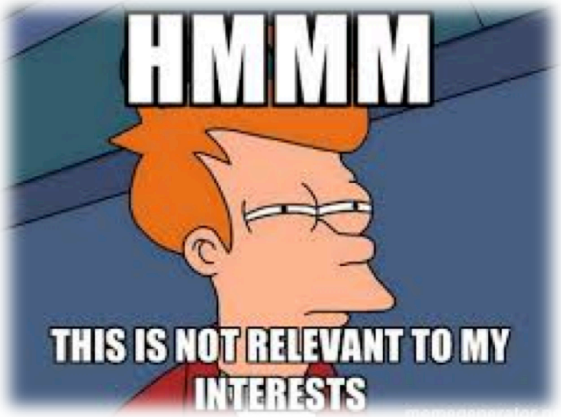
Migration to IPv6 - Bhutan: Policy and Regulation

IPv6 migration : *The Why? questions of stakeholders*



Business continuity (esp. 4G, IoT)
IPv6 in IPv4 only network (Security risks)
Economic decision – Invest in IPv6 Vs Prolong IPv4
IPv6 is growing rapidly
Resources and best practices available
Policy and regulatory support

Convincing decision makers in stakeholders – A major challenge

Who are these stakeholders?

-Ministry, Regulatory authority, e-Government agencies, Telecom service providers, Content developers and providers, Standardization agencies, IP address allocation agencies, Development agencies, Academia and Training Providers, Telecom research organizations, Data centre providers, Internet exchange providers, Equipment importers, Type approval agencies, Enterprises with own networks, End Users ……..

Singapore: IPv6 Adoption Guide Report - I

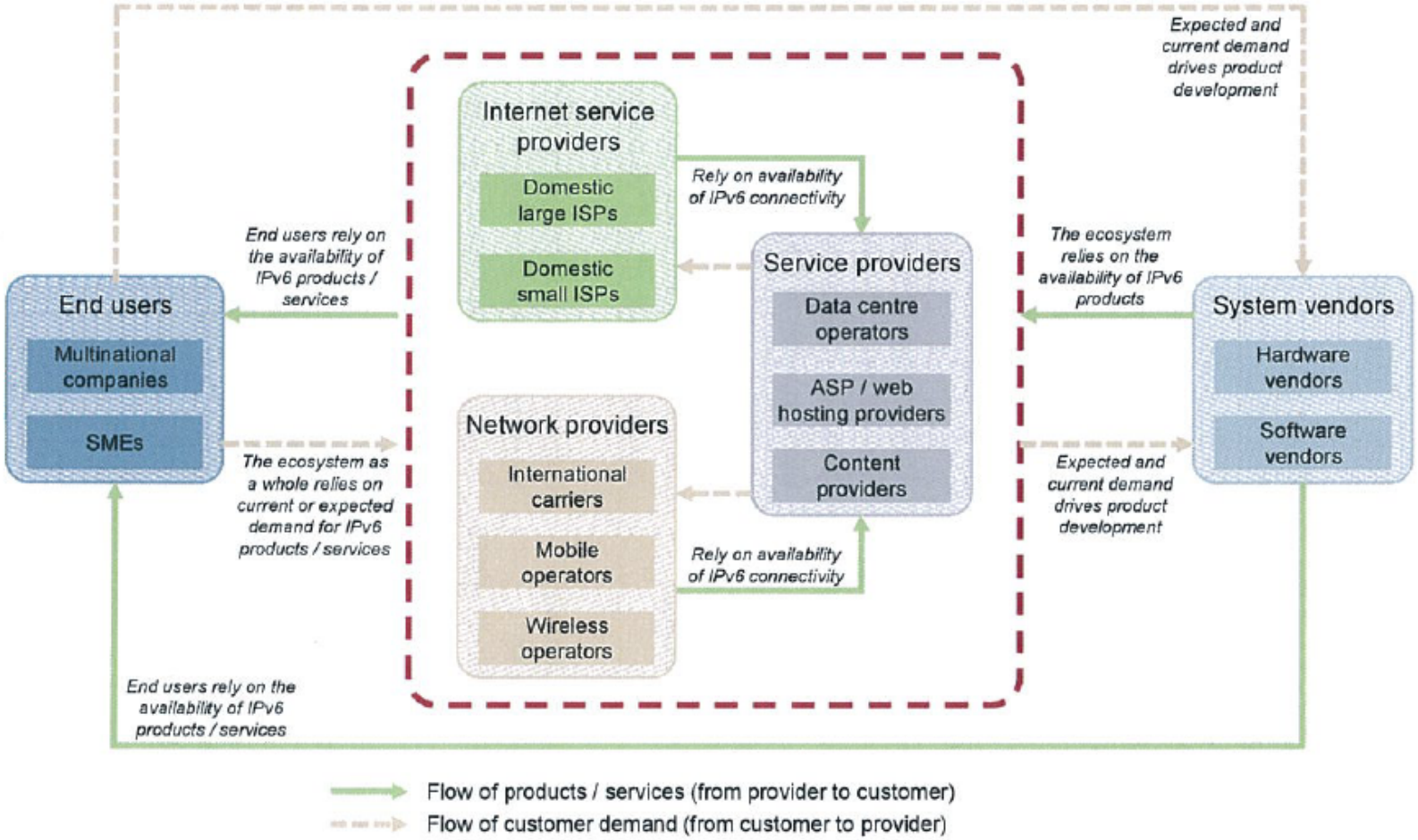


Figure 3.1: Summary of IPv6 dependencies between stakeholder categories [Source: Analysys Mason]

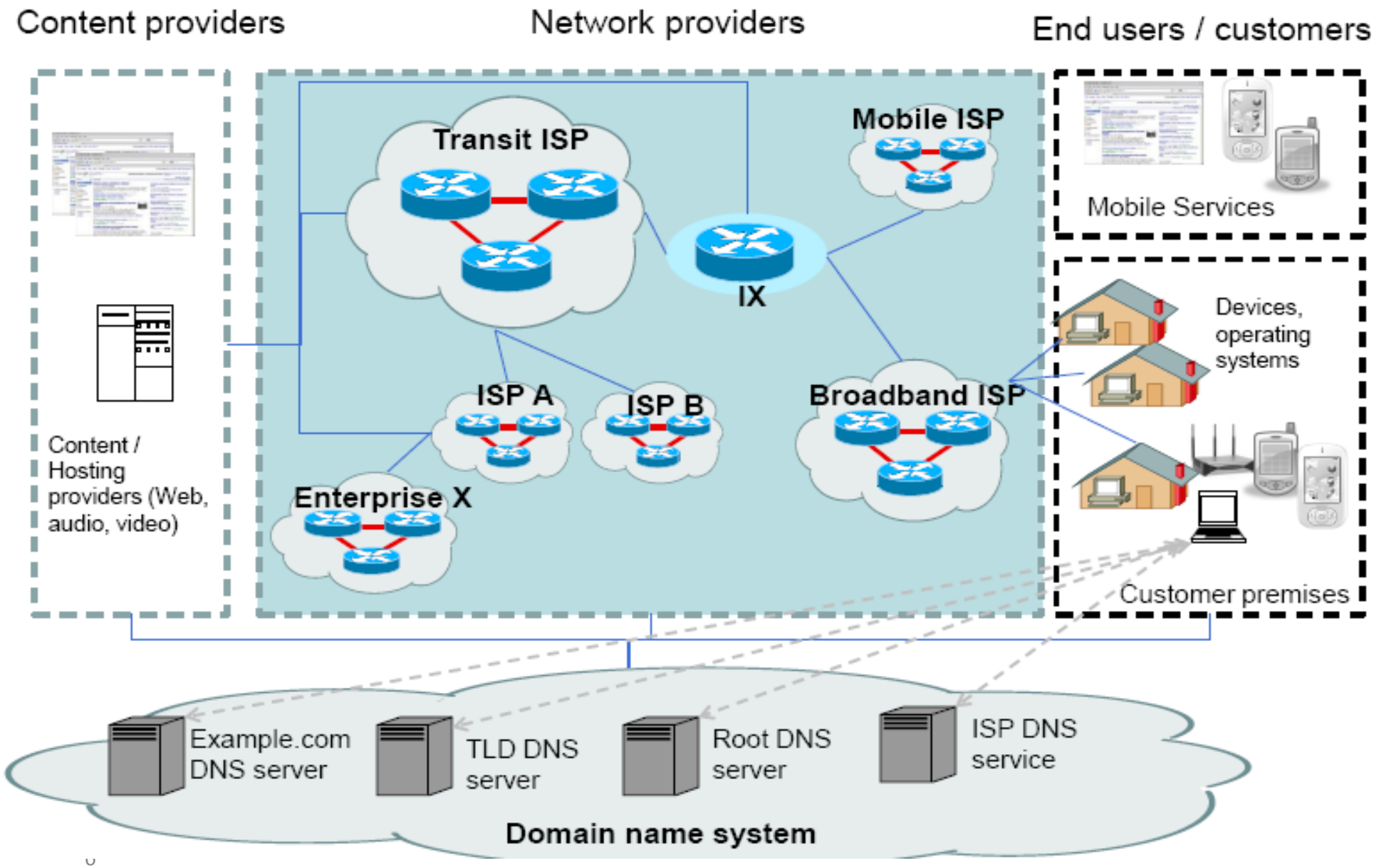
Report prepared by analysys mason and Tech Mahindra for IDA Singapore available at http://www.ida.gov.sg/images/content/Technology/Technology_Level1/ipv6/download/IPv6AdoptionGuideforSingapore.pdf

Singapore: IPv6 Adoption Guide Report - II

Focus areas identified in the report

- *Planning*
- *Network*
- *Applications*
- *Skills*
- *Services / products*

Zoom on **network providers**



Source: OECD Presentation; Measuring Deployment of IPv6, Karine Perset

Country experiences

Lao PDR

Cambodia

Mongolia

Bhutan (2017)

COMMUNICATIONS REGULATORY COMMISSION OF MONGOLIA

INFORMATION TECHNOLOGY, POST AND TELECOMMUNICATIONS AUTHORITY

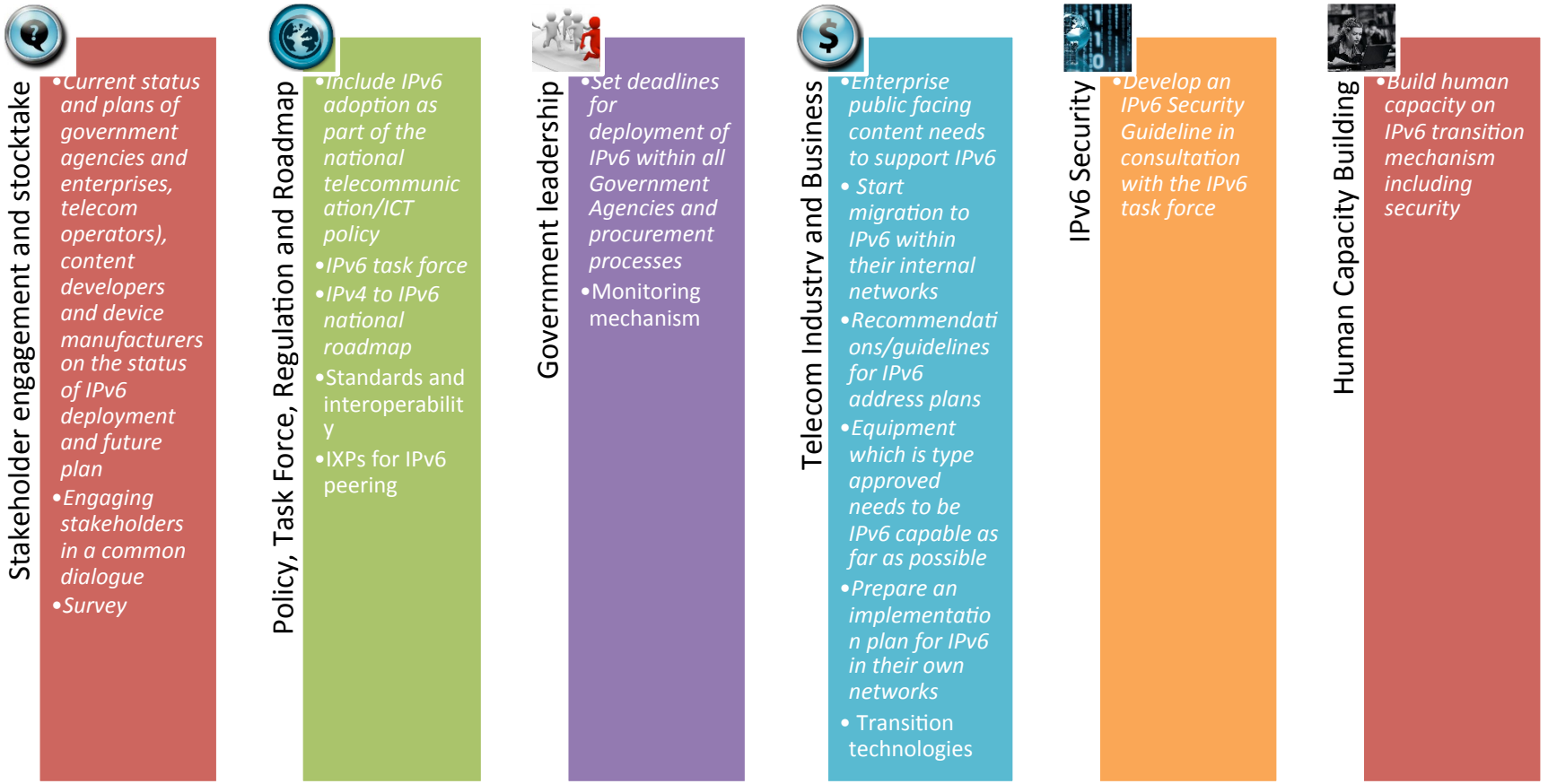
Training on IPv6 deployment and IPv6 Infrastructure Security

Specialized technical advice to interested telecom operators

Recommendations on IPv6 deployment

Australian Government
Department of Communications and the Arts

IPv6 migration - Experiences



Source: Roadmap assistances by APNIC and ITU

Key elements of government action

• Establishing or supporting national IPv6 transition task forces (often in conjunction with multistakeholder groups or RIRs);

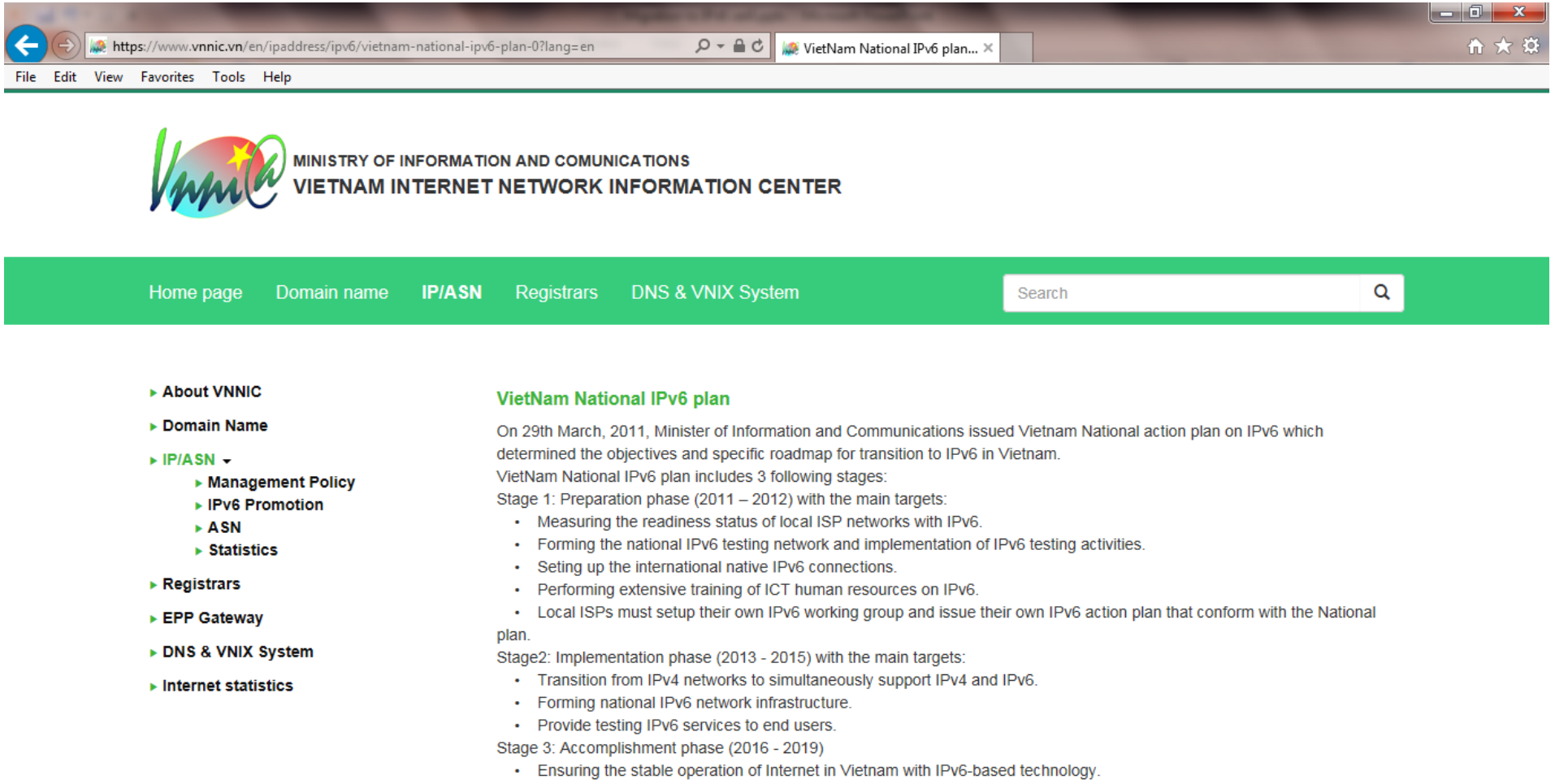
• Establishing national “roadmaps” with benchmarks and timetables for IPv6 deployment;

• Mandating that government agencies adopt IPv6 technology for their networks, websites or services;

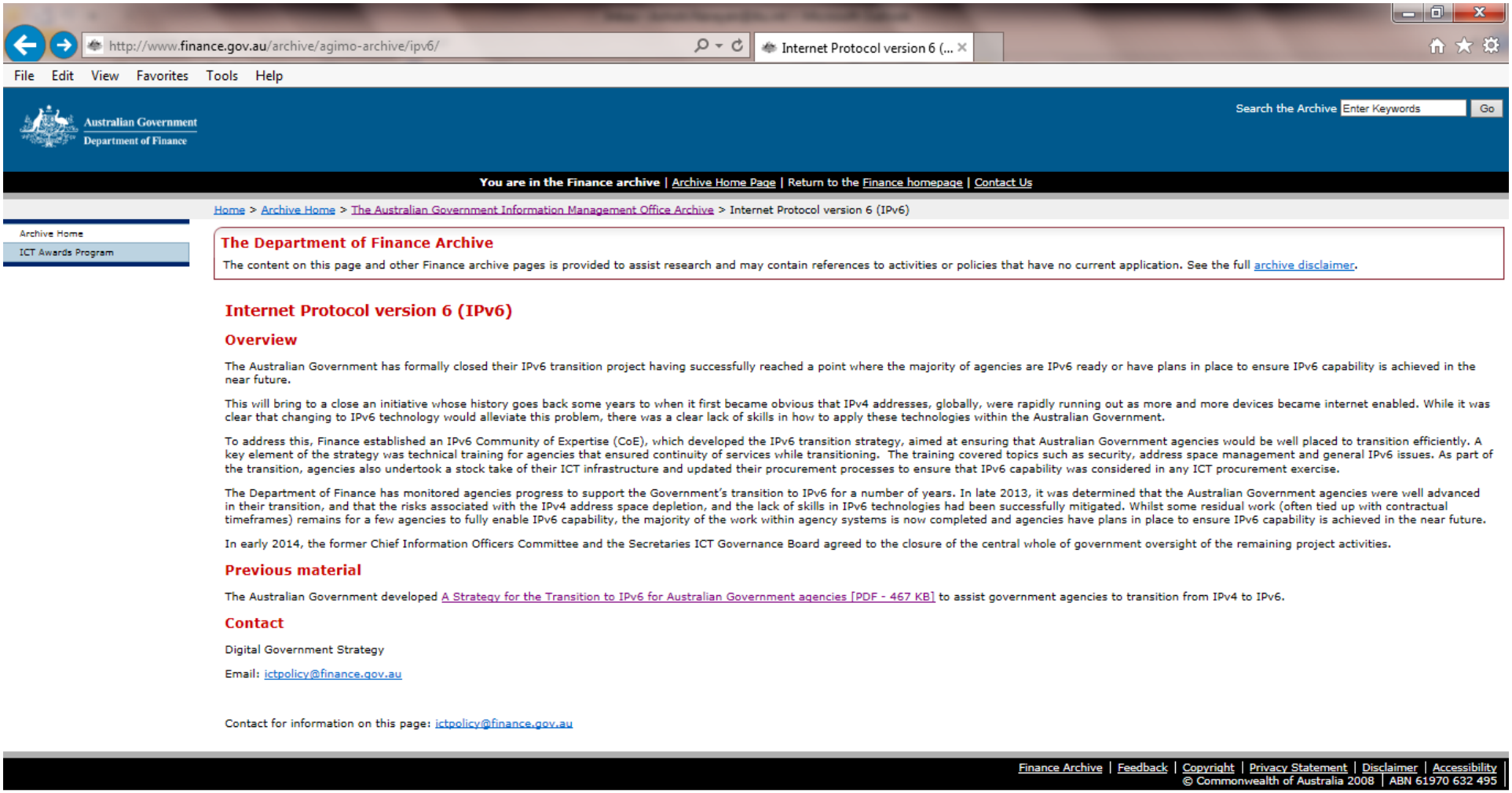
• Promoting the use of IPv6 in government-funded educational, science and research networks; and

• Promoting overall awareness of the transition through setting up websites, hosting workshops or forums, and setting up training programmes.

Governments promoting IPv6 deployment (examples)



Governments promoting IPv6 deployment (examples)



http://www.finance.gov.au/archive/agimo-archive/ipv6/

Internet Protocol version 6 (...

File Edit View Favorites Tools Help

Australian Government
Department of Finance

Search the Archive Enter Keywords Go

You are in the Finance archive | Archive Home Page | Return to the Finance homepage | Contact Us

Home > Archive Home > The Australian Government Information Management Office Archive > Internet Protocol version 6 (IPv6)

Archive Home
ICT Awards Program

The Department of Finance Archive

The content on this page and other Finance archive pages is provided to assist research and may contain references to activities or policies that have no current application. See the full archive disclaimer.

Internet Protocol version 6 (IPv6)

Overview

The Australian Government has formally closed their IPv6 transition project having successfully reached a point where the majority of agencies are IPv6 ready or have plans in place to ensure IPv6 capability is achieved in the near future.

This will bring to a close an initiative whose history goes back some years to when it first became obvious that IPv4 addresses, globally, were rapidly running out as more and more devices became internet enabled. While it was clear that changing to IPv6 technology would alleviate this problem, there was a clear lack of skills in how to apply these technologies within the Australian Government.

To address this, Finance established an IPv6 Community of Expertise (CoE), which developed the IPv6 transition strategy, aimed at ensuring that Australian Government agencies would be well placed to transition efficiently. A key element of the strategy was technical training for agencies that ensured continuity of services while transitioning. The training covered topics such as security, address space management and general IPv6 issues. As part of the transition, agencies also undertook a stock take of their ICT infrastructure and updated their procurement processes to ensure that IPv6 capability was considered in any ICT procurement exercise.

The Department of Finance has monitored agencies progress to support the Government's transition to IPv6 for a number of years. In late 2013, it was determined that the Australian Government agencies were well advanced in their transition, and that the risks associated with the IPv4 address space depletion, and the lack of skills in IPv6 technologies had been successfully mitigated. Whilst some residual work (often tied up with contractual timeframes) remains for a few agencies to fully enable IPv6 capability, the majority of the work within agency systems is now completed and agencies have plans in place to ensure IPv6 capability is achieved in the near future.

In early 2014, the former Chief Information Officers Committee and the Secretaries ICT Governance Board agreed to the closure of the central whole of government oversight of the remaining project activities.

Previous material

The Australian Government developed A Strategy for the Transition to IPv6 for Australian Government agencies [PDF - 467 KB] to assist government agencies to transition from IPv4 to IPv6.

Contact

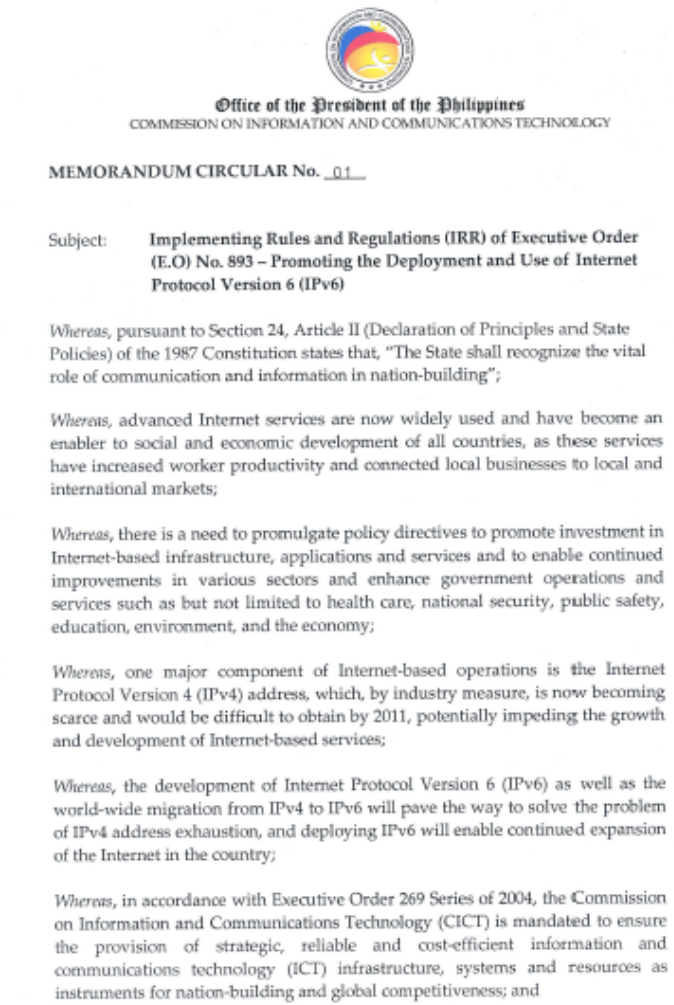
Digital Government Strategy

Email: ictpolicy@finance.gov.au

Contact for information on this page: ictpolicy@finance.gov.au

Finance Archive | Feedback | Copyright | Privacy Statement | Disclaimer | Accessibility
© Commonwealth of Australia 2008 | ABN 61970 632 495

Governments promoting IPv6 deployment (examples)



Office of the President of the Philippines
COMMISSION ON INFORMATION AND COMMUNICATIONS TECHNOLOGY

MEMORANDUM CIRCULAR No. 01

Subject: **Implementing Rules and Regulations (IRR) of Executive Order (E.O) No. 893 – Promoting the Deployment and Use of Internet Protocol Version 6 (IPv6)**

Whereas, pursuant to Section 24, Article II (Declaration of Principles and State Policies) of the 1987 Constitution states that, "The State shall recognize the vital role of communication and information in nation-building";

Whereas, advanced Internet services are now widely used and have become an enabler to social and economic development of all countries, as these services have increased worker productivity and connected local businesses to local and international markets;

Whereas, there is a need to promulgate policy directives to promote investment in Internet-based infrastructure, applications and services and to enable continued improvements in various sectors and enhance government operations and services such as but not limited to health care, national security, public safety, education, environment, and the economy;

Whereas, one major component of Internet-based operations is the Internet Protocol Version 4 (IPv4) address, which, by industry measure, is now becoming scarce and would be difficult to obtain by 2011, potentially impeding the growth and development of Internet-based services;

Whereas, the development of Internet Protocol Version 6 (IPv6) as well as the world-wide migration from IPv4 to IPv6 will pave the way to solve the problem of IPv4 address exhaustion, and deploying IPv6 will enable continued expansion of the Internet in the country;

Whereas, in accordance with Executive Order 269 Series of 2004, the Commission on Information and Communications Technology (CICT) is mandated to ensure the provision of strategic, reliable and cost-efficient information and communications technology (ICT) infrastructure, systems and resources as instruments for nation-building and global competitiveness; and

Promotion of IPv6

IPv6 deployment and use

Interagency Task Force

Funding

Singapore: IPv6 Transition Programme

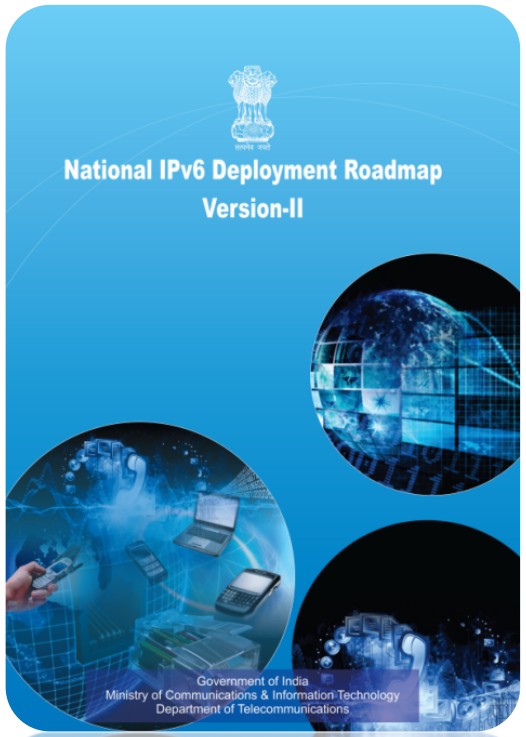
The IPv6 Transition Programme is a national effort spearheaded by IDA in its role as the national planner for Infocomm development, to address the issue of IPv4 (Internet Protocol version 4) exhaustion and to facilitate the smooth transition of the Singapore Infocomm ecosystem to IPv6 (Internet Protocol version 6).

Developed by the Singapore IPv6 Task Force, it involves a two-pronged approach to drive IPv6 adoption in the nation as well as encourage the efficient use of the remaining pool of IPv4 addresses to minimise the risks of depletion

Developing reference specifications and transition guides	Engaging stakeholders	Developing IPv6 capabilities	Establishing an IPv6 Marketplace	Setting up IPv6 industry exemplars	Others

Source: http://www.ida.gov.sg/Technology/20110414104645.aspx

IPv6 Roadmap (example - India)



India: NTP 2012 and IPv6

Preamble

NTP-2012 recognises futuristic roles of Internet Protocol Version 6 (IPv6) and its applications in different sectors of Indian economy.

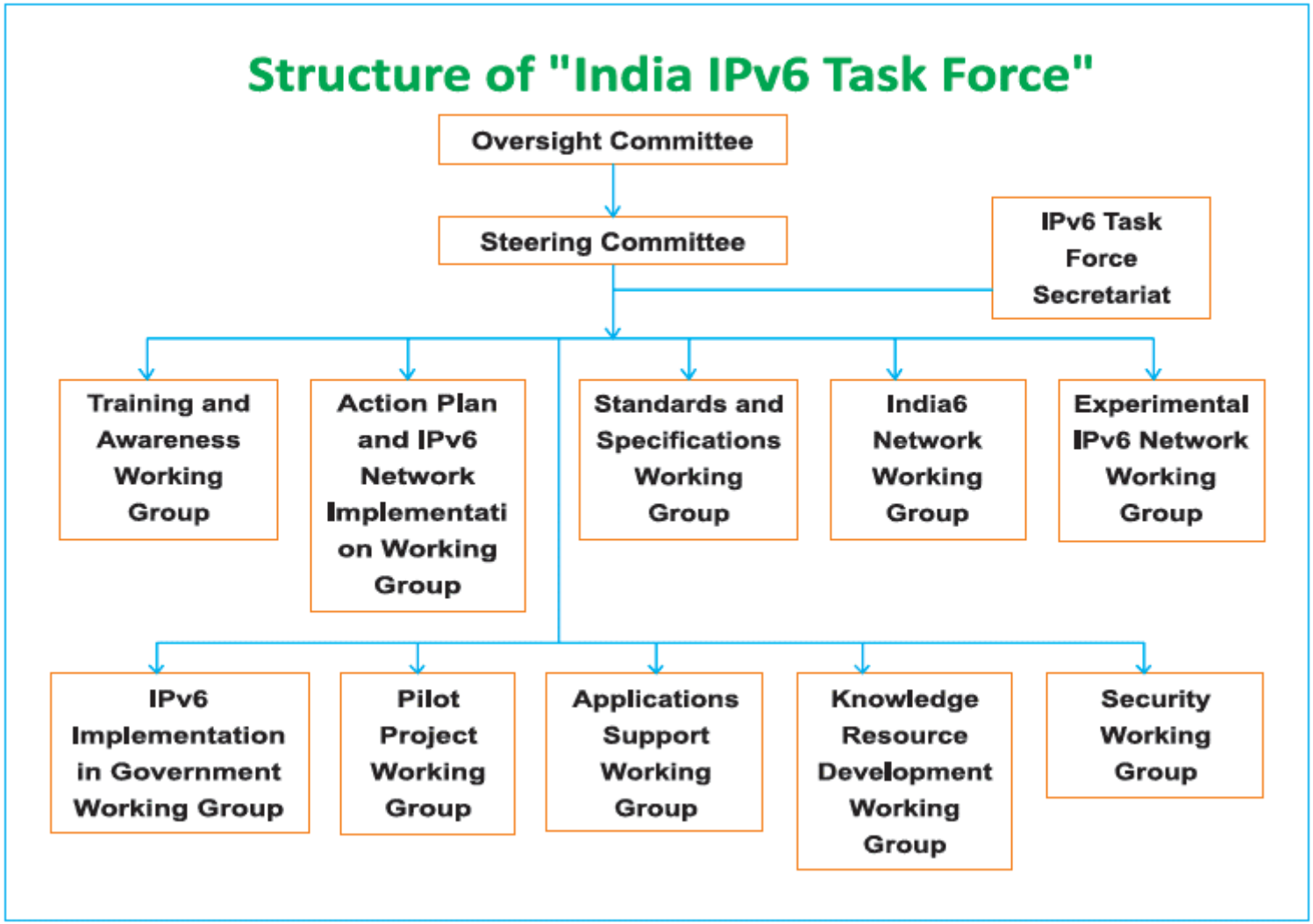
Objectives

Achieve substantial transition to new Internet Protocol (IPv6) in the country in a phased and time bound manner by 2020 and encourage an ecosystem for provision of a significantly large bouquet of services on IP platform.

Telecom Enterprise Data Services, IPv6 Compliant Networks and Future Technologies
To recognize the importance of the new Internet Protocol IPv6 to start offering new IP based services on the new protocol and to encourage new and innovative IPv6 based applications in different sectors of the economy by enabling participatory approach of all stake holders.

To establish a dedicated centre of innovation to engage in R & D, specialized training, development of various applications in the field of IPv6. This will also be responsible for support to various policies and standards development processes in close coordination with different international bodies.

Structure of "India IPv6 Task Force"



Governments promoting IPv6 deployment (example India)

Government Organisations:

- The Government organisations should prepare a detailed transition plan for complete transition to IPv6 (dual stack) by December 2017 based on the network complexity & equipment/ technological life cycles. The plan should be prepared latest by December 2013 and accordingly the required budgetary provisions should be made in their demand for grant.
- For this purpose, it is recommended that a dedicated transition unit in each organisation should be formed immediately to facilitate entire transition.
- All new IP based services (like cloud computing, data centres etc.) to be provisioned for / by the Government organisations should be on dual stack supporting IPv6 traffic with immediate effect.
- The public interface of all Government projects for delivery of citizen centric services should be dual stack supporting IPv6 traffic latest by 01-01-2015. The readiness of Government projects in turn will act as a catalyst for private sector transition from IPv4 to IPv6.

Governments promoting IPv6 deployment (example India)

Government Organisations:

- The Government organisations should procure equipments which are also IPv6 Ready (Dual Stack) and go for deployment of IPv6 ready (Dual Stack) networks with end to end IPv6 supported applications. The equipment should be either TEC certified or IPv6 Ready Logo certified.
- The Government organisations should go for IPv6 based innovative applications in their respective areas like smart metering, smart grid, smart building, smart city etc.
- The Government organisations should develop adequate skilled IPv6 trained human resources within the organisation through periodic trainings over a period of one to three years to have a seamless transition with minimum disruption.
- The IPv6 should be included in the curriculum of technical courses being offered by various institutes / colleges across the country.

Governments promoting IPv6 deployment (example India)

Service Providers:

Enterprise Customers

- All new enterprise customer connections (both wireless and wireline) provided by Service Providers on or after 01-01-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.
- Regarding the existing enterprise customers which are not IPv6 ready, the Service Providers shall educate and encourage their customers to switch over to IPv6.

Retail Customers (Wireline)

- All new retail wireline customer connections provided by Service Providers on or after 01-01-2017 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.
- The Service Providers shall endeavor to progressively replace/ upgrade the Service Providers owned CPEs which are not IPv6 ready as per the following timelines:
- Replacement/ upgradation of 25% of CPEs by December 2014.
- Replacement/ upgradation of 50% of CPEs by December 2015.
- Replacement/ upgradation of 75% of CPEs by December 2016.
- Replacement/ upgradation of 100% of CPEs by December 2017.

Regarding the customer owned CPEs which are not IPv6 ready, the Service Providers shall educate and encourage their customers to replace/ upgrade such CPEs to IPv6 ready ones.

Governments promoting IPv6 deployment (example India)

Retail Customers (Wireless)

- All new LTE customer connections provided by Service Providers with effect from 01-01-2017 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.
- All new GSM/ CDMA customer connections provided by Service Providers on or after 01-01-2017 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6

Content & Application Providers:

- All contents (e.g. websites) and applications providers should endeavour to adopt IPv6 (dual stack) by 01-01-2017.'

- The complete financial ecosystem including payment gateways, financial institutions, banks, insurance companies etc. should endeavour to adopt IPv6 (dual stack) by 01-01-2017.'

- The entire '.in' domain should endeavour to adopt IPv6 (dual stack) by 01-01-2017.'

Governments promoting IPv6 deployment (example India)

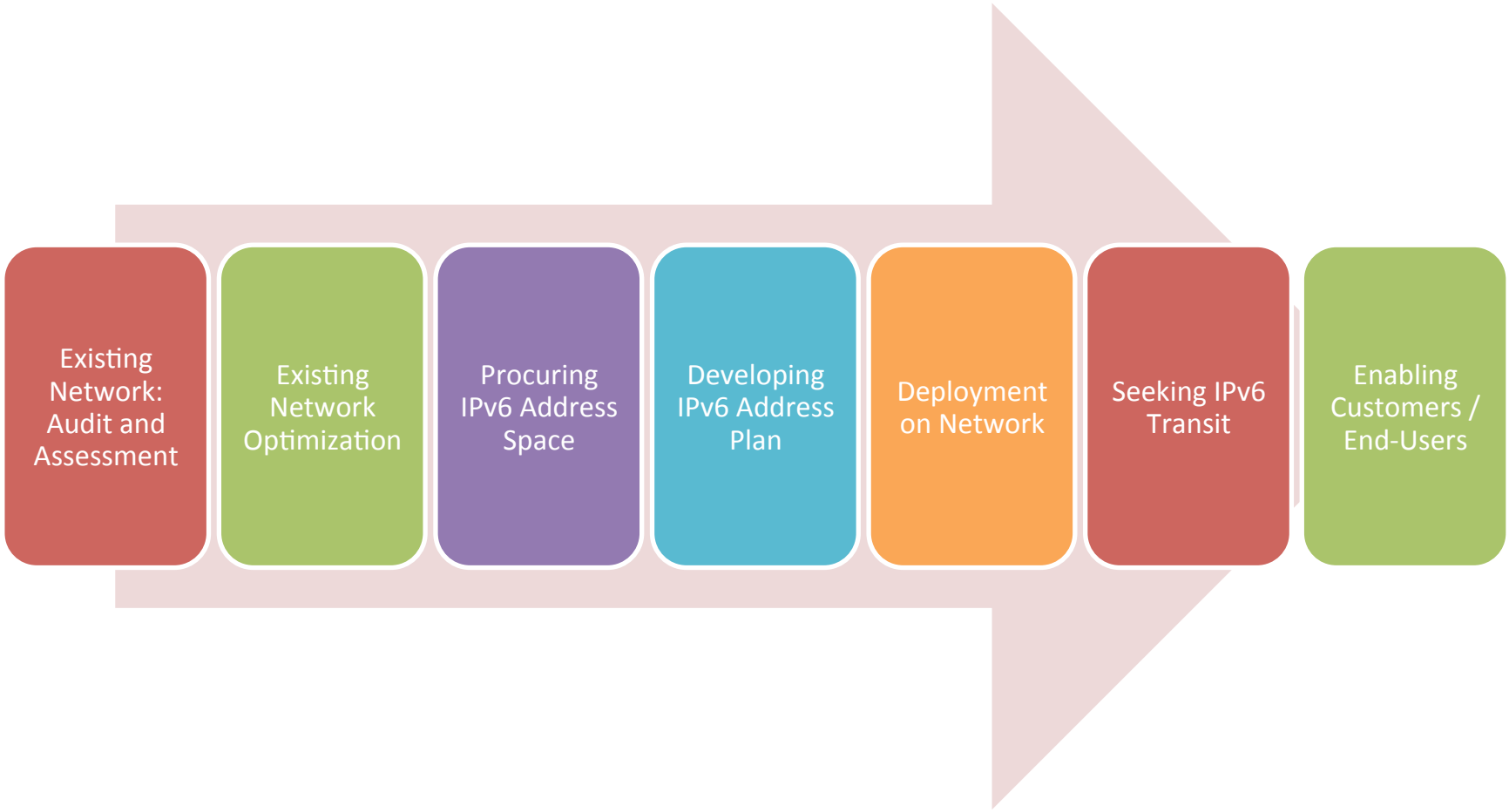
Equipment Manufacturers:

- All mobile phone handsets/ data card dongles/ tablets and similar devices used for internet access supporting GSM/CDMA version 2.5G and above sold in India on or after 30-06-2014 shall be capable of carrying IPv6 traffic either on dual stack (IPv4v6) or on native IPv6.
- All wireline broadband CPEs sold in India on or after 01-01-2014 shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6.

Cloud Computing / Data Centres:

- All public cloud computing service / data centres providers should endeavour to adopt IPv6 (dual stack) latest by 01-01-2017.

Telecom Service Provider - Migration



Source: Dr. Philip Smith, Roadmaps assistances by APNIC and ITU

IPv6 related standards
(Non – exhaustive)

IETF RFC	Title
IETF RFC 3964 (2004)	Security Considerations for 6to4.
IETF RFC 4593 (2006)	Generic Threats to Routing Protocols.
IETF RFC 4795 (2007)	Link-Local Multicast Name Resolution (LLMNR).
IETF RFC 4861 (2007)	Neighbor Discovery for IP version 6 (IPv6).
IETF RFC 4942 (2007)	IPv6 Transition/Coexistence Security Considerations.
IETF RFC 5942 (2010)	IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes.
IETF RFC 5969 (2010)	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification.
IETF RFC 6106 (2011)	IPv6 Router Advertisement Options for DNS Configuration.
IETF RFC 6333 (2011)	Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion.
IETF RFC 6434 (2011)	IPv6 Node Requirements.
IETF RFC 6618 (2012)	Mobile IPv6 Security Framework Using Transport Layer Security for Communication between the Mobile Node and Home Agent
IETF RFC 6686 (2013)	Problem Statement for Renumbering IPv6 Hosts with Static Addresses in Enterprise Networks
IETF RFC 6879 (2013)	IPv6 Enterprise Network Renumbering Scenarios, Considerations, and Methods
IETF RFC 6883 (2013)	IPv6 Guidance for Internet Content Providers and Application Service Providers
IETF RFC 6889 (2013)	Analysis of Stateful 64 Translation
IETF RFC 6946 (2013)	Processing of IPv6 "Atomic" Fragments
IETF RFC 6980 (2013)	Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery
IETF RFC 7059 (2013)	A Comparison of IPv6-over-IPv4 Tunnel Mechanisms
IETF RFC 7113 (2014)	Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)
IETF RFC 7123 (2014)	Security Implications of IPv6 on IPv4 Networks
IETF RFC 7283 (2014)	Handling Unknown DHCPv6 Messages
IETF RFC 7368 (2014)	IPv6 Home Networking Architecture Principles
IETF RFC 7381 (2014)	Enterprise IPv6 Deployment Guidelines
IETF RFC 7526 (2015)	Deprecating the Anycast Prefix for 6to4 Relay Routers
IETF RFC 7527 (2015)	Enhanced Duplicate Address Detection
IETF RFC 7610/BCP 199 (2015)	DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers
IETF RFC 7707 (2016)	Network Reconnaissance in IPv6 Networks
IETF RFC 7721 (2016)	Security and Privacy Considerations for IPv6 Address Generation Mechanisms
IETF RFC 7739 (2016)	Security Implications of Predictable Fragment Identification Values
IETF RFC 7824 (2016)	Privacy Considerations for DHCPv6

IPv6 Infrastructure Security (ITU-T X.1037)

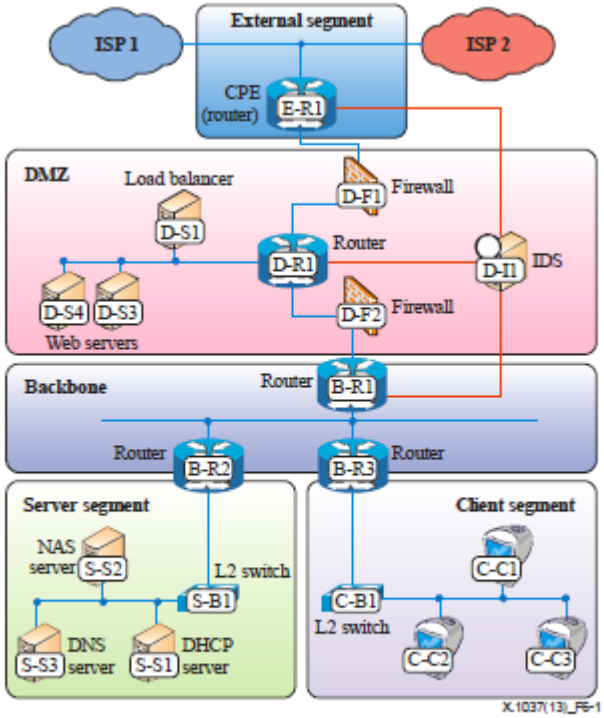


Figure 6-1 – Example topology of an IPv6 enterprise network

Network Devices
(Router, Switch, NAT device)

Security devices such as firewalls and IDS Devices
(Intrusion Detection System, Firewall)

Clients, servers, and other end devices
(End Nodes, DHCP, DNS)

Bhutan Telecommunications and Broadband Policy 2014

Develop IPv6 migration plan

Key issues to consider in Bhutan

- Policy, legislation and regulation cluster
- Institution, stakeholder engagement and coordination cluster
- Technology (hardware and software), standards, type approval, infrastructure, and interoperability cluster
- Security cluster
- Assessment, pilot, testing and deployment cluster
- Knowledge, awareness and skills cluster
- Procurement and financial cluster

Thank You