6. Pendahuluan

6.1. Pelaksanaan IPv6 akan menjadi keperluan asas bagi kesinambungan sistem rangkaian digital dalam tempoh terdekat. Bagi memastikan kelancaran transisi dan pemakaian IPv6 dalam rangkaian ICT Sektor Awam, beberapa perkara asas perlu dipertimbangkan. Aspek terpenting adalah tadbir urus.

7. Struktur Tadbir Urus Pelaksanaan IPv6 Sektor Awam

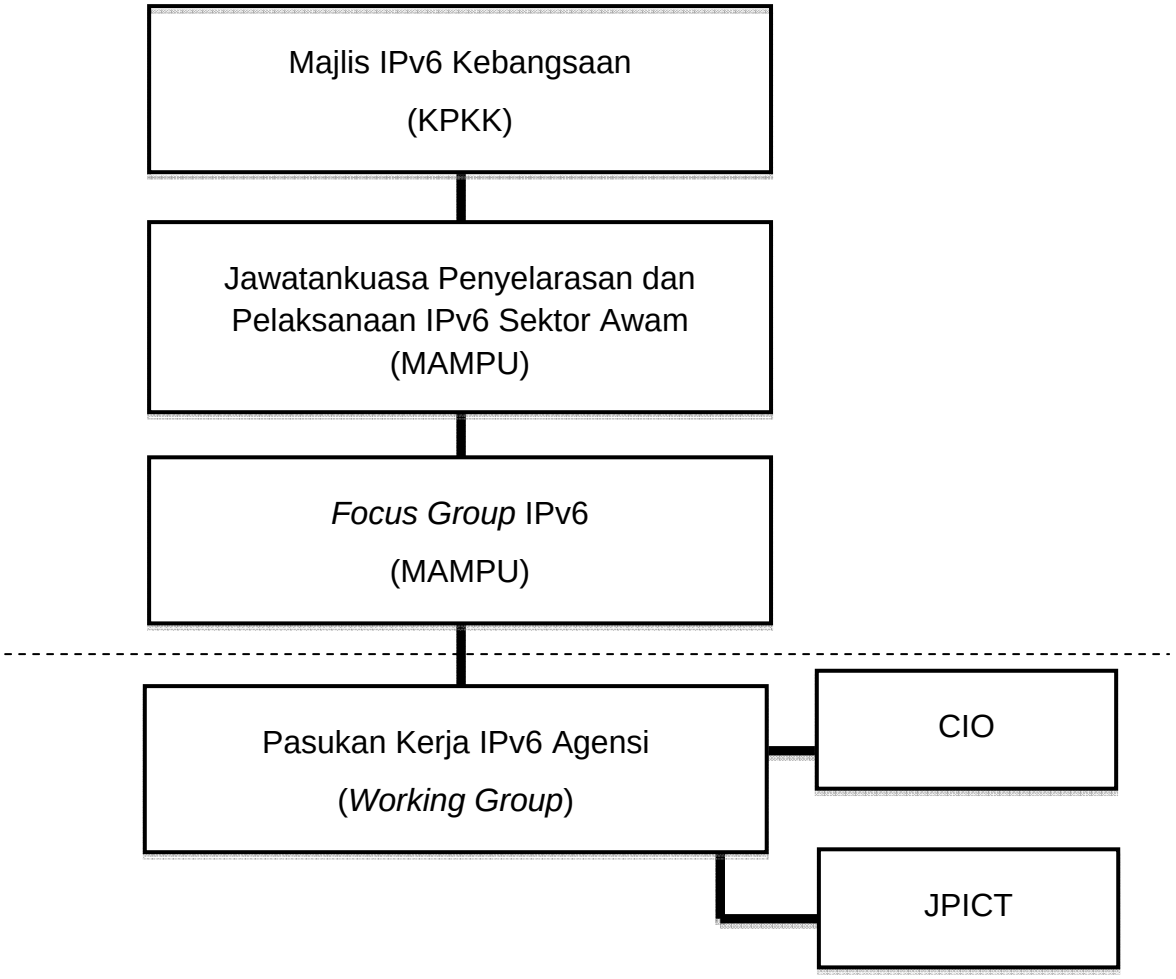
7.1. Pelaksanaan IPv6 akan melibatkan pelbagai pihak yang terdiri daripada agensi Sektor Awam, pembangun kandungan digital, pembangun perisian, pembekal ICT dan penyedia perkhidmatan internet. Peranan semua pihak yang terlibat perlu ditentukan bagi memastikan tanggungjawab perlu dilaksanakan untuk kelancaran pelaksanaan IPv6 dalam Sektor Awam.

7.2. Perancangan dan pelaksanaan transisi IPv6 dalam Sektor Awam memerlukan kerjasama dari semua pihak yang terlibat.

7.3. Setiap agensi perlu membangunkan dan melaksanakan satu pelan transisi IPv4 kepada IPv6 (Sila rujuk perenggan 2.3).

7.4. **Rajah 3-1** menunjukkan struktur tadbir urus pemantauan pelaksanaan IPv6.

Rajah 3-1 Struktur Tadbir Urus Pelaksanaan IPv6 Peringkat Kebangsaan



7.5. Kementerian dan agensi Sektor Awam yang terlibat dalam pelaksanaan IPv6 adalah seperti berikut:

(a) **Kementerian Penerangan, Komunikasi dan Kebudayaan (KPKK)**

KPKK[5] adalah peneraju utama dalam agenda IPv6 Kebangsaan. Kementerian ini bertanggungjawab dalam menyelaras pelaksanaan IPv6 di Malaysia menerusi dua (2) entiti penting seperti berikut:

[5] Pada 9 April 2009, Perdana Menteri telah mengumumkan Kementerian Tenaga, Air dan Komunikasi (KTAK) distruktur semula sebagai Kementerian Tenaga, Teknologi Hijau dan Air (KeTTHA). Bahagian Komunikasi telah dipindahkan ke Kementerian Penerangan, Komunikasi dan Kebudayaan.

(i) Majlis IPv6 Kebangsaan; dan

(ii) Pusat Termaju Negara IPv6 (NAv6).

(b) **Majlis IPv6 Kebangsaan**

Peranan Majlis IPv6 Kebangsaan adalah untuk menyediakan hala tuju nasional dalam menggerakkan agenda IPv6 di Malaysia. Ini melibatkan penetapan visi, misi dan perancangan strategik untuk pelaksanaan IPv6 di peringkat nasional.

(c) **Pusat IPv6 Termaju Negara (NAv6)**

(i) NAv6 ditubuhkan berdasarkan cadangan oleh Majlis IPv6 Kebangsaan dan bertindak sebagai pusat rujukan IPv6 di Malaysia. NAv6 menyediakan kepakaran dalam bidang teknikal, pentadbiran dan perundangan berkaitan IPv6. NAv6 juga berperanan dalam aktiviti-aktiviti berikut:

a. Penyelidikan dan Pembangunan (R&D);

b. Pembangunan Sumber Manusia;

c. Audit dan Pemantauan; dan

d. Promosi dan Kesedaran.

(ii) Bagi melaksanakan aktiviti-aktiviti tersebut, NAv6 akan bekerjasama dengan beberapa agensi Sektor Awam seperti berikut:

a. Kementerian Sains, Teknologi dan Inovasi (MOSTI) dalam bidang penyelidikan dan pembiayaan pembangunan;

b. Kementerian Pengajian Tinggi (MOHE) dalam bidang pembangunan sumber manusia;

c. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) bagi memastikan semua agensi Sektor Awam mematuhi jadual pelaksanaan IPv6 yang ditetapkan oleh Majlis IPv6 Kebangsaan; dan

d. Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) bagi memastikan penyedia perkhidmatan internet (ISP) di negara ini adalah IPv6 *ready* mengikut perancangan yang ditetapkan.

(d) **Kementerian Sains, Teknologi dan Inovasi (MOSTI)**

MOSTI bertanggungjawab untuk menyediakan hala tuju Penyelidikan dan Pembangunan (R&D) dan juga telah diberi mandat untuk penghasilan kandungan (Pembangunan ICT dan multimedia) yang merangkumi teknologi IPv6.

(e) **Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM)**

(i) SKMM adalah badan kawal selia untuk komunikasi dan industri multimedia. Peranannya adalah termasuk dalam memantau perkhidmatan Internet oleh ISP.

(ii) Pada tahun 2006, SKMM telah mengenal pasti IPv6 sebagai sebahagian daripada prasarana dalam strategi MyICMS 886. Sehubungan itu, SKMM akan memastikan bahawa

semua ISP adalah IPv6 *ready* seperti yang dinyatakan dalam strategi tersebut.

(iii) SKMM melalui badan industri sukarela, memainkan peranan penting dalam penerimaan IPv6 di Malaysia, kerana ia memainkan peranan sebagai badan kawal selia pada semua peringkat. Sebagai usaha untuk mempromosikan teknologi baru, SKMM akan mempelopori skim intensif yang akan mendorong industri dalam menggunakan teknologi-teknologi baru seperti IPv6.

(iv) SKMM adalah bertanggungjawab dalam merangka garis panduan dan dasar-dasar kepada ISP serta terlibat secara lansung dalam pensijilan IPv6. Komitmen SKMM dalam IPv6 boleh dilihat menerusi penyertaan aktifnya dalam perbincangan yang dijalankan oleh pihak industri dan usahanya dalam mendapatkan maklum balas daripada industri mengenai penerimaan IPv6.

(f) **Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)**

(i) MAMPU berperanan dalam memastikan semua agensi Sektor Awam mematuhi tempoh jangkamasa pelaksanaan IPv6 yang telah ditetapkan oleh Majlis IPv6 Kebangsaan di mana semua agensi Sektor Awam harus menjadi IPv6 *ready* bermula pada tahun 2008.

(ii) MAMPU memainkan peranan penting dalam melaksanakan dasar-dasar yang telah ditetapkan oleh Majlis IPv6 Kebangsaan. MAMPU juga akan menentukan perubahan

infrastruktur yang diperlukan untuk membolehkan IPv6 digunakan dalam insfrastruktur rangkaian e-Kerajaan.

(iii) MAMPU akan menyediakan garis panduan dalam pelan transisi dan pelaksanaan IPv6 dalam rangkaian Sektor Awam.

(b) Kementerian dan Agensi yang lain

(i) Membangunkan dan melaksanakan pelan transisi agensi berdasarkan pelan transisi yang telah dibangunkan oleh pihak bertanggungjawab. (Sila rujuk perenggan 2.3)

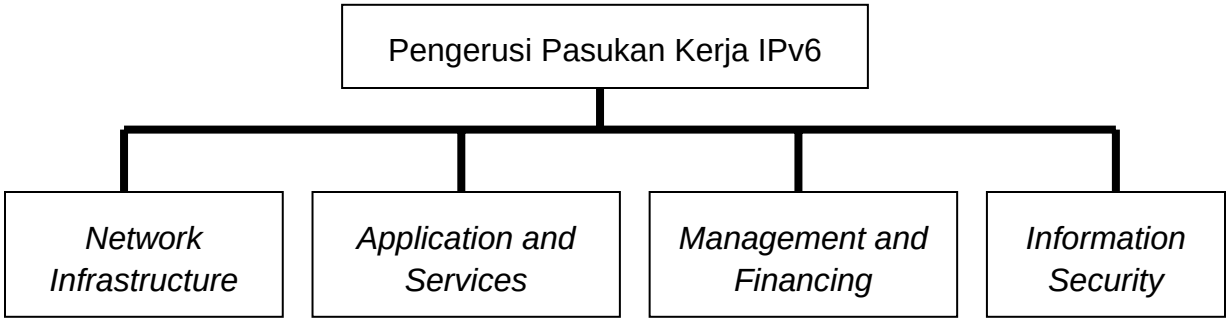
8. Struktur Tadbir Urus di Peringkat Agensi

8.1 Struktur tadbir urus perlu diwujudkan bagi memastikan pelaksanaan agenda IPv6 berjalan dengan lancar. Setiap agensi dikehendaki untuk menubuhkan Pasukan Kerja IPv6 yang diterajui oleh Pengurus ICT Agensi.

8.2 Ahli-ahli pasukan kerja tersebut terdiri daripada wakil-wakil dari bidang fungsi utama iaitu infrastruktur rangkaian, perkhidmatan pembangunan aplikasi, keselamatan maklumat dan khidmat pengurusan kewangan.

8.3 Ketua Pegawai Maklumat (CIO) perlu memantau dan memastikan pelaksanaan transisi IPv6 agensi dilaksanakan dengan lancar. Struktur Pasukan Kerja IPv6 adalah seperti di **Rajah 3-2**.

Rajah 3-2 Cadangan Struktur Tadbir Urus Peringkat Agensi



8.4 Pasukan Kerja IPv6 bertanggungjawab memastikan pelaksanaan transisi IPv6 dibuat mengikut jadual pelaksanaan yang telah ditetapkan. Bagi menjayakan pelaksanaan IPv6 setiap agensi, terma rujukan Pasukan Kerja IPv6 juga perlu disediakan. Terma Rujukan Pasukan Kerja IPv6 adalah seperti berikut:

(a) Mengenal pasti aset-aset ICT yang terlibat dalam proses transisi IPv6;

(b) Mengenal pasti keperluan dan kepakaran sumber manusia;

(c) Merancang dan menyediakan pelan transisi;

(d) Mendapatkan kelulusan pelaksanaan yang melibatkan sumber-sumber dari pihak pengurusan (CIO dan Jawatnkuasa Pemandu ICT (JPICT));

(e) Melaksanakan pelan transisi; dan

(f) Melaporkan status pelaksanaan kepada CIO, JPICT dan Pasukan *Focus Group* IPv6 MAMPU.

Bab 4

Pelaksanaan IPv6

Bab 4: Pelaksanaan IPv6

9. Pendahuluan

9.1 Pelaksanaan IPv6 akan dibahagikan kepada tiga (3) fasa utama. Pelaksanaan secara berfasa ini adalah untuk memudahkan pengurusan dan penyelesaian kepada masalah yang mungkin timbul. Objektif setiap fasa adalah seperti berikut:

(a) **Fasa 1:** Memastikan ibu pejabat agensi berkeupayaan menyokong IPv6 dan mempunyai sambungan global yang selamat.

(b) **Fasa 2:** Memastikan pejabat cawangan berkeupayaan menyokong IPv6 dan mempunyai sambungan global yang selamat.

(c) **Fasa 3:** Memastikan migrasi aplikasi utama agensi supaya berkeupayaan menggunakan ciri-ciri IPv6 secara maksimum.

10. Fasa 1

10.1 Objektif fasa 1 adalah untuk memastikan ibu pejabat agensi berkeupayaan menyokong IPv6 dan mempunyai sambungan global yang selamat. Bagi mencapai objektif ini, perkara-perkara berikut perlu dilaksanakan:

(a) Merancang belanjawan, seni bina rangkaian dan perkara-perkara lain yang berkaitan;

(b) Mewujudkan persekitaran simulasi;

(c) Melaksanakan audit pematuhan dan audit keselamatan secara komprehensif;

(d) Menyediakan beberapa aplikasi untuk memanfaatkan IPv6; dan

(e) Menilai pelaksanaan yang telah dijalankan.

10.2 Merancang belanjawan, seni bina rangkaian dan perkara-perkara lain yang berkaitan.

(a) Peruntukan kewangan merupakan perkara utama yang perlu dipertimbangkan bagi perolehan perkakasan atau perisian yang baru (jika perlu). Keperluan agensi bagi penggunaan IPv6 perlu diambil kira semasa penyediaan belanjawan. Antara persoalan yang mungkin timbul adalah seperti berikut :

(i) Bagaimana IPv6 dapat memberi faedah kepada sesebuah agensi?

(ii) Apakah faedah-faedah teknikal yang dapat diperoleh dari IPv6 untuk agensi?

(iii) Apakah bidang perkhidmatan yang dapat diperluaskan dengan penggunaan IPv6?

(iv) Apakah impak daripada pelaksanaan IPv6 kepada agensi?

(b) Agensi boleh merujuk kepada senarai semak seperti di **Lampiran E** dan **Lampiran F** bagi mengumpulkan maklumat berkaitan infrastruktur rangkaian, perisian dan perkhidmatan rangkaian sedia ada di agensi masing-masing.

(c) Setelah keperluan pelaksanaan IPv6 dikenalpasti, agensi perlu melaksanakan perkara-perkara berikut:

(i) Merancang peruntukan untuk pembelian perkakasan atau perisian yang baru (jika diperlukan); dan

(ii) Menganalisis semula infrastruktur rangkaian yang menyokong IPv6.

(d) Proses transisi yang akan dijalankan dipengaruhi oleh persekitaran sedia ada. Sebagai contoh, terdapat aplikasi yang telah dibangunkan secara khusus dan mungkin tiada lagi sokongan daripada pembekal. Sesetengah aplikasi mungkin menghantar alamat IPv4 dalam aliran data yang akan menjejaskan penggunaannya dalam persekitaran IPv6. Persoalan dan isu ini sepatutnya telah dikenalpasti semasa pelaksanaan persekitaran simulasi. Isu ini akan menentukan kos dan masa yang diperlukan untuk melaksanakan IPv6.

(e) Agensi perlu mengetahui jangka hayat sesebuah produk kerana sesetengah perisian mungkin sudah tidak mempunyai sokongan daripada pembekal (mencapai "*end-of-life*") dan penggantian perlu dipertimbangkan sebelum membuat sebarang keputusan untuk melakukan penggantian dibuat.

(f) Agensi juga perlu mengenal pasti mekanisme transisi yang boleh digunakan untuk memudahkan proses transisi. **Lampiran B** digunakan untuk mengenal pasti mekanisme peralihan bagi menjelaskan cadangan dan pelaksanaan keseluruhan rangkaian secara teratur.

(g) Bagi agensi yang memutuskan untuk tidak menggunakan sebarang mekanisme transisi, maka agensi tersebut hanya akan berkeupayaan untuk menggunakan IPv6 sahaja tetapi tidak dapat berhubung dengan IPv4. Pendekatan terbaik yang disyorkan dalam menyelesaikan isu ini adalah dengan menggunakan mekanisme *dual-stack* kerana ia memberikan keserasian untuk kedua-dua protokol. Mekanisme *tunneling* boleh digunakan sekiranya rangkaian tiada keupayaan IPv6.

(h) Agensi boleh mendapatkan khidmat nasihat perunding yang berpengalaman bagi membantu pelaksanaan IPv6 kerana kekurangan kepakaran, kakitangan, pengalaman dan sebarang isu yang akan timbul semasa pelaksanaan dijalankan.

(i) Agensi boleh mendapatkan prefiks alamat IPv6 daripada pembekal perkhidmatan Internet (ISP) setelah kaedah pelaksanaan ditentukan. Tiga (3) kaedah untuk pengagihan alamat IPv6 adalah seperti berikut:

(i) *Stateless autoconfiguration* – juga dikenali sebagai "*serverless*". Pelayan tidak diperlukan untuk membekalkan maklumat alamat rangkaian seperti DHCP. Hos menghasilkan alamat sendiri menggunakan kombinasi maklumat berdasarkan maklumat prefiks rangkaian IPv6 yang dibekalkan oleh *router*.

(ii) *Statefull Configuration* – pelayan diperlukan untuk menghantar maklumat dan parameter sambungan rangkaian kepada nod dan hos. Pelayan menyelenggara

pangkalan data yang menyimpan semua alamat yang telah diberikan kepada nod dan memadankan dengan alamat yang diberikan oleh hos. Mekanisme ini adalah berasaskan penggunaan *Dynamic Host Control Protocol version* 6 (DHCPv6).

(iii) Konfigurasi secara manual – alamat IPv6 untuk hos dan nod adalah ditetapkan oleh pentadbir rangkaian secara manual.

10.3. Mewujudkan persekitaran simulasi.

(a) Setiap agensi digalakkan untuk melaksanakan pengujian IPv6 dengan mewujudkan persekitaran simulasi IPv6 di agensi masing-masing. Persekitaran simulasi ini hendaklah dilaksanakan berasingan daripada persekitaran sedia ada. Dengan mewujudkan persekitaran ini, dapat membantu agensi mendapat gambaran berkaitan pelaksanaan IPv6. Selain itu, kakitangan juga dapat memperolehi pengalaman untuk pelaksanaan sebenar di agensi tanpa menganggu operasi sedia ada secara terkawal.

(b) Persekitaran simulasi merangkumi kriteria-kriteria seperti berikut :

(i) Fleksibel

Persekitaran simulasi hendaklah menyokong pelbagai jenis ujian seperti ujian ke atas komponen, perisian dan perkakasan dalam mengenal pasti keupayaan terhadap IPv6.

(ii) Pengasingan

Persekitaran simulasi perlu dilaksanakan secara berasingan dengan persekitaran sedia ada supaya tiada gangguan terhadap operasi sedia ada.

(iii) *Interoperability*

Persekitaran ini membolehkan pelbagai peralatan yang dibekalkan oleh pembekal yang berbeza dapat diuji untuk memastikan peralatan tersebut berkomunikasi antara satu sama lain serta membolehkan agensi membuat pemilihan peralatan yang terbaik. Perkara ini dapat diuji dalam persekitaran simulasi tanpa dipengaruhi oleh pembekal.

(iv) Rangkaian

a. Infrastruktur

Reka bentuk persekitaran simulasi mesti menyerupai persekitaran rangkaian sebenar yang sekurang-kurangnya merangkumi *core* atau *edge router, switches* dan peralatan keselamatan.

b. Sistem pengoperasian

Persekitaran simulasi yang menyediakan pelbagai persekitaran sistem pengoperasian dapat memberi pengalaman dalam mengkonfigurasikan IPv6 di rangkaian sebenar.

c. Perkhidmatan

Mengenal pasti perubahan (jika ada) kepada perkhidmatan (*services*) yang digunakan. Contohnya SSH, HTTP, SNMP.

d. *Routing Protocols*

Kebanyakan *routing protocols* merupakan protokol yang khusus. Kesediaan *routing protocols* ini hendaklah diuji terhadap kedua-dua IPv4 dan IPv6.

(c) Dengan wujudnya persekitaran simulasi, pengalaman yang diperolehi dapat memberikan maklumat yang boleh digunakan untuk mengenal pasti masalah-masalah serta perkakasan dan perisian yang diperlukan.

10.4. Melaksanakan audit pematuhan dan audit keselamatan secara komprehensif.

(a) Setiap agensi hendaklah menjalankan dua (2) audit utama iaitu audit pematuhan IPv6 dan audit keselamatan.

(b) Agensi hendaklah melantik pakar secara dalaman atau pihak luar bagi menjalankan aktiviti audit pematuhan IPv6 dan audit keselamatan.

(c) Audit pematuhan IPv6 akan membantu sebuah agensi untuk membuat keputusan seperti di bawah:

(i) Mengenal pasti sebarang perubahan yang mungkin diperlukan kepada infrastruktur rangkaian;

(ii) Mengenal pasti perkakasan yang digunakan dan tahap sokongan yang diperlukan terhadap IPv6; dan

(iii) Menyediakan perancangan pelaksanaan IPv6 dengan lebih baik.

(d) Dari penemuan audit pematuhan IPv6, agensi boleh membuat keputusan untuk melaksanakan IPv6 dengan mengambil kira jenis trafik yang menggunakannya. Soalan-soalan di bawah perlu diberi perlu diberi perhatian:

(i) Adakah pengendalian paket dilaksanakan pada peringkat perkakasan atau perisian?

Pengendalian paket di peringkat perkakasan adalah lebih baik berbanding peringkat perisian. Walaubagaimanapun, sesetengah perkakasan yang membenarkan penaiktarafan *firmware* untuk membolehkan pemprosesan paket IPv6. Ini bermakna paket tersebut dikendalikan pada peringkat perisian. Perkara ini akan meningkatkan beban pemprosesan dan mengakibatkan pengurangan dalam bilangan paket yang diproses.

(ii) Apakah konfigurasi *routing* yang digunakan dan bagaimana ianya disokong oleh IPv6? Adakah kedua-dua *routing protocol* dalaman dan luaran dapat digunakan dalam persekitaran IPv6?

Routing protocol seperti RIP, OSPF dan BGP mempunyai versi tersendiri untuk IPv6 iaitu RIPng, OSPFv3 dan BGP4 yang tidak serasi dengan IPv4. Sehubungan itu, agensi perlu mempunyai dua (2) versi *routing protocol* dalam rangkaian (IPv4 dan IPv6).

(iii) Adakah *layer 3 switches* (VLAN) dan *load balancers* menyokong IPv6?

Sekiranya *layer 3 switches* dan *load balancers* tidak menyokong IPv6, maka penaiktarafan perkakasan ini hendaklah dibuat agar tidak menjejaskan rangkaian agensi secara menyeluruh terhadap kedua-dua persekitaran IPv4 dan IPv6.

(e) Audit keselamatan boleh membantu mengenal pasti kelemahan dalam aspek keselamatan dan kaedah untuk memperkukuhkannya. Tahap keselamatan infrastruktur rangkaian sedia ada perlu dikaji sebelum sebarang teknologi baru diperkenalkan.

(f) Audit kawalan keselamatan terdiri daripada dua (2) kategori iaitu:

(i) Audit luar merangkumi kriteria seperti berikut:

a. Imbasan rangkaian (*Site scans*);

b. Audit jarak jauh (*Remote*);

c. Ujian Penembusan (*Penetration tests*); dan

d. *IP Spoofing.*

(ii) Audit dalaman merangkumi kriteria seperti berikut:

a. Menilai diagram rangkaian sedia ada;

b. Menemuduga pentadbir-pentadbir berkenaan mengenai:

i. Akses fizikal dan infrastuktur

ii. Perkakasan keselamatan

iii. *Router*

iv. Sistem pengoperasian (OS)

v. Perkhidmatan seperti SSH, telnet dan lain-lain

vi. Pangkalan data

vii. Aplikasi-aplikasi

c. Imbasan dalaman; dan

d. Ujian Penembusan (*penetration tests*).

(g) Hasil penilaian audit boleh digunakan untuk memperkukuhkan infrastruktur sedia ada dan membantu dalam menentukan perkara berikut:

(i) Adakah amalan terbaik diguna pakai dalam infrastruktur semasa?

(ii) Adakah terdapat sebarang trafik IPv6 yang tidak dikehendaki atau tidak diketahui dalam infrastruktur?

(iii) Adakah keupayaan *firewall* dapat mengesan dan menyekat mekanisme *tunneling* seperti 6to4, ISATAP, IPsec dan sebagainya? Ini bertujuan untuk memastikan sambungan IPv6 yang tidak dikehendaki menerusi *tunneling* dapat dihalang.

(h) Perkara-perkara yang perlu dipertimbangkan dalam memastikan keselamatan semasa pelaksanaan IPv6 adalah seperti di **Lampiran C.**

10.5. Mewujudkan aplikasi yang menggunakan kelebihan IPv6.

(a) Contoh aplikasi yang menggunakan ciri IPv6 adalah seperti berikut:

(i) *Internal Messaging System* untuk kegunaan agensi.

(ii) *Website* dalaman agensi yang boleh dicapai melalui sambungan IPv6.

(iii) *Mail Server* untuk kegunaan dalaman.

(b) Pada peringkat ini, pelaksanaan IPv6 tidak perlu dilakukan kepada aplikasi utama. Ini bagi mengelakkan sebarang permasalahan

berlaku yang boleh menjejaskan perkhidmatan agensi. Pelaksanaan IPv6 terhadap aplikasi utama hanya akan dibuat pada fasa ketiga.

10.6. Penilaian pelaksanaan IPv6.

(a) Setiap agensi hendaklah melaksanakan penilaian terhadap pelaksanaan IPv6 yang telah dilakukan. Penilaian yang merangkumi perkara-perkara berikut:

(i) Adakah jangka masa pelaksanaan yang ditetapkan dipatuhi?

(ii) Apakah isu dan permasalahan yang dihadapi semasa pelaksanaan IPv6?

(iii) Apakah aspek yang perlu diberi tumpuan dan perhatian?

(iv) Adakah pelaksanaan IPv6 dapat membantu memenuhi keperluan agensi?

(v) Adakah agensi bersedia untuk melaksanakan IPv6 di peringkat cawangan?

(b) Berdasarkan penilaian yang telah dijalankan, agensi boleh mengenal pasti langkah-langkah bersesuaian yang boleh memudahkan pelaksanaan IPv6 seterusnya.

10.7. Kajian kes pelaksanaan IPv6 boleh didapati di **Lampiran D.**

11. Fasa 2

11.1. Objektif fasa 2 adalah untuk memastikan pejabat cawangan berkeupayaan menyokong IPv6 dan mempunyai sambungan global yang selamat dengan melaksanakan semula aktiviti fasa 1 di cawangan-cawangan agensi. Ini juga akan memberikan agensi lokasi kedua untuk melakukan percubaan terhadap keupayaan IPv6.

11.2. Berikut merupakan perkara yang perlu dilakukan di cawangan agensi tersebut:

(a) Merancang belanjawan, seni bina rangkaian dan perkara-perkara lain yang berkaitan;
(b) Mewujudkan persekitaran simulasi;
(c) Melaksanakan audit pematuhan dan audit keselamatan secara komprehensif;
(d) Menyediakan beberapa aplikasi untuk memanfaatkan IPv6; dan
(e) Menilai pelaksanaan yang telah dijalankan.

11.3. Pelaksanaan bagi setiap tindakan yang dinyatakan di atas adalah seperti yang dilakukan dalam fasa 1.

12. Fasa 3

12.1. Fasa 3 adalah tertumpu kepada transisi aplikasi utama bagi memanfaatkan penggunaan IPv6 untuk mempertingkatkan prestasi, kestabilan dan ciri-ciri keselamatan.

12.2. Perkara yang perlu dipertimbangkan dalam pembangunan aplikasi adalah seperti berikut:

(a) Memahami impak dan kelebihan yang boleh didapati dari setiap ciri IPv6 yang digunakan; dan

(b) Penggunaan IPv6 sepenuhnya mungkin melibatkan kos tambahan dan keperluan latihan. Walaubagaimanapun penggunaan IPv6 akan menjimatkan kos dalam jangka masa panjang.

12.3 Penting bagi personel ICT untuk memastikan aplikasi ICT Sektor Awam adalah menepati ciri-ciri IPv6 (IPv6 *compliance*). Ini termasuklah aplikasi-aplikasi berikut:

(a) Aplikasi yang baru dibangunkan sama ada secara *in-house* atau *out-source*; dan

(b) Aplikasi sedia ada yang perlu disemak dan dinaiktaraf bagi mematuhi ciri-ciri IPV6.

Lampiran A

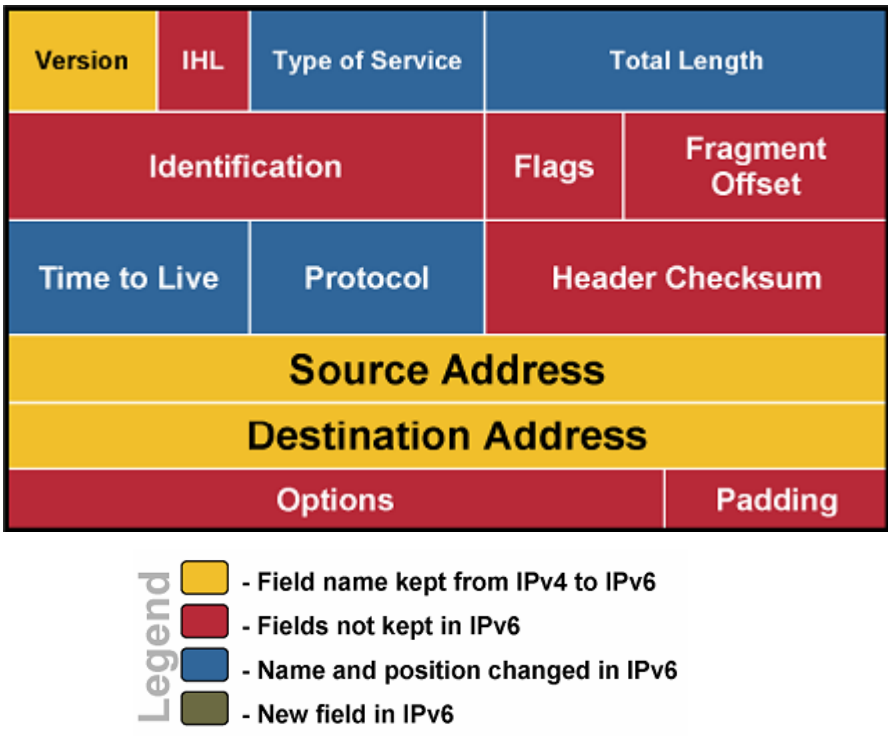
Perbezaan Antara

IPv4 dan IPv6

Lampiran A. *Differences between IPv4 and IPv6*

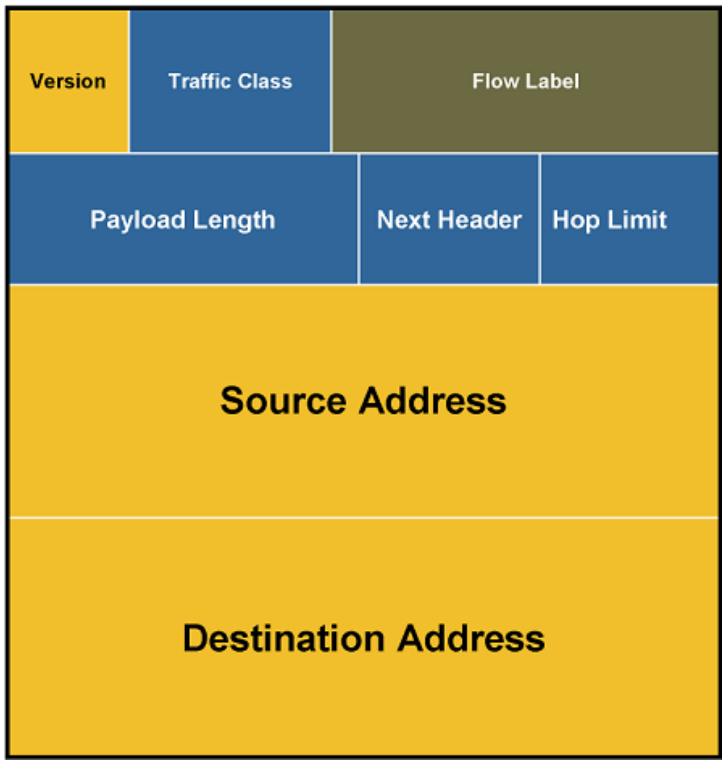
The packet structure of IPv4 and IPv6 are shown below to help illustrating the differences between the two (2) protocols.

Figure A-1 IPv4 Header



As the structure indicates, the packet structure for IPv6 is cleaner and simpler than the IPv4 packet. The removal of certain fields such as checksum has been done as the lower layer i.e. Ethernet already does verification therefore there is no reason for the IP layer to perform any additional checking. Additionally, IPv6 offers the ability to extend the header to support newer features by using something called ***Extension Headers****. This feature was added to allow IPv6 to be extended with minimal changes.*

Figure A-2 IPv6 Header



The table below highlights the key differences between IPv4 and IPv6.

Table A.1 Comparison between IPv4 and IPv6

IPv4	***IPv6***
Source and destination addresses are 32 bits (4 bytes) in length	*Source and destination addresses are 128 bits (16 bytes) in length.*
IPsec header support is optional.	*IPsec header support is required.*
No identification of packet flow for prioritized delivery handling by routers is present within the IPv4 header.	*Packet flow identification for prioritized delivery handling by routers is present within the IPv6 header using the Flow Label field.*
Fragmentation is performed by the	*Only the sending host performs*

IPv4	***IPv6***
sending host and at routers, slowing router performance.	*fragmentation.*
Has no link-layer packet-size requirements, and must be able to reassemble a 576-byte packet.	*Link layer must support a 1280-byte packet and be able to reassemble a 1500-byte packet.*
Header includes a checksum.	*Header does not include a checksum.*
Header includes options.	*All optional data is moved to IPv6 extension headers*
ARP uses broadcast ARP Request frames to resolve an IPv4 address to a link-layer address.	*ARP Request frames are replaced with multicast Neighbor Solicitation messages.*
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	*IGMP is replaced with Multicast Listener Discovery (MLD) messages.*
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	*ICMPv4 Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and it is required.*
Broadcast addresses are used to send traffic to all nodes on a subnet.	*There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.*
Must be configured either manually or through DHCP for IPv4.	*Does not require manual configuration or DHCP for IPv6.*
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4	*Uses AAAA records in the DNS to map host names to IPv6 addresses.*

IPv4	***IPv6***
addresses.	
Uses pointer (PTR) resource records in the INADDR. ARPA DNS domain to map IPv4 addresses to host names.	*Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.*

Lampiran B

Strategi Peralihan

IPv6

Lampiran B. *IPv6 Transition Strategies*

B.1. *Introduction to IPv6 Transition*

1. *The huge Internet size and the unlimited number of IPv4 users today make it inappropriate to migrate from IPv4-only to IPv6-only. As organizations are depending more on the Internet to perform their daily tasks, the downtime to replace the protocol will not be tolerated. Thus, the best alternative will be the co-existence of the both protocols at the same time and the transition should be implemented node by node based on the auto configuration procedure which makes it unnecessary to configure IPv6 hosts manually. This will be the best way for users to derive the IPv6 advantages while still being able to communicate with IPv4 devices.*

2. *There are a number of requirements that has been identified as the way IPv6 services should be introduced in a network such as:*

    (a) *The current existing IPv4 services should not be adversely disrupted as such situation might happen when router loading process of encapsulating IPv6 in IPv4 for tunnels;*
    (b) *IPv6 services should perform as well as the IPv4 services (For instance, at the IPv4 line rate and with similar network characteristics);*
    (c) *The services must be easily managed and monitored whereby tools should be available for both the protocols;*
    (d) *Network security should not be at stake because of the additional protocol itself or loophole of if any, the transition mechanism used; and*
    (e) *A plan for IPv6 address allocation should be created.*

B.1.1. *Requirements for the Transition to IPv6*

1. *The requirements that should be meet when creating the transition part of the transition plan according to RFC1752 (The Recommendation for the IP Next Generation Protocol) are as below:*

    (a) *Incremental upgrade whereby upgrading for IPv4 devices to IPv6 with no dependencies on other devices.*
    (b) *Incremental deployment whereby new IPv6 devices can be installed with no prerequisites.*
    (c) *Easy addressing in which the upgrading of IPv4 devices to IPv6 allows the current addressing to continually be used.*
    (d) *Low start-up costs, as not much preparation work is necessary to upgrade the current IPv4 systems to IPv6 or deploying the new IPv6 systems.*

B.1.2. *Transition Techniques*

2. *The transition from IPv4 to IPv6 will be done one step at a time, initiating from a single host or subnet. Deployment of IPv6 in a large-scale network will require more than just one technique according to the various demands and requirements of the network. The three main transition techniques are:*

    (a) ***Dual-Stack***

        (i) *Dual stack mechanism is one of the simplest methods of introducing IPv6 to a network and is also the best way for IPv4 and IPv6 to co-exist in the same time before the complete transformation to IPv6-only network in the future.*

With the dual-stack technique, a host or router has IPv4 and IPv6 protocol stacks in the operating system. IPv4 and IPv6 addresses are configured into each IPv4/IPv6 node whereby the node can send and receive datagram and communicate with nodes in the IPv4 combined with IPv6 network. Dual stack scenario does not require any real transition mechanism as it can integrate IPv6 by itself.

(ii) *The issue of deploying an IPv4/IPv6 dual stack network is the configuration of internal and external routing for IPv4 and IPv6 protocols. The interaction of the IPv4 and IPv6 protocols is also a challenge as it is necessary to oversee the management of the interaction, whereby the dual-stack network mostly be interacting with IPv4 external networks in the beginning of the IPv6 deployment.*

(iii) *Basically, a network or backbone becomes dual-stack if the routers and switches in the network routes both IPv4 and IPv6. The implementation of the dual-stack technique will require the upgrading of routers to dual-stack which supports both IPv4 and IPv6 addresses. In a dual-stack implementation, access to IPv6 Domain Name System (DNS) as well as adequate memory for both IPv4 and` IPv6 is necessary. The challenges that may arise during dual-stack implementation are memory and CPU exhaustion as well as the need to introduce additional security requirement. Thus, steps should be taken to ensure that these issues and challenges do not arise; and a more smooth and cost-effective solution is obtained.*

(b) ***Tunneling***

(i) *Tunneling or encapsulation techniques used in the transition from IPv4 to IPv6 simply means that IPv6 is used on top of the current IPv4 infrastructure with no changes made to the routers or IPv4 routings. Tunnels encapsulate the IPv6 packets in IPv4 packets and are carried out to the network parts that are not IPv6 enabled. Tunneling technique is used only when the network is not able to offer native IPv6 functionality. The tunneling technique is used when the network is not at all or partly offering native IPv6 functionality. There are generally three steps involved in the tunneling process such as encapsulation, decapsulation and tunnel management. Two tunnel endpoints are required for the tunneling process. Most of the time the tunnel endpoints are IPv4/IPv6 dual-stack nodes which most of the time are the routers.*

(ii) *Tunneling is considered a practical approach to the transition from current IPv4 networks adopting the IPv6 technology but as there are quite a number of existing tunneling mechanisms, it is a difficult task to choose the right tunneling mechanisms.*

(iii) *There are varieties of methods for carrying IPv6 over existing IPv4 networks through either manually or automatically configured tunneling mechanism. The various kind of tunneling mechanisms includes configured tunnel; tunnel broker; automatic tunnels; 6to4; 6over4; ISATAP; Teredo; Tunnel Setup Protocol (TSP); DSTM; and Open VPN-based tunneling solution.*

(c) ***Translation Methods***

Translation methods are basically used when an IPv4-only device wants to communicate with an IPv6-only device, or vice-versa. Most importantly, IPv4-in-IPv6 is not used in this case. The various translation methods includes Stateless IP/ICMP Translation Algorithm (SIIT), Network Address Translation with Protocol Translation (NAT-PT) and Network Address Port Translation with Packet Translation (NAPT-PT); Bump-in-the-Stack (BIS); Bump-in-the-API (BIA); Transport Relay; SOCKS; Application Layer Gateway (ALG);

B.1.3. *Node Types*

3. *RFC 2893, "Transition Mechanisms for IPv6 Hosts and Routers," defines the following node types:*

(a) ***IPv4-only node*** *Implements only IPv4 and is assigned only IPv4 addresses. This node does not support IPv6. Most hosts—such as client computers, server computers, and network-capable devices such as printers—and routers installed today are IPv4-only nodes.*

(b) ***IPv6-only node*** *Implements only IPv6 and is assigned only IPv6 addresses. An IPv6-only node is only able to communicate with IPv6 nodes and IPv6-enabled applications. Although this type of node is not common today, it will become more prevalent as smaller devices such as cellular phones and handheld computing devices include only IPv6 stacks.*

(c) ***IPv6/IPv4 node*** *Implements both IPv4 and IPv6 and is assigned both IPv4 and IPv6 addresses. Computers running Windows Server 2008 or Windows Vista are by default IPv6/IPv4 nodes.*

(d) ***IPv4 node*** *Implements IPv4 and can send and receive IPv4 packets. An IPv4 node can be an IPv4-only node or an IPv6/IPv4 node.*

(e) ***IPv6 node*** *Implements IPv6 and can send and receive IPv6 packets. An IPv6 node can be an IPv6-only node or an IPv6/IPv4 node.*

B.1.4. *Comparison of transition techniques*

4. ***Dual-Stack***

(a) *Easy to use and flexible technique.*
(b) *Host can communicate with IPv4 hosts via IPv4 or communicate with IPv6 hosts via IPv6.*
(c) *IPv4 stack can be disabled when everything is fully IPv6.*
(d) *The greatest flexibility is obtained in deploying dual-stack hosts and routers as it deals with IPv4-only applications, equipments and networks.*
(e) *Dual-stack is a basis of the other transition techniques as tunnels need dual-stack endpoints and translators need dual-stack gateways.*
(f) *The disadvantage of this technique is that when there are two separate protocol stacks running, an additional CPU power and memory are required on the host.*

(g) *As all tables are kept twice with one per protocol stack, a DNS resolver who runs on the dual-stack host must be able of resolving both IPv4 and IPv6 address types.*

(h) *Applications that run on the dual-stack host must be able to determine on whether the host is communicating with an IPv4 or IPv6 peer.*

(i) *There is a necessity to have a routing protocol that is able to deal with IPv4 and IPv6 protocol (e.g. IS-IS which deals with both protocol); or routing protocols that deals with the both protocol separately (e.g. OSPFv2 for IPv4 network) and (OSPFv3 for IPv6 network).*

(j) *Firewall must be able to protect both IPv4 network and the IPv6 network; as well as separate security concepts and firewall rules for each of the protocol.*

5. ***Tunneling***

(a) *This technique allows the transition of IPv6 to take place the way the user wants.*

(b) *A specific order is not present for this technique as the upgrade of single hosts or single subnets can be done within a network and can connect to separate IPv6 clouds via tunnels.*

(c) *ISP support for IPv6 to able to access remote IPv6 networks is not necessary as tunneling is possible via IPv4 infrastructure.*

(d) *The upgrading of the backbone is not needed as if the backbone is IPv4, tunneling can be done to transport IPv6 packets over to the backbone.*

(e) *With an MPLS infrastructure, it is better to use this technique to tunnel the IPv6 packets if there is no necessity of upgrading the backbone routers to support IPv6 natively.*

(f) *The setback of this technique is additional load is placed on the router.*

(g) *The tunnel entry and exit points also need more time and CPU power to encapsulate and decapsulate packets.*

(h) *Complex troubleshooting as it is likely to have hop count or MTU size issues and also fragmentation issues. Managing encapsulated traffic such as per-protocol accounting is also tougher because of the encapsulation.*

(i) *Tunnels also rises security attack points.*

6. ***Translation***

(a) *Translation technique should only be used when other techniques are not suitable.*

(b) *Translation should be a temporary solution until the other techniques can be used.*

(c) *The setback of this technique is advanced IPv6 features such as end-to-end security is not supported.*

(d) *The design topology has limitations as there are no replies from the same NAT router that was initially sent.*

(e) *NAT routers are viewed as a single point of failure and it is not able to use the flexible routing mechanisms.*

(f) *Applications with IP addresses in the packets payload will stumble.*

(g) *The benefit of translation technique is IPv6 host's direct communication with IPv4 hosts and vice versa is allowed.*

Lampiran C

Keselamatan IPv6

Lampiran C. *IPv6 Security*

C.1. *Security implication in IPv6 Transition*

1. *The term security here is defined as steps taken to measure risks that software applications and network infrastructures are exposed to and implement solutions to overcome the risks. Risks and countermeasures includes the below:*

   (a) *Attacks on network infrastructure and network elements*
   (b) *Software application attacks, Denial-of-Service (DoS) attacks, Distribution of virus and data security breaches*
   (c) *Interception of data that travels across public domain*
   (d) *Security in IP is not only a concern for enterprise networks, but also for home networks.*

C.1.1. *Security in IPv4*

2. *Communications that a public network such as the internet facilitates require cryptographic services that protect the data sent from being modified or viewed. Despite having IPv4 security standard, it is still an option to have it implemented as propriety security solutions are also available.*

C.1.2. *Security in IPv6*

3. *IPv6 enhances many security issues suffered by IPv4. IPv6 has prominent security features such as IPSec (AH/ESP) that were back-ported to IPv4. The structure of IPv6 addressing too provides the resistance to scanning.*

The massive size of the IPv6 address creates a shield to block people from performing vulnerability scanning. Since IPv6 address can be auto configured, it makes it more complex for malicious attackers to search systems for weaknesses. This makes it a troublesome job to scan specific IPv6 networks. But, a poorly designed IPv6 network can be easily scanned, which is pretty much similar to the IPv4 model. IPv6 auto configuration offers easy setup and renumbering on demand which makes it simple for intruders to acquire access to local sub-networks to announce routers and routers to forward an attack or route systems through tunnels under illicit control.

4. *To cut it short, IPv6 comes with many features such as the reliable and easy set up using automatic configuration making it more appealing from a security perspective. The huge number of IP addresses it can generate makes it resistant to activity such as malicious scans and also inaccessible to hybrid threats as well as automated, self-propagating, and scanning worms. However, it should not be misunderstood that IPv6 would be the ultimate solution to all security risks. IPv6 is an enhanced internet protocol that provides mechanisms to overcome problems that occur specially at layer 3 – the network or IP layer. IPv6 may not be able to provide protection if applications are designed poorly, or servers are not configured properly.*

5. *Networks should also be monitored for IPv6 auto-configuration packets, router and neighbor discovery, and solicitation and advertisement packets. Sometimes, IPv6 may not be supported on a specific network segment. If such event occurs, it is a strong indication of possible misconfiguration, rouge tunnels and routing, or malicious actively. In contrast to that, if IPv6 is supported, then router advertisements and solicitations should be monitored for rouge routers, which may be an indication of intrusions or*

backdoors. Any non-infrastructure device which advertises a new IPv6 route or prefix should be immediately marked for investigation.

C.2. *Security Considerations during Transition/Transition*

6. *The most crucial procedure of the transition is to consider the security aspect during the deployment and transition process. It is important to make sure that the outcome of the transition would improve the overall security level of the current infrastructure or at least the transition process should not worsen the current security level. It has to be made sure that the current security products should be able to support IPv6. Security is the key factor to IPv6 adoption, so current IPv4 security solutions must be upgraded to support IPv6 even though IPSec is included in the IPv6 specification.*

C.2.1. *Application Layer*

7. *Having an IPv6 infrastructure, applications can take advantage of the new security features that have the ability to solve some of the issues discussed earlier. Some of these features offer better protection against address and port scanning attacks. Since it is a requirement for all IPv6 implementations to support IPSec, authentication and/or cryptographic protection of IPv6 traffic could be enabled.*
8. *IPSec is centrally controlled with administrative policy, such as the Microsoft Group Policy. If this policy needs to be configured, then it should be directly applied to the operating system. This eliminates the need for administrators or applications to pay special attention to network-level security with new features that configure and control IPSec. This also makes the deployment of IPSec uniform and consistent across the enterprise or government organization.*

C.2.2. *Premises*

9. *Whether it is central site, remote branch, or a regional office, the utilization of production grade security appliances and systems is paramount. It is important to have these security appliances as they can be used to implement security policies, including firewall access control, traffic management, and VPN encryption at all relevant locations.*

10. *A firewall delegates itself as a first layer security mechanism by controlling who and what has access to the network, providing network segmentation and user containment through secure virtual segments, employing user access control and authentication, and by protecting against Denial of Service (DoS) attacks by leveraging stateful inspection capabilities. The next layer of security mechanism uses a VPN solution for encryption of communications traversing an untrusted medium that may include the internet or an internal network segment. Other than that, these security appliances will need to provide additional protection from a number of threats, including viruses, worms, backdoors, Trojans through antivirus, Web filtering, and anti-spam methods.*

11. *As organizations migrate from IPv4 to IPv6, it is crucial to have these security appliances deployed to enable stateful firewall and IPSec VPN capabilities for IPv4 and IPv6 traffic. It has to be made sure that these appliances must be able to provide full support to IPv6 protocol, most of the transition mechanisms, and traditional networking, routing, and addressing features to enable customers deploy them in a production IPv6 or IPv4/IPv6 hybrid network. These appliances must also be able to provide optimum performance for all applications through the use of integrated hardware acceleration techniques.*

C.2.3. *Infrastructure*

12. *In order to get transitioned to IPv6, these infrastructure products will have to support full routing and MPLS, and provide a rich set of IP services including security, policy, and control for both IPv4 and IPv6 traffic.*

13. *The security features these IPv6 infrastructure products have to offer should include sophisticated schemes that protect the appliances in real time from unauthorized access and unsolicited attacks of either forged routing packets or bogus management traffic. By using hardware-based filtering mechanism and IPSec, these products should be able to protect the system and its interfaces, including the control plane and data plane during any communication session between devices.*

Lampiran D

Kajian Kes

Pelaksanaan IPv6

Lampiran D. *Generic IPv6 Deployment Case Study*

D.1. *The IPv6 Pilot Project*

1. *The transition process will comprise of 4 phases that includes the infant stage of the transition process until a functional dual-stack IPv6 network is achieved. The four phases include:*

Phase 1	***Phase 2***	***Phase 3***	***Phase 4***
Single and isolated network dual-stack tunneling before the main firewall	*IPv6 connectivity for selected virtual networks using a fixed tunnel client (dual-stack)*	*Implementation of IPv6 network in the entire network infrastructure*	*IPv6 usage and deployment for application and network services*

2. *The four phases described are implemented based of the current techniques of IPv6 network transition techniques that are recognized by the IPv6 Forum. The first and second phase will provide network administrators and consultants a primary view on the how the current network setting respond to the transition process. There will be categorized as the "**Primary Stage**" of the transition. The expectation of any serious network problems occurring in the 1st phase is quite low as there is no need for any production networks to be involved in this phase. Several primary parameters will be evaluated in this phase of transition. The systems administrators and the network consultants will conduct the observation of these parameters.*

D.2. *Implementation Phases Descriptions*

3. *The process of the transition is to be performed based on [RFC 3053] and [RFC 2743] which describes the use of the tunneling technique for IPv6 networks to travel through the IPv4 Internet.*

4. ***Phase 1***

(a) *The following are the objectives of the Phase 1 implementation:*

(i) *Ensure that seamless internet connection is available from the IPv6 Replica Network (RN);*

(ii) *The tunneling client receives the intended host address delegated by the tunneling sever; and*

(iii) *Data communications at the application level is expected to perform at an acceptable degree.*

(b) *The mentioned objectives are fundamental requirements to ensure that the intended IPv6 network works within an accepted level of performance. The performance will be evaluated upon the success of the IPv6 network being able to reach the global internet via the intended gateway using IPv6 addresses. The tunnel broker will be expected to provide a running /64 prefixes to the end hosts. Any timeout in the process of an ICMPv6 [RFC 2463] echo will serve as an initial evaluation for network stability. However, the network needs to run on a stable IPv4 environment before the evaluation on the network stability can be made. The success in achieving the listed objectives will be based on the report by the network consultants in charge on the testing.*

(c) *The first phase can be summarized into the following:*

(i) *Install the IPv6 tunnel client create an IPv6-in-IPv4 tunnel from IPv6 Agency to the IPv6 service provider/tunnel broker.*

(ii) *Test the tunnel connectivity to ensure that the security products (firewall, router's ACL etc.) do not block the tunnel connectivity to the IPv6 service provider/tunnel broker.*

(iii) *Once the tunnel is successfully established, a node at the agency will be used to check the IPv6 connectivity continuously for several working days.*

(d) *Planning for the phase 2 will be made once the IPv6 connectivity is proven to be at a working and reliable state. The establishment of the IPV6 RN will allow close monitoring of the IPv6 network within the agency. The equipment setup will not interfere with the existing production network. The testing includes of the tunnel will involve the following:*

(i) *IPv4 ICMP echo from IPV6 RN to the IPv6 service provider/tunnel broker (end to end point testing);*

(ii) *IPv6 address allocation by the tunnel broker to the host at the agency;*

(iii) *IPv6 ICMP echo from IPV6 RN to the IPv6 service provider/tunnel broker (gateway test); and*

(iv) *IPv6 ICMP echo from IPV6 RN to other sites within the global IPv6 network.*

(e) *Once successful a custom firewall will be located between the connection of IPv6 RN and NAv6 to test if there is any traffic interruption to the link due to IPv4 firewall settings. Continuous testing of the IPv6 connectivity will be either of the following:*

(i) *Continuous ICMP echo request and reply from IPv6 RN to any connected sites*

(ii) *Periodic file transfer activity activities between IPV6 RN and NAv6*

(f) *The commencement for phase 2 will be confirmed once the tests are completed with reasonable results provided that there are no errors in the configurations. Current configuration will then be adjusted to the network settings in phase 2.*

5. ***Phase 2***

(a) *The followings are the objectives of the Phase 2 Pilot Project implementation:*

(i) *Users will be able to access the IPv6 networks via virtual LANs in certain production networks within the agency;*

(ii) *The success of the virtual IPv6 LAN to communicate to the internet over a Firewall; and*

(iii) *Host will receive delegated prefix from the tunnel broker*

(b) *After recognizing the fundamental needs for the network to communicate through IPv6, the following step requires the network to provide IPv6 prefixes for hosts. The virtual LANs will operate under the surveillance of a firewall. The IPv6 tunnel broker will create the virtual LAN. The firewall will ensure that unwanted traffic will not go into the network via the tunnel. The performance and the responsiveness of the networks to the implementation will be documented for further action to be taken either for the purpose of maintenance or proceeding to the next phase.*

(c) *The second phase of the network will be performed according to the following steps:*

(i) *IPv6 connection will be made available to the 'User Virtual LAN'.*

(ii) *A firewall will be installed to secure the IPv6 connection for the 'User Virtual LAN'*

(iii) *Network utilization and security implication analysis will be made available once IPv6 connectivity is established.*

(d) *IPv6 connectivity will be provided to the extended in certain location within the agency via a Virtual LAN with a tunnel provided to each points of the selected network. Host machines will use IPv6 addresses with the addressed assigned by the tunnel broker with no specific IPv6 link-local address as the IPv6 network interface only appears as a virtual device in the host machine.*

(e) *A firewall will be placed to monitor and manage the traffic that is moving along the selected locations of the IPv6 Tunnel Gateway/IPv6 Router. Once IPv6 connectivity is made available, the network utilization and other security implications will be monitored using available commercial network monitoring tools.*

6. ***Phase 3***

(a) The following are the objectives of the Phase 3 Pilot Project implementation:

(i) *The entire agency IPv6 network will be connected to internet over the IPv6 gateway; and*

(ii) *The core IPv6 traffic filtering firewall is expected to be in place*

(b) The transition in this phase will proceed to the point where the entire agency's network will be tunneled to the Internet via an IPv6 Router. It is also expected that all hosts in the agency's network will acquire its own IPv6 address via the prefixes delegated by the IPv6 Router. The IPv6 address will conform to the address assignment scheme assigned by the tunnel broker with an initial /64 prefix being delegated to each host. However each host in the network will also be configured to run on dual-stack with prefixes delegated by the routers configured with IPv6.

(c) An IPv6 core firewall will also be in place to protect the networks from any unwanted IPv6 traffic from different departments of the entire agency's IPv6 network. The issue on the security for IPv6 network coexistence will be taken into consideration based on [RFC 4942]. Information collected in this phase will serve as a reference for maintenance and procession to the next phase.

(d) The third phase of the IPv6 Pilot Project includes the following:

(i) *IPv6 connectivity will be made available throughout the agency's network via the manually configured tunnel from the agency to NAv6.*
(ii) *Gradually remove the need for a tunnel broker.*
(iii) *The study on the current network infrastructure will be done and the requirements of making necessary purchases will be made available for further discussion. (if necessary)*
(iv) *The core firewall will be configured to secure the IPv6 traffic.*

(v) *IPv6 capabilities will be made available to all the servers via operating system configuration. A dual stack system will be configured for all nodes.*

(vi) *Network utilization and security implication analysis will be made available once IPv6 connectivity is established throughout the agency.*

7. ***Phase 4***

(a) *The following are the objectives of the Phase 4 Pilot Project implementation:*

(i) *Collective and comprehensive information based on the network is acquired*

(ii) *A guideline for IPv6 services transition is to be made available*

(b) *The final product of the entire preliminary transition of the pilot project is included in this phase whereby a comprehensive study on the network setup is done. The experiences and the problems that may have occurred on the entire 4 phases is analyzed and documented. The documentation is also expected to serve as a base for the guideline of IPv6 based services to be drafted. All IPv6 services that are to be implemented will have to abide to the policies and recommendations documented in findings of the transition study.*

(c) *The entire four phases of the transition is aimed at allowing the agency's networks to experience a trial IPv6 environment with the aid of a tunnel broker and later to run it via an IPv4/IPv6 dual-stack environment. It will provide the network engineers with a clearer*

insight on the potential benefits of IPv6 running on local area networks in a large enterprise environment. However, problems or obstacles that occur during the 4 phases of early transition to IPv6 should serve a note to network engineers to pay attention to the behavior of the network while running in IPv6.

Lampiran E

Senarai Keperluan

Peralihan IPv6

Lampiran E. *IPv6 Transition/Deployment Requirements Checklist*

Another activity that can assist agencies with requirements gathering is to answer a series of questions about the segments of their network infrastructure. The network infrastructures components are identified below provide an initial template to ascertain the requirements to determine an agency plan to transition to IPv6.

Agency's Provider Requirements

No.	***Items***
1	*Question: Is external connectivity required?*
	Answer:
2	*Question: Do your agency have only one site or multiple sites, and are they within different geographies?*
	Answer:
3	*Question: Is the private wide area network (WAN) infrastructure (e.g., leased lines) shared (e.g., VPNs/ISP)?*
	Answer:
4	*Question: If the agency has multiple sites, how is the traffic exchanged securely?*
	Answer:
5	*Question 5: How many global IPv4 addresses are available to the agency?*
	Answer:

No.	***Items***
6	*Question: What is the IPv6 address assignment plan available from the provider?*
	Answer:
7	*Question: What prefix delegation is required by the agency?*
	Answer:
8	*Question: Will the agency be multi-homed?*
	Answer:
9	*Question: What multi-homing techniques are available from the provider?*
	Answer:
10	*Question: Will clients within the agency be multi-homed?*
	Answer:
11	*Question: Does the provider offer any IPv6 services?*
	Answer:
12	*Question: Which site-external IPv6 routing protocols are required?*
	Answer:
13	*Question: Is there an external data center to the agency, such as servers located at the Provider?*
	Answer:
14	*Question: Is IPv6 available using the same access links as IPv4, or different ones?*
	Answer:

Agency's Application Requirements

No.	***Items***
1	*Question: List of applications used?*
	Answer:
2	*Question: Which applications must be moved to support IPv6 first?*
	Answer:
3	*Question: Can the application be upgraded to IPv6?*
	Answer:
4	*Question: Do the application have to support both IPv4 and IPv6?*
	Answer:
5	*Question: Do the enterprise platforms support both IPv4 and IPv6?*
	Answer:
6	*Question: Do the applications have issues with NAT v4-v4 and NAT v4-v6?*
	Answer:
7	*Question: Do the applications need globally routable IP addresses?*
	Answer:
8	*Question: Do the applications care about dependency between IPv4 and IPv6 addresses?*
	Answer:
9	*Question: Are applications run only on the internal network?*

No.	***Items***
	Answer:

Agency's IT Department Requirements

No.	***Items***
1	*Question: Who "owns"/"operates" the network: in house or outsourced?*
	Answer:
2	*Question: Is working remotely (i.e., through VPNs) supported?*
	Answer:
3	*Question: Are inter-site communications required?*
	Answer:
4	*Question: Is network mobility used or required for IPv6?*
	Answer:
5	*Question: What are the requirements of the IPv6 address plan?*
	Answer:
6	*Question: Is there a detailed asset management database, including hosts, IP/MAC addresses, etc.?*
	Answer:
7	*Question: What is the agency's approach to numbering geographically separate sites that have their own Service Providers?*

No.	***Items***
	Answer:
8	*Question: What will be the internal IPv6 address assignment procedure?*
	Answer:
9	*Question: What sites internal IPv6 routing protocols are required?*
	Answer:
10	*What will be the IPv6 Network Management policy/procedure?*
	Answer:
11	*Question: What will be the IPv6 QOS policy/procedure?*
	Answer:
12	*Question: What will be the IPv6 Security policy/procedure?*
	Answer:
13	*Question: What is the IPv6 training plan to educate the enterprise?*
	Answer:
14	*Question: what will network operations software IPv6 impact?*
	Answer:
15	*Question: what will network hardware IPv6 impact?*
	Answer:
16	*Question: Are all these hardware functions upgradeable to IPv6?*
	Answer:

No.	***Items***
17	*Question: If not, what are the workaround?*
	Answer:
18	*Question: Do any of the hardware functions stores, display, or allow input of IP addresses?*
	Answer:
19	*Question: Are the nodes moving within the agency network?*
	Answer:
20	*Question: Are the nodes moving outside and inside the agency network?*
	Answer:

Agency's Network Interoperation and Coexistence Requirements

No.	***Items***
1	*Question: What platforms are required to be IPv6 capable?*
	Answer:
2	*Question: What network ingress and egress points to the site are required to be IPv6 capable?*
	Answer:
3	*Question: What transition mechanisms are needed to support IPv6 network operations?*

No.	***Items***
	Answer:
4	*Question: What policy/procedures are required to support the transition to IPv6?*
	Answer:
5	*Question: What policy/procedures are required to support interoperation with legacy nodes and applications?*
	Answer:

Lampiran F

Senarai Semak Penilaian Infrastruktur Rangkaian

Lampiran F. *Network Infrastructure Assessment Checklist*

This checklist is to identify IPv6 compliance for existing networking peripherals, software and services.

Technical Personnel Detail	
Name	
Tel	
Fax	
Email	

1. Devices

1.1 Network Device (Layer 2)

Identify Network Device (3Com 3300 Switch, Cisco Catalyst 2960 Series Switches etc.)					
Device ID	***Name***	***Model***	***Firmware***	***Manufacturer***	***IPv6 Support***

1.2 Network Device (Layer 3)

Identify Network Device (Cisco 7200 Router etc).					
Device ID	***Name***	***Model***	***Firmware***	***Manufacturer***	***IPv6 Support***

1.3 Security

Identify Security Device (firewall, IDS, etc.)					
Device ID	***Name***	***Model***	***Firmware***	***Manufacturer***	***IPv6 Support***

1.4 Network Management (hardware base)

Identify Management Tool Device (Ciscoworks, etc.)					
Device ID	***Name***	***Model***	***Firmware***	***Manufacturer***	***IPv6 Support***

2. Operating Systems

2.1 Server

Identify Operating System for Server (Windows 2000,Linux etc.)			
Operating Systems	***Purpose***	***Version***	***IPv6 Support***

2.2 Client/Host

Identify Operating System for Hosts (Windows XP, Fedora etc.)			
Operating Systems	***Purpose***	***Version***	***IPv6 Support***

3. Network Service

3.1 Email

Identify Application for Services (pop3, smtp..etc)			
Application	***Package***	***Version***	***IPv6 Support***

3.2 Remote Shell

Identify Application for Services (telnet,ssh..etc)			
Application	***Package***	***Version***	***IPv6 Support***

3.3 File Sharing

Identify Application for Services (samba, tftp..etc)			
Application	***Package***	***Version***	***IPv6 Support***

3.3 Domain Name System

Identify Domain Name System Server application (bind, dbind..etc)			
Application	***Package***	***Version***	***IPv6 Support***

4. Network Application

4.1 Monitoring

Identify Network Configuration tools/applications (mrtg, nmap, tcpdump etc.)			
Application	***Package***	***Version***	***IPv6 Support***

4.2 Production

Identify office production tools (email client, Microsoft office etc.)			
Application	***Package***	***Version***	***IPv6 Support***

4.3 Web Server

Identify Web Servers (apache 1.3.37, Lighttpd 1.4.16, etc.)			
Application	***Package***	***Version***	***IPv6 Support***

4.4 DNS Server

Identify DNS Server (BIND 9.3.4, Windows Server 2003 DNS,...etc)			
Application	***Package***	***Version***	***IPv6 Support***

4.5 Email Server

Identify Email Server (Postfix & Dovecot, Sendmail & Cyrus IMAPD...etc)			
Application	***Package***	***Version***	***IPv6 Support***

4.6 Proxy Server

Identify Proxy Server (Squid Cache 2.6.STABLE12 + IPv6 Patch, Apache 2.0.59...etc)			
Application	***Package***	***Version***	***IPv6 Support***

4.7 Database Server

Identify Database Server (MySQL , Microsoft SQL 2000 / 2005...etc)			
Application	***Package***	***Version***	***IPv6 Support***

5. Sign Off

This is to certify that the Check List for Implement IPv6 has been completed successfully.

……..

Review & Confirm By:

Title:

Agency:

Rujukan

Lampiran G. *References*

1. **Siil, Karl A.** *IPv6 Mandates.* s.l. : Wiley, 2008.

2. **Grossetete, Patrick, Popoviciu, Ciprian P. and Wettling, Fred.** *Global IPv6 Strategies.* s.l. : Cisco Press, 2008.

3. **Beijnum, Iljitsch van.** *Running IPv6.* s.l. : Apress, 2005.

4. **Amoss, John A. and Minoli, Daniel.** *Handbook of IPv4 to IPv6 Transition: Methodologies for Institutional and Corporate Networks.* s.l. : Auerbach Publications, 2007.

5. **Hagen, Silvia.** *IPv6 Essentials.* s.l. : O'Reilly Media, 2006.

6. **Davies, Joseph.** *Understanding IPv6, Second Edition.* s.l. : Microsoft Press, 2008.

7. **Popoviciu, Ciprian, Levy-Abegnoli, Eric and Grossetete, Patrick.** *Deploying IPv6 Networks.* s.l. : Cisco Press, 2006.

8. **Blanchet, Marc.** *Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks.* s.l. : Wiley, 2006.

9. *IPv6: Legal Aspects of the New Internet Protocol.* s.l. : Euro6ix Book, 2006.

10. **Stockebrand, Benedikt.** *IPv6 in Practice: A Unixer's Guide to the Next Generation Internet.* s.l. : Springer, 2007.

11. **Malone, David and Murphy, Niall.** *IPv6 Network Administration.* s.l. : O'Reilly, 2005.

12. **Dunmore, Martin.** *An IPv6 Deployment Guide.* s.l. : 6Net Consortium, 2005.

13. **Rooney, Tim.** *IPv6 Addressing and Management Challenges.* s.l. : BT Diamond IP.

14. —. *Best Practices for Next-Generation IP Address Management.* s.l. : BT Diamond IP, 2007.

15. —. *IPv4-to-IPv6 Transition Strategies.* s.l. : BT Diamond IP, 2007.

16. *Evaluating IPv4 to IPv6 Transition Mechanisms.* **Raicu, Ioan and Zeadally, Sherali.** s.l. : IEEE, 2003.

17. IPv6 Transition Guidance. *Chief Information Officers Council (CIO Council).* [Online] 2005. http://www.cio.gov.

Glosari

Lampiran H. *Glossary*

A	
AH	*Authentication Header*
ARP	*Address Resolution Protocol*
ALG	*Application-level gateway*

B	
BGP	*Border Gateway Protocol*
BGP4+	*Border Gateway Protocol 4+*
BIA	*Bump-in-the-API*
BIS	*Bump-in-the-Stack*

D	
DHCP	*Dynamic Host Configuration Protocol*
DHCPv6	*Dynamic Host Configuration Protocol version 6*
DSTM	*Dual Stack Transition Mechanism*
DNS	*Domain Name System*

E	
ESP	*Encapsulating Security Payload*

H	
HTTP	*Hypertext Transfer Protocol*

I	
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ICMP	*Internet Control Message Protocol*
ICMPv6	*Internet Control Message Protocol version 6*
IPsec	*Internet Protocol Security*
ISP	*Internet Service Provider*
ISATAP	*Intra-Site Automatic Tunnel Addressing Protocol*
IGMP	*Internet Group Management Protocol*

M	
MyICMS 886	*Malaysia Information, Communication and Multimedia Services 886*

N	
NAT-PT	*Network Address Translation - Protocol Translation*
NAPT-PT	*Network Address Port Translation Protocol Translation*
NAT	*Network Address Translator*

O	
OSPF	*Open Shortest Path First*
OSPFv3	*Open Shortest Path First version 3*

P	
PDA	*Personal Digital Assistant*

Q	
QoS	*Quality of Service*

R	
RIP	*Routing Information Protocol*
RIPng	*Routing Information Protocol Next Generation*
RFID	*Radio-frequency identification*

S	
SSH	*Secure Shell*
SNMP	*Simple Network Management Protocol*
SIIT	*Stateless IP/ICMP Translation Algorithm*

T	
TSP	*Tunnel Setup Protocol*

V	
VLAN	*Virtual Local Area Networks*