IPv6 Deployment Strategies in APEC Economies

APEC Telecommunications and Information Working Group

August 2017

APEC Project:

Produced by
Ms Yang Xinrong
Infocomm Media Development Authority
10 Pasir Panjang Road
#10-01
Mapletree Business City
Singapore 117438

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#217-ES-01.1

IPv6 Deployment Strategies in APEC Economies

The objective of this project is to share APEC economies' IPv6 deployment strategies and to take stock of their adoption strategies. The aim is to enable economies currently in transition to benefit from the experiences of other economies.

Contents

Chapter 1. Introduction

Internet Protocol (IP) addresses are needed for devices that are connected to the Internet. These numeric addresses allow users to communicate by sending and receiving information. The proliferation of smart phones and other devices have driven the need for more IP addresses as more users and devices are connected via the Internet.

The Asia Pacific Network Information Centre (APNIC), which is the regional Internet Registry administering IP addresses for the Asia Pacific, reached the last /8[1] of Internet Protocol version 4 (IPv4) addresses in April 2011[2], making Asia Pacific the first region in the world to run out of IPv4. The scarcity of IPv4 therefore makes IPv6 deployment critical.

The Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL) initiative to adopt a set of APEC TEL IPv6 Guidelines in 2010 reflects the foresight and resolve that APEC economies have in facilitating the deployment of IPv6.

This project aims to enhance the mutual learning and understanding of IPv6 transition strategies to enable APEC economies to benefit from smooth deployment. The adoption of the new IP in economies' infocomm ecosystem will in turn drive the Internet's continued growth as a platform for innovation and economic development.

This project is in line with the priorities set out in the Strategic Action Plan 2016-2020, as endorsed at the 10th APEC TELMIN held in March 2015 in Kuala Lumpur, Malaysia, which seek to enhance online connectivity through the greater adoption of IPv6. It is also in line with the objective of the APEC TEL Development Steering Group (DSG) to promote ICT applications for socio-economic development.

In this paper, APEC economies have shared their IPv6 deployment strategies noting the various stages of preparatory work before actual deployment. Each APEC economy is unique in its geopolitical conditions, but common in its goal to be IPv6 capable. This paper will seek to note trends in their deployment strategies in order to serve as learning points for interested economies who are in the midst of their own IPv6 deployment planning.

[1] A /8 is made up of about 16 million IPv4 addresses

[2] https://www.apnic.net/community/ipv6-program

Chapter 2. IPv6 Adoption Strategy in APEC Economies

2.1 Australia

Background

The Australian Government Information Management Office (AGIMO) prepared a strategy for the implementation of IPv6 in Australian Government Agencies for endorsement by the Australian Government Chief Information Officer Committee (CIOC).in 2007[3] . Once endorsed, the Strategy was distributed to all Australian Government agencies and made publicly available in January 2008.

The Strategy proposed that all Government agencies should have IPv6 capable hardware and software platforms by 2012 and be able to operate dual stack IPv4 / IPv6 environments by 2015. In January 2009, the CIOC endorsed a revised strategy which brought these key milestones forward to end 2011 and end 2012 respectively.[4]

Issues relating to the implementation of IPv6 in an Australian Government context include:

- Government services remaining accessible to all citizens, regardless of whether they are using IPv4 or IPv6;
- Agencies being able to access web based services, regardless of whether they are provided over IPv4 or IPv6;
- The risk that unplanned and uncontrolled implementation of IPv6 equipment into government networks could compromise service delivery capability;
- The risk that the skills shortage in the ICT arena and in particular, the IPv6 field, may increase to the point that the government will not be able to engage suitably qualified IPv6 skilled technical and administrative staff;
- The opportunities for enhanced service delivery, particularly in the health, environment and transport industries, that IPv6 will allow with its ability to have multiple sensor / tracking devices in a variety of fields; and
- The risk that the cost of moving to IPv6 when industry and suppliers are driving the market will be significantly greater than if the whole-of- government transition is undertaken in a planned way.

[3] http://www.ipv6.org.au/09ipv6summit/talks/DBeauchamp_JHillier.pdf

[4] https://www.finance.gov.au/sites/default/files/Endorsed_Strategy_for_the_Transition_to_IPv6_for_Australian_Government_agencies.pdf

Overview of IPv6 action plan and strategies

The purpose of the Strategy was to assist agencies and interested parties by providing guidance on the steps that the Australian Government was taking to plan and manage the transition from IPv4 to IPv6. Co-ordinated planning of the transition allowed agencies to take advantage of the features of dual capable IPv4 / IPv6 platforms as they become available, while providing time to undertake the necessary training of staff and testing of systems.

IPv6 deployment strategy

The CIOC provided oversight for Australia's whole-of-government IPv6 deployment strategy. The CIOC established an IPv6 Community of Expertise to advise on issues that needed to be addressed in the strategy and to share information between agencies regarding the strategy, transition issues and IPv6 technical issues.

To assist the CIOC to implement the strategy, AGIMO coordinated whole-of-government reporting, coordinated management of whole-of-government issues, liaised with industry, state and territory governments, and internationally, to share lessons learned, promoted the availability of IPv6 test-bed facilities to all agencies to enable them to undertake specific tests if required.

While CIOC provided oversight and AGIMO provided assistance the assistance outlined above, each government agencies were responsible for the governance and implementation of the IPv6 deployment strategy within its portfolio.

The Australian Government undertook its IPv6 transition in three stages.

Stage 1: Preparation

The preparation stage of the Strategy involved each agency planning, conducting, and managing the following activities in preparation for the transition:

- Reviewing procurement policies to ensure that IPv6 capability was reflected in agency procurement process guidelines.
- Conducting a stock take of equipment to understand the current state of IPv6 readiness and the assist with the preparation of an agency-specific transition timeline.
- Conducting a stock take of applications to determine the priority of upgrading specific applications, including assessing how critical the application was for the agency's ability to deliver services.
- Progressively installing IPv6 capable equipment as part of their regular ICT refresh cycles
- Completing training and training needs analyses to ascertain what training was relevant, required and available.
- Undertaking threat and risk assessments to ensure that IPv6 related security threats and risks were considered as part of the regular Threat and Risk Assessments of their networks.

Stage 2: Transition

This transition stage of the Strategy involved agencies planning, conducting and managing the following tasks as they moved to a state of IPv6 readiness:

- Upgrading:
    - ICT hardware
    - Operating systems
    - Applications
    - ICT Gateways
- Ensuring that all IPv6 capability had been certified to the appropriate level of security.

Agencies were required to complete their certification of IPv6 capabilities by end 2011.

Agencies undertook their own testing of all IPv6 capability ready hardware and software installed in their ICT environments. This testing required agencies to enable IPv6 capability in order to check the readiness of components being tested. Agencies were required to disable these capabilities upon completion of testing.

Stage 3: Implementation

The implementation stage of the Strategy involved agencies confirming their IPv6 readiness and commencing operations through the following tasks:

- Undertaking final testing of IPv6 ready hardware and software to ensure all systems were operating as expected and the desired level of connectivity hd been achieved.
- Enabling IPv6 capability, subject to the satisfactory conduct of all Threat and Risk Assessments and certification of IPv6 platforms. In this regard, AGIMO consulted with agencies on the timing and process for enabling IPv6 across government and CIOC endorsed the timing and coordinated the approach for agencies to enable IPv6.

As part of this final stage, AGIMO was required to provide a report to the government advising that the stages in the Strategy had been completed and that the Australian Government was IPv6 ready.

Conclusion

The Australian Government closed its IPv6 transition in 2014 as by that stage all agencies had either reported that they had either successfully transitioned or put a transition plan in place.

2.2 Brunei Darussalam

Background

Brunei Darussalam, as with other countries in the region, has been following the issue of IPv4 exhaustion and its impact to the economy. In this regard, in an assessment report titled “Brunei Darussalam’s IPv6 Status Quo & Readiness Assessment”, which was published in May 2010, the Authority for Infocommunications Technology Industry (AITI) assessed the readiness of Internet Service Providers and also the E-Government National Centre on adopting IPv6.

This report gives an overview of the benefits and challenges of implementing IPv6 vis-à-vis IPv4 and analysed the impact (both positive and negative) on 3 stakeholder groups, namely Internet Service Providers (ISPs), Internet Users and Vendors.

Overview of IPv6 action plan and strategies

An IPv6 Committee, led by AITI, was established and comprised of representatives from ISPs, Government agencies and AITI. The IPv6 Committee is responsible for communicating and sharing all strategies and plans related to IPv6. AITI is also working with a local IT company, Asaff Solutions, on providing IPv6 training for technicians and engineers from ISPs as well as government agencies.

IPv6 Deployment strategies

The first meeting of the IPv6 Committee was in September 2013. Following that meeting, a seminar was held in AITI in December 2013 to discuss Global IPv6 deployment and the Brunei Darussalam IPv6 roadmap. The seminar was presented by an APNIC representative.

From the seminar, 4 main initiatives were identified, namely:

Initiative 1: Readiness of IPv6 Infrastructure.

Initiative 2: Human Capacity.

Initiative 3: Content and Services.

Initiative 4: Collaboration.

<u>Initiative 1: Readiness of IPv6 Infrastructure.</u>

The focus for this initiative is to create a national IPv6 network backbone through the national ISPs. This is done through the assessment of ISP’s current network infrastructure, the development of a manual for the IPv6 adoption in enterprises and the creation of a test bed for the purposes of testing IPv6 enabled networks.

Initiative 2: Human Capacity.

The focus here is to build up the awareness and skills required for the adoption of IPv6 through training courses and awareness programs. One of the aims of this area is also to provide certified IPv6 training programs in Brunei Darussalam in order to build up the next generation workforce with the skills required to assist in the transition to IPv6.

Initiative 3: Content and Services.

The aim of this initiative is to ensure the availability of IPv6 content nationally through programmes and/or pilot projects. For instance, the Government IPv6 project provided IPv6 enabled content from Government websites and services such as the e-Darussalam e-services. This also served as a "lead by example" approach before the wider adoption of IPv6 by the private sector and general public.

Initiative 4: Collaboration.

Collaboration is the foundation thrust recognized to be necessary for the successful implementation of the three thrusts mentioned above. The focus is to ensure that there will be a collaborative effort, and through that, a mutual understanding among stakeholders for IPv6 adoption in Brunei Darussalam.

In Brunei Darussalam, the transition phases are as follows: -

- Phase 1 – Assessments on current readiness for IPv6 adoption
    - This includes assessments on the readiness of current technical capabilities and human capacities, and the development of recommendations for the next phase.

- Phase 2 – Planning & Design
    - This includes planning budgets and designing of deployment methods, testing and simulation environments.

- Phase 3 – Implementation
    - This involves the implementation of recommendations from the previous phases.

- Phase 4 - Auditing / Maintenance
    - This includes assessing the success of the implementation (phase 3) and recommending improvements for the future.

State of Progress

The industry is fully supportive of the deployment of IPv6 ready networks for Brunei Darussalam. Generally, all ISPs have plans to make changes to their network. Some will deploy NAT due to budget constraints and legacy equipment, while others are looking into direct replacement of their systems.

Government agencies have a central IT unit (EGNC) that looks after all IT requirements such as network equipment, data servers, data storages and Internet connectivity. EGNC has deployed a dual stack architecture for their networks, where internally they are utilising IPv6 but communicating to other agencies that they are using IPv4.

Government agencies under EGNC are still using legacy equipment. Currently, there is no clear plan for replacing their networks but any new additions to their network are advised to be IPv6 ready. The same scenario is happening in private sectors as well.

For the near future, AITI plans to increase the rate of awareness for IPv6 adoption, especially in government networks. There is a possibility that due to budget constraints, it will take government agencies longer to plan for IPv6 adoption. At the same time, AITI plans to approach technical institutes and discuss the possibility of introducing IPv6 related subjects to their courses.

2.3 Hong Kong, China

Background

Hong Kong, China is one of the economy with highest IPv6 capability in the AP region.[5] The Internet infrastructure for Hong Kong, China is ready for IPv6 deployment and the adoption rate of IPv6 has been growing in the past years. Commercial IPv6 services are available from local Internet Services Providers. In particular,

- The Internet exchange services provided by the Hong Kong Internet Exchange (HKIX) have been supporting IPv6 since March 2004.
- Since 2006, the Hong Kong Internet Registration Corporation (HKIRC) has been offering IPv6 domain name services.
- Major ISPs in Hong Kong, China are well aware of the IPv4 address exhaustion issue and offer IPv6 access services to their customers.
- As at November 2016, around 325 organisations in Hong Kong, China have been allocated IPv6 addresses.
- As at November 2016, around 174 organisations and Internet Service Providers (ISPs) have IPv6 connections to HKIX.

[5] IPv6 Capable Rate by economy (%), http://stats.labs.apnic.net/ipv6/

Overview of IPv6 action plan & strategies

The member economy Government of the Hong Kong Special Administrative Region (HKSARG) supports the gradual migration of IPv4 to IPv6 and encourages the ICT sector to enhance their products and services to support IPv6. In Hong Kong, China, the regulatory framework for Internet carriers is technology-neutral. The adoption of IPv6 is driven by business needs and adopts a market driven approach for IPv6 development. The HKSARG has been working closely with industry players to promote IPv6. It also leads by example to demonstrate its support in adopting IPv6.

The HKSARG has taken forward the following actions for IPv6 adoption:

- The HKSARG Interoperability Framework recommends both IPv6 and IPv4 as specifications for network communications;

- The HKSARG requires the latest products to support IPv6 in government standing offer agreements;

- The HKSARG provides IPv6 support in the Government's core Internet infrastructure, and supports both IPv4 and IPv6 in the Government Wi-Fi Programme; and

- The HKSARG has set up theme pages in the website of the Office of the Government Chief Information Officer (www.ogcio.gov.hk) showing IPv6 information, resources and deployment; etc.

IPv6 deployment strategies

The HKSARG considers that the progressive IPv6 readiness of HKSARG services will encourage and promote the development of more IPv6 products and services in the local IT industry.

Meanwhile, the HKSARG actively promote the awareness of IPv6 among the general public over the years to equip business and Internet users with knowledge to migrate to IPv6:

During October 2011 to October 2012, the HKSARG sponsored Internet Society Hong Kong (ISOC HK) to take forward the "IPv6 in Action!" project which targeted the general public and SMEs. The project aimed to provide a better understanding of the IPv4 address space exhaustion situation as well as pre-requisites and potential issues for using IPv6, raise awareness on new applications and services for IPv6, and provide guidelines on how to select and apply IPv6 services offered in the market. The project deliverables included a thematic website, radio programs, promotion pamphlets, a consumer guide and seminars.

- In September 2013, the Hong Kong Science & Technology Parks Corporation (HKSTPC), which is a statutory body, organised the "IPv6 Certification Testing and Application Sharing Forum" to introduce IPv6 product certification testing service to the local market.

- Hong Kong Cyberport, which is fully owned by the HKSARG, is providing its tenants with an IPv6-based network infrastructure within its campus, which serves as a research and development platform as well as a conduit for connection to IPv6 networks outside Hong Kong, China since April 2006.

The HKSARG has already enabled IPv6 support in core Government IT infrastructure. Examples are:

- The HKSARG's Backbone Network connecting all bureaux and departments started supporting IPv6 in 2008.

- The central Internet infrastructure of the HKSARG for supporting the hosting of the Government's websites, Internet access and Internet mail access supports IPv6 since 2009. The public may access the HKSARG websites and exchange Internet mails with the HKSARG over IPv6.

- The e-Government Infrastructure Service for G2C and G2B transactions started similar support in 2010.

- The Hong Kong Observatory launched the IPv6 network time service on 29 March 2012.

- The GovWiFi Programme launched in December 2012 supports IPv6.

Progress of Private Sector

Private sector has also been spending efforts in taking forward IPv6 adoption since 2004:

The progress of the private sector in taking forward IPv6 adoption:

- In March 2004, the HKIX started the operation of Hong Kong IPv6 Exchange service.

- The Hong Kong Internet Registration Corporation (HKIRC), which manages ".hk" domain names under an agreement with the HKSARG, has commenced to offer IPv6 domain name service since 2006.

- In January 2007, the IPv6 Forum Hong Kong Chapter was founded to facilitate local research and development work for the deployment of IPv6 in Hong Kong, China.

- Hong Kong Next Generation Internet Society was formed in March 2010 to promote IPv6 and related technologies.

- The Internet Society Hong Kong (ISOC HK) provided training and seminars on IPv6 to its members/IT professionals.

- In July 2013, the “goIPv6 Consortium” launched the “goIPv6” programme to create business cases for commercial ISPs and offer each subscriber free-of-charge IPv6 tunnelling trial service.

- In March 2014, ISOC HK organised the “Are you ready for IPv6?” conference. The conference reviewed the latest development of IPv6 in Hong Kong, China and Asia Pacific after the World IPv6 Day and World IPv6 Launch in 2011 and 2012.

- Since 2011, ISOC HK has been provided training and seminars on IPv6 to its members/IT professionals.

As of November 2016, Hong Kong, China has the largest number (i.e. 206) of people in Asia whom were accredited IPv6 Sages certification. Besides, the percentage of IPv6 enabled networks in Hong Kong, China, as presented by the percentage of networks (ASes) that announce IPv6 prefix, is higher than both worldwide average as well as the APNIC region average.

Conclusion

The exhaustion of IPv4 addresses will not have immediate impact to Hong Kong, China. The Internet will continue to work and the IPv4 addresses already in use will continue to function. Both IPv4 and IPv6 protocols are expected to co-exist for a long period.

The progressive IPv6 readiness of government services will encourage and promote the development of more IPv6 products and services in the local IT industry. In addition, the HKSARG encourages businesses to plan for better utilisation of already allocated IPv4 addresses as an interim measure. In the long run, they should adopt IPv6 in addition to IPv4 for their Internet services.

2.4 Republic of Korea

Background

In its Implementation Guidelines for Fiscal Budget and Public Funds Management Plan 2008, the Ministry of Strategy and Finance advised that information systems should be constructed and operated using equipment that supports IPv6.

The e-Government Network had earlier (March 2006) also made IPv6 a requirement in all requests for proposal. In addition, the Technological Guidance on the Construction and Operation of Information Systems under the Act on Efficient Operation of Information Systems (September 2006) had made the application of IPv6 mandatory.

The following are key milestones in the promotion of IPv6 adoption in Korea:

- In 2008, a total of 16 agencies including municipal governments, research institutes in the Daedeok Special R&D District and the Korea Internet & Security Agency (KISA) were provided with IPv6 network equipment (routers, switches and firewalls, etc.) to encourage them to adopt IPv6. This led to the adoption of IPv6 by KT's e-Government Network.

- Through a pilot program to build IPv6-based services in 2010, IPv6 was applied to a commercial 4G wireless network for the first time in Korea.

- In 2012, three Korean telecom companies (KT, SK Broadband and LGU+) interlocked their backbones and Internet Exchanges (IXs) with IPv6 to create an environment where domestic commercial ISPs can also have access to IPv6. In addition, through a Private/Government collaboration, the KISA developed best practice guidelines for IPv6 switchover in wired and wireless services with a view to create an environment for IPv6-based wireless network and web hosting services.

- In order to encourage the use of IPv6 in wireless networks, SK Telecom developed an IPv6-based wireless network infrastructure (LTE and WiFi) and provided IPv6-based services with devices that supported IPv6.

In August 2013, LGU+ started to provide commercial, IPv6-based voice over LTE (VoLTE) services. At that point, compared to 2012, network operators were significantly more ready for an IPv6 subscriber network. More details are as follow:

Year	Backbone Network	Subscriber Network
2012	91.2%	19%
2013	92.1%	65%

Table 1 Readiness Ratio: The proportion of equipment that support IPv6 within backbone network (routers, switches, etc.) and subscriber network (OLT, CMTS, etc.).

- In 2014, commercial IPv6 services were fully deployed including for devices (Korean smartphones), network services (LTE) and content services (CP and CDN).

- After the successful launch of commercial IPv6 services in 2014, IPv6 service use rate reached 3.98% according to Google data as of December 2016.

- Through a Private/Government collaboration, including with CDN operators (KINX/K-grid), an IPv6-based CDN infrastructure was constructed. This facilitated interlocking with commercial web VoD services (Filecity).

- As of December 2014, Korea owned approximately 111 million IPv4 addresses and secured a sufficient number of IPv6 addresses (/32, 5,245) for domestic allocation.

- The krDNS is distributed and operated among 15 sites domestically and abroad with a total of five sites currently operating, which can support for both IPv4 and IPv6:

2004	2005	2006	2008
• Constructed the world-first .kr IPv6 DNS in Seoul (Jul)	• Constructed in Daejeon (Jun)	• Constructed in Germany (Aug) • Constructed in China (Oct)	• Constructed in Brazil (Sep)

- In 2015, three Small and Medium ISP Enterprises (with subscribers of less than 1 million) applied IPv6 to create environment that provides wired IPv6 network.

- Through a joint test to introduce IPv6 to the interlocking with international network, subscriber network-compatible equipment (CMTS) and CPE (customer premises equipment), dual-stack IPv6 connection services were launched in December for 58,000 subscribers across 11 regions.

Overview of IPv6 action plan/strategies

Build and publicize best practices of IPv6 application by cooperating with various stakeholders; share issues revealed during such processes to minimize trial and error in the private sector; encourage the private sector to voluntarily switch over to IPv6 and introduce IPv6 and spread onto every area in Korea; create in advance infrastructure that can proactively address the shortage of Internet address resources. Based on these, minimize social and economic costs that may occur during a switch over to IPv6 by relying on market forces.

Strategic Trusts

The Ministry of Science, ICT and Future Planning and the KISA, together with various stakeholders, established the 'IPv6 Expansion Roadmap to Promote a New Internet Industry' (March 2014)

- The IPv6 Support Center was established to operate comprehensive support systems for the IPv6 switch-over. This includes the provision of information, consultancy and test beds, and the organisation of activities to raise awareness, that are relevant for stakeholders such as ISPs, portals, companies and manufacturers.

- The IPv6 Commercial Services Support Council is regularly held to promote cooperation between the public and the private sectors; to share the outcome from the government's IPv6 business, understand the status of preparation by each stakeholder; and to address other challenges.

Way forward

After 2014 which can be called the First Year of IPv6 Services in Korea, to establish an IPv6 ecosystem comprising of networks (N), services (S) and devices (D), by working closely with various operators such as ISPs and CPs based on the implementation plan for IPv6 Roadmap, so that IPv6-based commercial services can continue to spread.

In particular, given that the preparation* of IPv6-based equipment that support IPv6 is practically completed, undertake to introduce IPv6-based content and services.

*Readiness ratio is the proportion of IPv6-compatible equipment out of total equipment, indicating the degree of convertibility to IPv6.

Category	2011	2012	2013	2014	2015
Backbone Network	90.6	91.2	92.1	94.7	95.3
Subscriber Network	18.2	19.0	65.0	68.9	78.6
User Device	-	-	68.4	89.8	95.3

Table 2 IPv6 Readiness Ratio - % of equipment that support IPv6. Source – Survey on Domestic IPv6 Readiness Ratio and Relevant Industries Status (Dec 2015)

2.5 New Zealand

Background

The New Zealand government supports the move from a dependency on IPv4 towards greater use of IPv6 in New Zealand. New developments such as 4G mobile services will require a greatly expanded Internet addressing space which cannot be accommodated with the very limited remaining number of IPv4 addresses available for general use.

In 2010, the Department of Internal Affairs identified that the New Zealand Government needed to transition to IPv6 so that New Zealand Government online (publically accessible websites) and All-of-Government cloud computing initiatives remained fully accessible and compliant with international standards.

The New Zealand government is taking a lead-by-example approach to IPv6 adoption. In 2015 the office of the Government Chief Information Officer released the

IPv6 for New Zealand Government guidance document.[6] The document outlines the New Zealand government's current IPv6 readiness:

- All of New Zealand's major peering exchanges are sharing IPv6 routes.

- The high-speed research and education network, Research and Education Advanced Network of NZ (REANNZ), has been IPv6 enabled since 2006.

- The government Domain Name System (DNS) was IPv6 enabled in February 2012, and was further enhanced through the addition of IPv6-ready DNSSEC in March 2015.

- New Zealand Government provides a range of ICT Common Capability All of Government (AoG) cloud computing services that are IPv6 ready, reducing the requirement and cost of individual agencies needing to implement IPv6 capabilities themselves.

Broad overview of IPv6 action plan

The IPv6 transition process is industry/market-led. The New Zealand government believes that the IPv6 transition should be achieved through the course of technology and application refresh cycles, planned system upgrades, or funded new capability project business cases.

The government is strongly supporting the adoption of IPv6 by New Zealand Internet Service Providers and website developers. The Industry and Government have raised awareness with New Zealand ISPs through an IPv6 taskforce. However, as with most governments worldwide, New Zealand consider that adoption should be encouraged but not mandated. The Industry and Government have worked together to raise awareness with New Zealand ISPs through an IPv6 taskforce.

The government is taking the following steps:

(i) Through the DIA, the government is providing leadership in the adoption and use of IPv6. DIA maintains the IPv6.govt.nz website and supports the use of dual stack (combined IPv4 and IPv6) access to its own and other government websites.

(ii) The Statistics New Zealand annual survey of New Zealand Internet Service Providers includes a set of questions relating to the provision of IPv6 and barriers to adoption.

[6] https://www.ict.govt.nz/guidance-and-resources/architecture/architecture-resources/internet-protocol-version-6-for-new-zealand-government/

As mentioned previously, Government Chief Information Officer released the IPv6 for New Zealand Government guidance document in 2015. This guidance states that:

- New Zealand Government publically accessible websites shall be IPv6-enabled and IPv4-capable where necessary;

- Transition of agency networks to IPv6 should only occur when all aspects of agencies' IT environments are fully capable of managing IPv6 traffic and addressing; and

- New Zealand Government operational systems and internal agency networks shall remain IPv4-enabled.

Strategic Thrusts

As noted above, the IPv6 transition is an industry led approach and progress is occurring steadily.

Most of the large carriers state they are IPv6 ready in their core networks, however, IPv6 is not typically offered to their residential or mobile customers. SNAP Internet (now owned by 2Degrees) and Orcon (now owned by Vocus) have a strong focus on IPv6 penetration. According to the Asia-Pacific Network Information Centre (APNIC) 56.84% of SNAP and 21.55% of Orcon user devices prefer to connect over IPv6.[7] Other organisations are progressing IPv6 deployment through technology and application refresh cycles

[7] APNIC Statistics as at 11 May, 2016: http://stats.labs.apnic.net/ipv6/NZ

State of Progress

Use of IPv6 in New Zealand is steadily, if slowly, increasing. APNIC measurements show IPv6 capability in the New Zealand and Australia sub-region of Oceania is at 3.43%, placing it in the middle of the pack within APEC.[8]

The table below provides data from Statistics New Zealand on the percentage of ISPs that have taken up IPv6 as of 30 June 2015.[9]

Timeframe	Percentage of ISPs[10]				
	2011	2012	2013	2014	2015
Already available[11]	30	33	33	52	48
Already available to all customers	…	…	…	17	20
Already available to some customers	…	…	…	26	20
Within the next 6 months	5	11	5	13	4
Between 6 months to a year	15	17	14	13	12
Between 1 to 2 years	25	28	19	22	20
Between 2 to 4 years	10	11	10	13	16
More than 4 years	0	0	0	0	1
No plans to make available	15	11	14	22	20
Did not respond	5	0	0	0	0

[8] APNIC Statistics as at 11 May 2016: http://stats.labs.apnic.net/ipv6/NZ

[9] Statistics New Zealand, 30 June 2015, at: http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/ISPSurvey_HOTP2015.aspx

[10] **Note:** All percentages are based on counts which have been randomly rounded to base 3. Therefore, the figures may not sum to 100 percent. Results should be treated with caution due to the small number of ISPs in some categories.

[11] Does not indicate that all Internet connections provided by these ISPs use IPv6, but that it is available through at least some of their connections.

The following table provided by Statistics New Zealand highlights the barriers to IPv6 deployment as of 30 June 2015.

Barrier	Percentage of ISPs[12]				
	2011	2012	2013	2014	2015
Lack of resources (cost / time)	36	50	54	50	43
Other business priority	36	58	54	58	43
Lack of vendor support	14	33	31	25	14
Lack of knowledge, education, training, and skills	14	17	23	25	14
Lack of user demand	43	75	62	67	79
Upstream transit (lack of capability with connection provider)	14	17	23	17	14
Interoperability (equipment not compatible)	29	42	31	33	14
Other	14	8	8	0	14
Did not respond	0	0	0	0	0

While there is some distance to go, the government is confident that IPv6 adoption will continue to progress through the course of technology and application refresh updates.

2.6 Singapore

Background

Singapore had anticipated that the rate of IPv4 free pool address consumption in 2009 would lead to an accelerated exhaustion of addresses available. Following a public information paper published by the Infocomm Development Authority of Singapore (IDA)[13], in 2006 to promote nationwide IPv6 transition, an IPv6 taskforce was formed in September 2006 to address the issue of IPv4 exhaustion and to facilitate the smooth transition of the Singapore Infocomm ecosystem to IPv6.

[12] **Note:** The percentages reflect only the responses from those ISPs that do not have IPv6 available through any of their connections. All percentages are based on counts which have been randomly rounded to base 3. In addition, categories are not mutually exclusive. Therefore, the figures sum to more than 100 percent. Results should be treated with caution due to the small number of ISPs in some categories.

[13] IDA was restructured to form the Info-communication Media Development Authority (IMDA) and Government Technology Agency on 1 October 2016

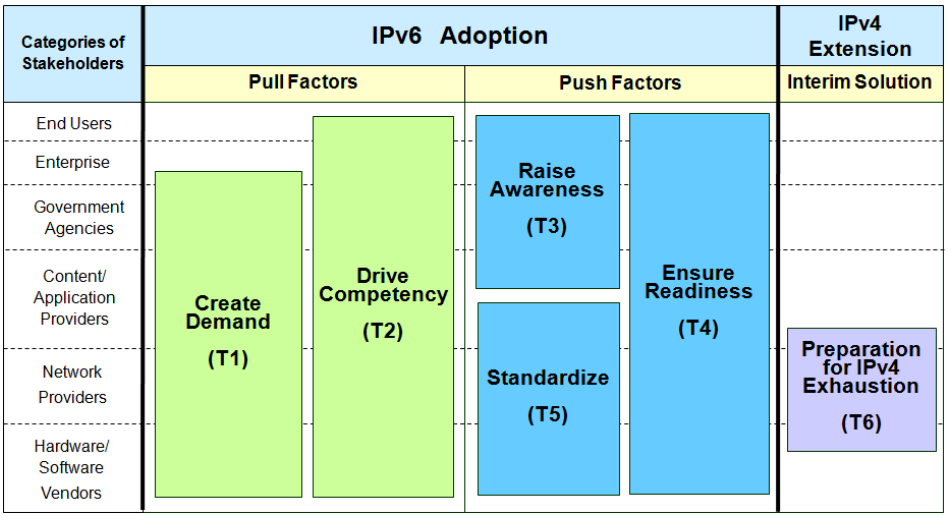
First Steps

The IPv6 Transition Programme, initiated in 2010, involved a two-pronged approach to drive domestic IPv6 adoption as well as to encourage the efficient use of the remaining pool of IPv4 addresses to slow down the rate of depletion. Under the programme, IDA embarked on a series of activities including IPv6 awareness drive and industry engagements to ensure that the Singapore Infocomm ecosystem will be prepared for a smooth transition to IPv6.

IPv6 Adoption

The IPv6 Adoption approach was executed over the course of three years and comprised both "push-inclined" and "pull-inclined" programmes to encourage the planning for transition to IPv6. This increased readiness allowed for faster response in the event of IPv4 exhaustion. There were five thrusts under IPv6 Adoption approach (T1-T5) and an interim solution under IPv4 Extension approach (table below). Each thrust aimed to achieve different market effect, but complemented each other. The thrusts were:

T1: To create demand for IPv6,
T2: Drive competency of the workforce to support the transition to IPv6,
T3: Raise awareness of the impending IPv4 exhaustion and its implications,
T4: Ensure the readiness of stakeholders in the transition,
T5: Ensure IPv6 / IPv4 performance equity to ensure IPv6 performance becomes more equitable to IPv4 over time, and
T6: Manage IPv4 exhaustion to assist players to extend their IPv4 address availability until their planned IPv6 adoption.



- Create Demand for IPv6 (T1)

This was a key thrust to create a “pull” effect on the ecosystem towards IPv6. Availability of market demand for IPv6 products and services was a key impetus to IPv6 Adoption. We leveraged upon the large purchasing power of the Singapore Government as a catalyst to create significant market demand for IPv6 to spur the market. For example, IDA mandated that Singapore government agencies procured only IPv6-ready equipment and encouraged them to enable IPv6 for public facing e-services. According to actual agencies’ declarations in 2014, 50% of public facing e-Services were at least 75% IPv6 ready. Further, IDA mandated the inclusion of IPv6 requirements into key IDA programs such as Next Generation Internet programs. This initiated business continuity planning, such as requiring the Operating Company to aggregate RSP’s IPv4 requirements to ease application for IPv4 address allocation.

Financial incentives were also provided to encourage the availability of IPv6-based services like the provision of IPv6-ready websites. The financial incentives only addressed the additional cost incurred due to the inclusion of the IPv6 capability. Some of the top internet traffic websites such as JobStreet, Streetdirectory, sgCarMart, Propertyguru and SingTel have enabled IPv6 under the IDA’s incentive programme and are already serving their IPv6 customers.

- Drive Competency (T2)

IPv6 skills are necessary to support this transition. Besides integrating IPv6 components into existing nationwide infocomm competency frameworks, IPv6 components were also incorporated into course curriculum at Singapore universities and other institutes of higher learning.

IDA, with the assistance of a training provider, has trained 300 professionals from the industry and more than 6,000 students from institutes of higher learning in IPv6. The supply of local talent pool would ensure that companies can find sufficient qualified professionals to implement IPv6 transition and hence would be less reliance on foreign manpower / services. The trained professionals from the industry received the globally recognized certification from IPv6 Forum.

To further stimulate interest and to promote creativity around the use of IPv6 for the students, an “IPv6 Innovation Challenge” was held for the students of institutes of higher learning. With the support from IPv6 Forum Singapore, this contest received various proposals and created good traction among the students.

- Raise Awareness (T3)

IDA was cognizant of the need to increase awareness of IPv4 exhaustion and its implications. The approach adopted was measured to avoid any unnecessary panic. A top-down approach was taken with proactive engagement through briefings and conferences organised with the support of the Internet Society and IPv6 Forum with a more passive approach taken towards the members of the public.

a. Executive Briefing(s)

Host an annual ½-day Executive Briefings at IDA once every 2 years. The target audiences are the senior leadership teams, agencies' Chief Information Officers and local industry leaders.

b. Conferences

Host a 2-day IPv6 conference/workshop once every 2 years, from 2010 to 2012. The target audiences were content providers, government agencies and enterprises.

c. Micro-site

Develop a micro-site as part of IDA corporate website, providing dynamic information such as IPv4 Address Exhaustion Counter and IPv6 Checker, event calendars, and program updates. The micro-site was also aligned with One-stop Knowledge Centre (developed under previous thrust) to offer IPv6 knowledge such as webinars, online presentations and technical sharing.

This website was then advertised to the users through IDA People Sector Enrichment program.

- Ensure Readiness (T4)

In encouraging the ecosystem towards IPv6 adoption, IDA wanted key stakeholders to be equipped to respond in the event of IPv4 Address Exhaustion. Efforts included engaging IPv6 experts to develop authoritative Reference IPv6 Transition Plans for each category of stakeholders, developing IPv6 test programmes to assist stakeholder's readiness implementation. Lastly, the National Internet Measurement Infrastructure was upgraded to measure IPv6 traffic.

- Ensure IPv6 / IPv4 performance equity (T5)

The objective of this thrust was to ensure IPv6 performance would become more equitable to IPv4 over time, given the maturity of IPv4-based services vis-a-vis IPv6-based services. On completion of the assessment on the performance comparison between IPv4 and IPv6, initial results showed that IPv6 throughput for data upload and download were better than that for IPv4 throughput in the overseas Internet traffic. However, for the local Internet traffic, the performance between IPv4 and IPv6 was similar

- Preparation for IPv4 Exhaustion (T6)

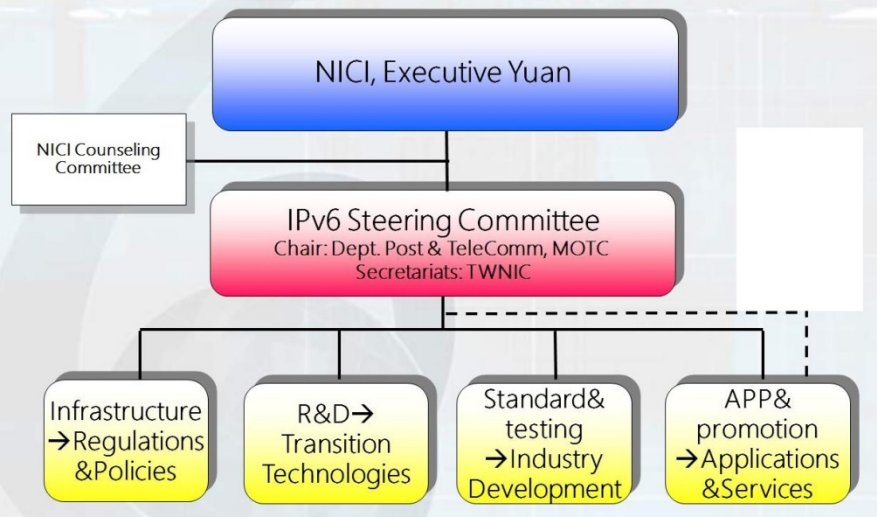
It was anticipated that despite the proactive IPv6 programmes rolled out, IPv4 would continue to exist due to legacy systems. This thrust was a defensive approach to ensure that Singapore could rapidly seize advantage of any policy changes that freed up more IPv4 addresses. In addition, this approach encouraged network providers to proactively manage their IPv4 address pool. To do so, industry

engagement was carried out to influence key industry partners to proactively manage their pool of IPv4 addresses. IDA monitored global IPv4 policy developments closely as well.

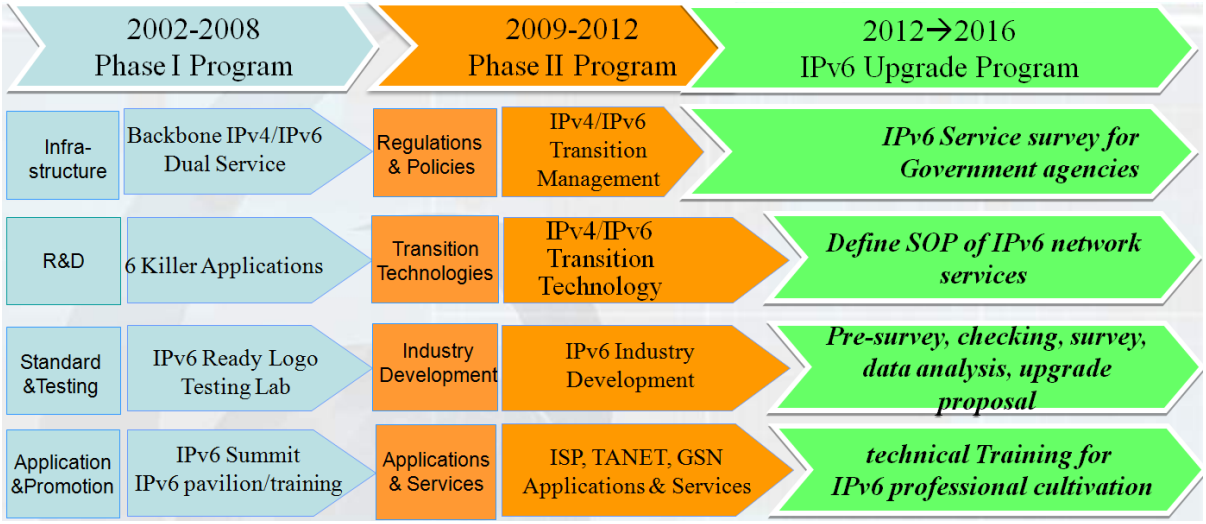
2.7 Chinese Taipei

Background

Chinese Taipei began planning for the forthcoming depletion of IPv4 addresses and the seamless transition to IPv6 in 2002 when the National Information and Communications Initiative (NICI) Committee of the Executive Yuan established a working group to promote the IPv6 network. The following year, the Directorate General of Telecommunications launched a five-year initiative entitled "*National IPv6 Deployment & Development Program.*" The Ministry of Transportation and Communications then launched the Interoperability and Accreditation of Next Generation Internet Project running from 2009 to 2012 and the IPv6 upgrade and promotion program from 2013 to 2016.



The IPv6 Program Framework of Chinese Taipei



The Roadmap of the IPv6 Program of Chinese Taipei

Overview of IPv6 Action Plan and Strategies

Facing the approaching exhaustion of IPv4 addresses and the growth of IPv6 services, the Executive Yuan, on 30 December 2011, approved the "*Internet Protocol Upgrade and Promotion Program (IPv6 UP)*" and on 30 January 2012, accordingly established, under the National Information and Communications Initiative Committee, the IPv6 Upgrade Promotion Office, which has been actively promoting government-wide upgrade of IPv6 since then.

According to the program schedule, fifty percent of external services, including the websites of government agencies, DNS, email and major international services would be upgraded to IPv6 by the end of 2013, and the remaining fifty percent by the end of 2015. As for internal services, the upgrade of IPv6 would begin in 2016.

IPv6 Adoption

Due to the increasing speed at which IPv4 addresses were depleting, finding a feasible approach that could ensure a smooth and steady upgrade to the IPv6 network environment became a major issue. The solution for the best approach to solve the issue was to prioritize the upgrade to IPv6 of government agencies. The decision to do so was based on the following reasons: first, it is much easier to conduct IPv6 transition of the government network services running from a top-down manner than commercial ISPs. Second, the knowledge and experience gained from the government IPv6 transition can help the industry realize the business opportunities of developing innovative applications and services. The third is that the budget can be more easily determined based on the existing or future investment in equipment.

- Government's Initiative

The strategies below have been implemented in accordance with the schedule of the IPv6 UP program with the aim of efficiently promoting the IPv6 upgrade and developing the IP network:

Strategy 1: Undertake surveys to determine problems and difficulties.

Strategy 2: Define the standard operating procedure (SOP) of the IPv6 upgrade for major Internet services.

Strategy 3: Encourage ISPs to provide dual-stack for IPv6 network connection.

Strategy 4: Facilitate technical training courses to cultivate greater IPv6 expertise.

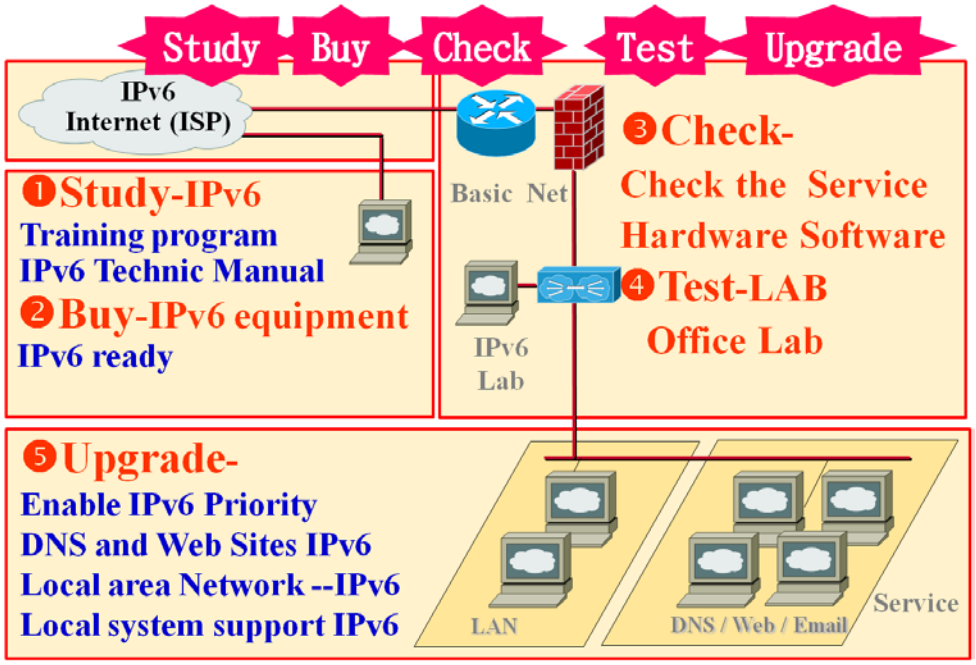
- Building an IPv6 upgrade model based upon cost-effective strategies

When a party undertakes plans for the IPv6 upgrade, the concerted effort of different organisations is required to determine priorities of the upgrade among the provided services according to the degree of necessity, the difficulty, and the annual budget of the software/hardware procurements.

As already briefly mentioned, our approach was first to upgrade the external network services of governmental agencies nationwide as the driving force of the upgrade and second put in place cost-effective strategies. Therefore, a two-stage IPv6 upgrade model was adopted to undertake IPv6 upgrade progressively according to the defined priority of the governmental organisation.

The first stage was to conduct a service-based survey, consisting of six steps: preparation, launch, pre-survey trial, checking, survey, and summarization. These six steps provide the required preparation for the IPv6 upgrade. For this stage, the survey proposed the strategy using a small-scale trial survey to a full-scale survey strategy in order to determine the challenges and issues of IPv6 deployment.

The second was the adaptive upgrade stage, consisting of four steps: organize sixteen support teams, facilitate technical training courses to cultivate greater IPv6 expertise, create an FAQ and case base, and progress tracking and monitoring. These steps focused on the user-oriented strategy. For this stage, providing adaptive upgrade support or solution for different services according to the results of the survey is a key factor. Hence, sixteen IPv6 supporting teams consisting of forty university professors and experts have been formed to assist organisations with the IPv6 upgrade.



Step by Step for IPv6 Network upgrade

This IPv6 upgrade model has already been successfully implemented on our Government Network Services. Using this model, we can cost-effectively handle large numbers of network services in the IPv6 upgrade. Up until 31 December 2015, 4,568 (100%) services had upgraded completely to IPv6. The Government's internal network service began its upgrade to IPv6 this year (2016).

- Technical training courses

Considering the cost and demand of training for the IPv6 upgrade, both real and virtual experimental models were integrated establishing a Multi-level Training Mechanism (MTM) to improve the learning effectiveness of the student and reduce costs of the implementation. An IPv6 virtual lab was constructed with a Multi-level Training Mechanism (MTM) consisting of three levels: basic training, simulation-based training, and virtual-machine-based hands-on training.

The first level of basic training provided the web courseware and its related quizzes for the novice to gain basic IPv6 knowledge. The simulation-based training of the second level uses Web-based Assessment Virtual Experiment (WAVE) to provide trainees with the virtual operation and their personalized diagnostic results for their learning problems. The third level training, the virtual-machine-based hands-on training, uses the Virtual-Machine-Based Hands-on Experiment in the cloud to offer a practical IPv6 environment for the technical engineer or the user who is in interested in the practical operation. This training mechanism not only minimizes face-to-face training, but also provides personalized diagnosis.

The designed courseware trains students according to their aptitudes by integrating multi-level IPv6 upgrade training courses with the assistance of learning diagnosis systems to offer the most suitable training approach according to the diverse requirements of trainees. Consequently, the training costs and required resources based on our MTM are reduced and expertise can be enhanced. This IPv6 virtual lab has already demonstrated its cost-effectiveness, and provides adaptive learning to help many users with different technical capabilities simultaneously. By the end of 2015, a total of 124 seminars and training sessions for government employees had been held serving more than 5,500 attendees.

- Promotion of the IPv6 CE router/Ready Logo for IPv6 equipment vendors

The IPv6 Ready Logo Program organized by the IPv6 Forum is a conformance and interoperability testing program intended to increase user confidence by demonstrating that IPv6 is available now and is ready to be used.

The IPv6 Ready Logo Committee's mission is to define the test specifications for IPv6 conformance and interoperability testing, provide access to self-test tools, and to deliver the IPv6 Ready Logo kicked-off in 2003. The Chunghwa Telecom-Telecom Laboratory (CHT-TL) IPv6 Testing Lab of Chinese Taipei officially became one of its 5 founding members.

The CHT-TL has participated as part of the "*National eTaiwan*" project since 2004. It is working for MOTC/TWNIC National IPv6 Deployment and Development Project which is responsible for carrying out standards and testing division to help domestic IPv6 equipment vendors sustain IPv6 technology competitiveness for next generation internet communication needs.

In Chinese Taipei, Information and Communication Technology (ICT) products were provided with assistance to apply for the International IPv6 Ready Gold Logo. As of 31 December 2015, 296 ICT products had been accredited with the IPv6 Ready Gold Logo (Phase 2), including 28 new additions in 2015. Chinese Taipei now ranks second in terms of the number of IPv6 Ready Gold Logo (Phase 2).

- Studies of IPv6 creative applications

Clearly, the IPv6 network is a key platform to develop new applications. As such, both network-related research and program should support IPv6. Some IPv6 applications that Chinese Taipei is interested in and has researched include

a. Internet of Things

b. Smart Home -Security Health

c. Smart Vehicle System

d. Smart Sensor Application

e. Point to Point, Sensor network

f. Mobile communications

g. Network TV

h. Cloud Applications

Challenges

Promotion of IPv6 upgrade in ISPs

Ten commercial ISPs currently operate in Chinese Taipei – all of which have deployed an IPv6 backbone. IPv6 Tunnel Services have been provided by major ISPs (HiNet, Sparq, SONET, APOL, TFN) since 2007. Chung-Hwa Telecom (HiNet) have provided IPv4 and IPv6 dual stack NGN (FTTX) services since 2011 and launched the online application of the IPv6 connection in March 2015. However, ISPs and ICPs should continually promote the upgrade of network services to IPv6 so that their subscribers can connect to the international IPv6 network.

Competency

Although the IPv6-enabled Home Gateway can support both IPv4 and IPv6 network access services at home, the Home Gateway lacking the function to support IPv6 has been a main factor impeding the ubiquity of IPv6. According to the market research undertaken in Chinese Taipei, many users still use the home gateway without IPv6 support. Hence, educating the public to buy an IPv6-enabled Home Gateway remains a key issue.

Security

While having a large number of IP addresses benefits companies from a management point of view, it also benefits cyber criminals. Although the majority of security professionals and networking engineers are mostly familiar with protecting IPv4 networks, their experience and skills in protecting IPv6 networks still need to be enhanced.

2.8 Thailand

Background

On 4 June 2013, the Thai cabinet approved the IPv6 Action Plan (2013-2015) which mandates all government agencies and service providers to start preparing their infrastructure and services to support IPv6. To this end, the IPv6 coordination and operation centre was established to provide guidance and technical assistance on IPv6 migration. Since 27 August 2013, the centre has been advising agencies on how to migrate their web, mail and DNS services to IPv6. In addition, the centre has developed tools to help IT personnel check and monitor their IPv6 connectivity. The centre has also created and distributed guidelines for specifying IPv6 support on computers, accessories, network equipment, enterprise software and IT systems.

On 1 December 2015, the Thai Cabinet approved the Action Plan for the mobilization, promotion, acceleration, and follow up of IPv6 in Thailand: Phase 2

(2016-2018), and appointed the Ministry of Information and Communication Technology (MICT) as the main agency to oversee its implementation. MICT is responsible for requesting for IPv6 numbers from the Asia Pacific Network Information Centre (APNIC) for governmental and related agencies. Concerned agencies are assigned to implement activities specified in the Action Plan (2016-2018).

Broad overview of IPv6 action plan/strategies

The MICT is authorized to act as the main agency to oversee the implementation of the IPv6 Action Plan (2013-2015), with the cooperation of the relevant agencies such as Electronic Government Agency, IPv6 Forum Thailand NECTEC and Prince of Songkla University (PSU).

Strategic Thrusts

The National IPv6 Thailand Master Plan (Action Plan Phase 2 (2016-2018)

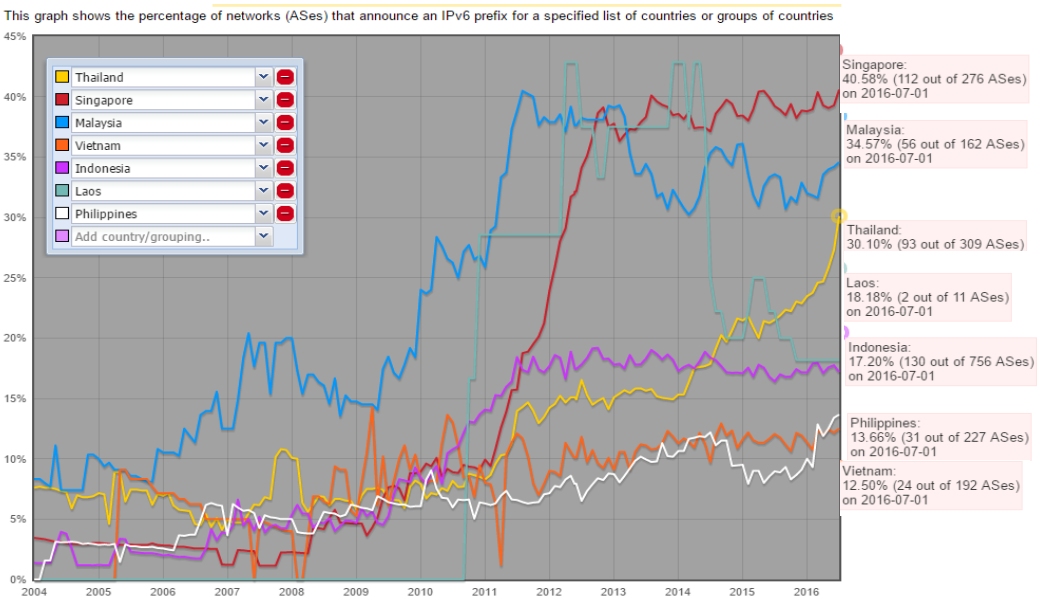
On December 1, 2015 the Thai Cabinet approved the three-year National IPv6 Action Plan Phase 2 (2016-2019). There are four strategic thrusts under the Action Plan:

1. IPv6 Infrastructure
2. Human Development
3. Services and Supports
4. Public Awareness

State of Progress

Since 1 January 2016, the IPv6 coordination and operation centre has been advising agencies on how to migrate their web, mail and DNS services to IPv6. The centre provides more than 430 consulting services by phone, email, and site visits. In addition, the centre has developed tools to help IT personnel check and monitor their IPv6 connectivity. Moreover, the centre has created and distributed guidelines for specifying IPv6 support on computers, accessories, network equipment, enterprise software and IT systems.

The Commission Policy plans to propose IPv 6policies to contribute to the goals of the Action Plan. MICT will also host an IPv6 seminar 2016, to promote awareness and provide training on the utilization of IPv6. It would cover topics such as the status and progress of IPv6 deployment, and reward organisations that have succeeded in doing so . The seminar is targeted at government units, public organisations, state enterprises, and public universities.



ที่มา http://v6asns.ripe.net/v/6

2.9 United States

Background

The United States is one of the world's leading countries in IPv6 traffic levels and adoption. According to the Asia-Pacific Network Information Center (APNIC), the United States is the top-ranking member economy in terms of the population of estimated IPv6 users,[14] and second only to Belgium in overall deployment.[15]

Public Sector (Federal Government)

In February 2003, the National Strategy to Secure Cyberspace called on the United States to identify a process for the IPv6 transition.[16] The strategy recognized

---

[14] Geoff Huston, *An Update on IPv6*, APNIC (June 16, 2015), http://blog.apnic.net/2015/06/16/an-update-on-ipv6/.

[15] *Id.* Recent estimates as to the percentage of U.S. end-users actively using IPv6 vary slightly. Compare i*d.* (estimating deployment at 22.21%), *with* Akamai, *State of the Internet: IPv6 Adoption Visualization* (Apr. 23, 2016), https://www.akamai.com/uk/en/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp (estimating deployment at 18.6%), *and* Google IPv6, *Per-Country IPv6 Adoption*, https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption (last visited May 6, 2016) (estimating deployment at 25.67%).

[16] The White House, The National Strategy to Secure Cyberspace at 30 (Feb. 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

that the shift to IPv6-based infrastructure must stem from a thorough understanding of the benefits and challenges of the transition, and noted that "the federal government can lead in developing this understanding by employing IPv6 on some of its own networks and by coordinating its activities with those in the private sector."[17] To this end, the strategy directed the Department of Commerce to establish a task force to examine IPv6 issues.[18]

In January 2006, following extensive consultations with public and private sector stakeholders, the IPv6 Task Force released its final report.[19] Among other findings, the report concluded that market forces should drive the private sector transition from IPv4 to IPv6. The report also determined, however, that the government has an important role to play as a major consumer of IPv6 products and services, and can lead by example as an early adopter of IPv6.[20]

The efforts of the Task Force coincided with concurrent policy guidance from other government agencies.[21] In particular, the Office of Management and Budget (OMB) outlined a series of steps to guide the IPv6 transition within federal networks. In August 2005, OMB initiated the transition planning process by specifying a timeline for federal agencies to demonstrate IPv6 readiness, culminating with the requirement that agencies support IPv6 capability on their backbone networks by June 30, 2008.[22]

Subsequently, in September 2010, the Federal Chief Information Officer (CIO) issued a memorandum expressing the federal government's commitment to the operational deployment and use of IPv6. To facilitate timely and effective IPv6 adoption, the memorandum gave federal agencies two deadlines: to upgrade public/external facing servers and services (e.g., web, email, DNS, ISP services, etc.) to IPv6 by the end of fiscal year 2012, and to upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to IPv6

---

[17] *Id.*

[18] Issues included "the appropriate role of government, international interoperability, security in transition, and costs and benefits." *Id.*

[19] *See* IPv6 Task Force, Technical and Economic Assessment of Internet Protocol Version 6 (IPv6) (Jan. 2006), https://www.ntia.doc.gov/files/ntia/publications/ipv6final.pdf.

[20] *Id.* at 56.

[21] *See, e.g.*, U.S. Gov't Accountability Office, GAO-05-471, Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks (May 2005), http://www.gao.gov/new.items/d05471.pdf (recommending that federal agencies begin to address key IPv6 planning considerations and take immediate steps to handle near-term security risks).

[22] Office of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-05-22 (Aug. 2, 2005), https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf.

by the end of fiscal year 2014.[23] In order to support agencies in achieving these objectives, the Federal CIO Council developed a "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government," which provides actionable best practice guidelines for implementing IPv6.[24]

The National Institute of Standards and Technology (NIST) tracks estimated IPv6 deployment across the U.S. government.[25] To assist agencies in acquisition and to protect investments made by early USG adopters, NIST developed a standards profile for IPv6 products: "A Profile for IPv6 in the U.S. Government"[26] NIST, in collaboration with the IPv6Forum developed a IPv6 product testing program, implemented by accredited 3rd party test labs that insures the conformance and interoperability of IPv6 products. See: "USGv6 Test Methods: General Description and Validation"[27] and "USGv6 Tested Devices."[28]

There is little inherently governmental about the NIST profile and test programs, such that other public and private institutions can, and have, leveraged components of this program. NIST makes public summary statistics from its surveys of .com, .gov. and .edu space.[29]

Private Sector (Industry)

In addition to focusing on its own internal transition to IPv6, the federal government has engaged in information-sharing and consumer outreach.[30] For example, the National Telecommunications and Information Administration (NTIA) has developed the IPv6 Readiness Tool, a comprehensive checklist to assist businesses

---

[23] Office of Mgmt. & Budget, Exec. Office of the President, Memorandum for Chief Information Officers of Executive Departments and Agencies: Transition to IPv6 (Sept. 28, 2010), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf.

[24] Fed. CIO Council, Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government (July 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf.

[25] *See* NIST, *Estimating USG IPv6 & DNSSEC External Service Deployment Status*, http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov (last visited May 17, 2016).

[26] http://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf

[27] http://www-x.antd.nist.gov/usgv6/docs/NIST-SP-500-273.v2.0.pdf

[28] https://www.iol.unh.edu/registry/usgv6

[29] http://fedv6-deployment.antd.nist.gov/snap-all.html

[30] *See* IPv6 Task Force, *supra* note 6, at 57 (Jan. 2006) (identifying the government's key role in information-sharing and consumer outreach).

in preparing to deploy and adopt IPv6,[31] and the Federal Communications Commission (FCC) has released an IPv6 Consumer Guide.[32]

By and large, however, strong IPv6 adoption in the United States has been driven by network providers, with the top three broadband operators (Comcast, AT&T, and Time Warner Cable) and the four national mobile operators (Verizon, AT&T, Sprint, and T-Mobile) all actively rolling out IPv6 to their end users.[33]

In July 2014, for example, Comcast became the first major U.S. internet service provider to deploy dual-stack connectivity over 100% of its network.[34] As of September 2015, more than 70% of Comcast broadband customers were actively provisioned with IPv6 support, and over 15% of Comcast's Internet traffic was over IPv6.[35]

Due to the challenges inherent in dual-stack configuration, many U.S. companies have started to deploy IPv6-only networks.[36] All of Comcast's products and services have plans, or have already begun preparations, to support IPv6 only.[37] Similarly, in the mobile arena, T-Mobile has pioneered the deployment of IPv6-only on its handsets.[38]

---

[31] NTIA, Dep't of Commerce, *IPv6 Readiness Tool for Businesses* (Apr. 8, 2011), https://www.ntia.doc.gov/other-publication/2011/ipv6-readiness-tool-businesses. *See also* NTIA, Dep't of Commerce*, About the IPv6 Readiness Tool* (Apr. 8, 2011), https://www.ntia.doc.gov/other-publication/2011/about-ipv6-readiness-tool (providing background information on the tool).

[32] *See* FCC, *Consumer Guide: Internet Protocol Version 6 (IPv6)*, https://transition.fcc.gov/cgb/consumerfacts/ipv6.pdf (last visited May 9, 2016).

[33] *See* Erik Nygren, *Three Years Since World IPv6 Launch: Strong IPv6 Growth Continues*, AKAMAI (June 8, 2015), https://blogs.akamai.com/2015/06/three-years-since-world-ipv6-launch-strong-ipv6-growth-continues.html.

[34] *See* John Brzozowski, Comcast, *Comcast Reaches Key Milestone in Launch of IPv6 Broadband Network* (July 22, 2014), http://corporate.comcast.com/comcast-voices/comcasts-xfinity-internet-now-the-worlds-largest-native-ipv6-deployment.

[35] *See* John Brzozowski, Comcast, *IPv4 Depletion Not the Beginning of the End, It's Just the End of the Beginning* (Sept. 24, 2015), http://corporate.comcast.com/comcast-voices/ipv4-depletion-not-the-beginning-of-the-end-its-just-the-end-of-the-beginning.

[36] *See* Nygren, *supra* note 16.

[37] *See* Brzozowski, *supra* note 18.

[38] *See* Andrew McConachie, Internet Soc'y, *Case Study: T-Mobile US Goes IPv6-Only Using 464XLAT* (June 13, 2014), http://www.internetsociety.org/deploy360/resources/case-study-t-mobile-us-goes-ipv6-only-using-464xlat/.

Chapter 3. Trends in IPv6 Adoption in APEC Economies

3.1 Overview

In general, most APEC economies that have provided inputs to this paper have gone above and beyond the guidelines set out in the 2010 APEC TEL IPv6 Guidelines. The governments of the economies in this paper recognised the need to exercise leadership in the deployment of IPv6 capabilities and the need for private sector involvement in one way or another. Through varying degrees of collaborative efforts across sectors to coordinate national deployment strategies, APEC economies have embarked on their respective IPv6 strategies having assessed their economies' technical infrastructure and human capacity needs. APEC economies have also demonstrated their willingness to work with experts from the private sector, the Internet technical community and academic institutions in various stages of their deployment strategies. Observed trends in the nine economies' IPv6 case studies are highlighted below.

3.2 Leading by Example

The key trend in the deployment strategies of all nine case studies in APEC is that the governments of these nine APEC economies had chosen to lead by example in pushing for IPv6 adoption. Most governments had taken the initiative to study the issue and came to their own conclusion on the need for a coordinated approach with the government taking the lead. Efforts to coordinate a whole-of-government approach through a concerted roadmap or strategy paper was a common approach that ensured government agencies worked toward achieving their milestones. While APEC economies differed in the level of involvement of the industry in coming up with an IPv6 deployment strategy, governments generally took the first step in their overall strategies.

This could be explained by the following. First, with the government's large purchasing power, it could drive demand for IPv6-ready equipment and in turn, could spur market supply and eventual take-up of IPv6-ready equipment in the private sector. Some economies went the extra step of mandating IPv6-ready equipment in their procurement principles. For example, Australia ensured that their federal agencies were allowed to procure IPv6 equipment when they first embarked on their federal IPv6 deployment strategy. In Republic of Korea, its e-Government Network made IPv6 a mandatory requirement in all requests for proposals.

Second, the central government would be in the best position in terms of availability of resources to coordinate a nationwide approach. Most economies described embarking on surveys or studies in order to assess the best way to coordinate a deployment strategy. More often than not, the conclusions of such assessments specified that the government had an important role to play in the deployment strategy. The Authority for Info-communications, Technology Industry of

Brunei Darussalam (AITI) published an assessment report[39] in May 2010 which analysed the IPv4 depletion issue and the case for IPv6 adoption. In the US, it was recognised that the move from IPv4 to IPv6 should be based on thorough understanding of the transition and noted that "the federal government can lead in developing this understanding by employing IPv6 on some of its own networks and by coordinating its activities with those in the private sector." The resulting study[40] on this transition concluded that the US government had an important role to play as a major consumer of IPv6 products and services, and can lead by example as an early adopter of IPv6.

3.3 Engaging the Private sector

On one end of the spectrum, some APEC economies have chosen to leave the industry largely to its own devices in the transition to IPv6. These APEC economies like the Hong Kong, China and the United States have achieved high rates of IPv6 deployment in their private sector. Most of their efforts were focused on ensuring that their government infrastructure was IPv6-ready. However, it is noted that there was some effort taken to encourage the private sector to take action. From organising IPv6 awareness campaigns to developing IPv6 standards replicable in the private sector, their efforts are examples of the types of private sector involvement and collaboration that governments can employ.

For Hong Kong, China, an awareness campaign was undertaken in 2011 by the government targeting SMEs as well as the public sector. Through the setting up of a website on IPv6, use of collaterals like promotion pamphlets, consumer guides and events like radio programs and seminars, the project aimed to provide a better understanding of the IPv4 address space exhaustion situation as well as to educate SMEs and consumers on IPv6.

In the United States, their government agency responsible for standards sought to develop a standards profile for IPv6 products in the US government. The US government agency collaborated with the IPv6 Forum to develop an IPv6 product testing programme that looks into the conformance and interoperability of IPv6 products. Such a tool could easily benefit the private sector that could be used to advance their IPv6 readiness as well.

On the other end of the spectrum, there are economies who have taken a more developmental approach in leading the industry to plan and achieve IPv6 readiness. In Singapore, besides having run several initiatives to create awareness of IPv6 readiness in the private sector, the government launched an IPv6 website seeding programme to provide financial incentives to businesses to offset the additional costs incurred from upgrading their websites to be IPv6-ready. In encouraging the ecosystem towards IPv6 adoption, IPv6 experts developed Reference IPv6 Transition Plans for each subset of stakeholders e.g. ISPs, network providers, service providers

[39] Brunei Darussalam's IPv6 Status Quo & Readiness Assessment

[40] *See* IPv6 Task Force, Technical and Economic Assessment of Internet Protocol Version 6 (IPv6) (Jan. 2006), https://www.ntia.doc.gov/files/ntia/publications/ipv6final.pdf.

and end users. IPv6 test programmes were developed to assist stakeholder's IPv6 readiness as well.

In Republic of Korea, the collaborative spirit between the government and the private sector had resulted in positive outcomes. Consultation efforts by the government to understand the interests of the private sector in IPv6 deployment paved the way for a Private Sector/Government collaboration that helped to launch commercial IPv6 services across the board including mobile devices like smartphones, to network (LTE) and content. Building on such collaborative engagements, the Korean government took the approach of sharing their IPv6 deployment experience with the private sector to minimise resource wastage.

3.4 Task Force Action/Coordination centres

APEC member economies found that setting up task forces and/or coordination centres was a useful way carryout whole-of-government IPv6 deployment strategies. These task forces and coordination centres served the purpose of pulling together and focusing efforts in their deployment strategies.

Thailand had set up its IPv6 Coordination and Operation Centre following the mandate given by the Thai cabinet to prepare for IPv6 deployment. Besides providing guidance and technical assistance on Web, mail and DNS services migration to government agencies, the Centre developed tools to help IT personnel monitor their IPv6 connectivity. It was reported that more than 430 consulting services by various means including site visits were conducted by the Centre over a six-month period.

Brunei Darussalam established an IPv6 Committee comprising of representatives from ISPs, government agencies and Brunei Darussalam's AITI. The Committee ensured that all updates, strategies and plans relating to IPv6 were communicated to government agencies. Besides assisting in coordination and technical aspects of the transition, task forces and coordination centres were useful in educating the public and industry of IPv6 transition. This was evident in New Zealand as well. Its IPv6 task force worked with industry and the New Zealand government to raise awareness of IPv6 transition to ISPs. Similar task forces were established in Australia, Chinese Taipei, the United States and in Singapore.

3.5 Training

Several economies recognised that in order to support the transition, skilled personnel played a vital role in an IPv6 ecosystem. Chinese Taipei embarked on a training approach that consisted of both real and virtual experimental models to build up a "Multi-level Training Mechanism". This was done with the goal to improve the efficacy of the training sessions and to keep costs low. An IPv6 virtual lab was used which allowed three levels of training: basic, simulation-based and virtual-machine-based hands-on training.

Economies made concerted efforts in building up IPv6 skillsets in order to prepare for the future. Brunei Darussalam focused on IPv6 training courses and awareness programs. For Singapore, besides ensuring that IPv6 components were included in existing nationwide infocomm competency frameworks, IPv6 components

were also incorporated into course curriculum at Singapore universities and other institutes of higher learning. Australia reported that whole-of-government IPv6 training curriculum for agency managerial and technical staff were organised where necessary. A reported key element of their IPv6 strategy was the technical training catered for agencies that ensured continuity of services while transitioning. The training covered topics such as security, address space management and general IPv6 issues.

3.5 Conclusion

The extensive planning carried out by member economies as part of their IPv6 deployment strategy reflects the high commitment level by their governments in ensuring that their networks and infrastructure are IPv6 ready. Many case studies detailed coordination efforts between multiple agencies across central governments and for some, with the private sector as well.

Most if not all case studies saw governments expanding on the general roadmap proposed by the APEC TEL IPv6 Guidelines to address their needs. The Guidelines comprise broad brushstrokes of a multi-stakeholder strategy that governments who have yet to embark on their IPv6 rollout can base their strategy on. As evident from the nine case studies here, governments need to have a clear policy and strategy to catalyse IPv6 adoption.

As a baseline, many economies' IPv6 deployment strategy was to ensure that all public/external facing servers and services under the government use IPv6. In addition, some anticipated the need to sustain IPv4 network traffic for a while. As evident from these case studies, given the inherent differences in each economies' ICT infrastructure, adequate preparation is needed.

The transition from IPv4 to IPv6 has to be completed in order to support the growth of the Internet. APNIC had reached its last block of IP addressed in April 2011.[41] APEC TEL economies are committed to this transition to enhance online connectivity, with this being one of the goals included in the APEC TEL Strategic Action Plan 2016-2020. Completing the rollout of IPv6 supports the key infrastructure upgrades that many APEC economies are currently pursuing in their race to achieve sustainable economic growth through ICT.

***

[41] https://www.apnic.net/community/ipv6-program/messages