IPv6 in Canada: Final Report and Recommendations of the ISACC IPv6 Task Group (IITG)

Approved at the 42nd ISACC Plenary meeting on March 16, 2010

The intended audience for this report includes:

- Members of the ICT Standards Advisory Council of Canada (ISACC); and
- CxO-level executives, chief architects, ICT managers and other decision makers within private and public sector organizations who are responsible for ensuring their Information Technology (IT) expenditures are planned and executed to assist in achieving the mission and objectives of their organizations.

Abstract

Shortly after the 40th ISACC Plenary meeting in April 2009, a Task Group was formed to investigate the status of IPv6 in Canada, and to recommend appropriate actions for consideration by the Government of Canada (GoC) and by Canadian industry.

The ISACC IPv6 Task Group (IITG) presented a set of interim recommendations to the 41st ISACC Plenary meeting in November 2009. This report contains the final recommendations of the Task Group for actions required to accelerate IPv6 in Canada. It summarizes the work of the Task Group that led to those recommendations, and includes several Annexes and Appendices containing detailed analyses and useful reference information.

Annex D of this report contains draft Terms of Reference for a Canadian Centre of Excellence on IPv6 as presented to the 42nd ISACC Plenary meeting in March 2010.

Executive Summary

Internet and enterprise networks typically use the same underlying transport protocol: the Internet Protocol (IP). Most traffic on the Internet uses Internet Protocol version 4 (IPv4) designed in 1981, and all devices networked using IPv4 (e.g. computers, servers, routers, access points) have an IPv4 address. IPv4 was designed to use 32-bit addressing and can handle approximately 4.3 billion addresses, a number which is smaller than the number of people on Earth today.

In the past two decades, more than 90% of the IPv4 address space has been allocated and used. Consumption of IPv4 address space has averaged 5% per year. As of February 2010, less than 9% of the IPv4 address space was left. Experts predict that complete exhaustion of the last remaining IPv4 addresses will occur in 2012.

After the complete exhaustion of the IPv4 address space in 2012, new devices and networks will be unable to obtain IPv4 addresses and will therefore need to use a new version of IP called Internet Protocol version 6 (IPv6). New content, applications, services and end-users will be assigned IPv6 addresses. In anticipation of this, a migration of existing networks and services to IPv6 has started in many parts of the world.

Even though IPv6 was first specified in 1996, very few commercial networks adopted it before 2009. There was no compelling business case for most of the installed base of networks (public or private) to deploy IPv6. IPv4 worked well and the anticipated run-out of IPv4 addresses was far in the future. This delayed the deployment of IPv6 into production networks for a long time.

In recent years however, many of Canada's largest trading partners including the United States, the European Union, China, Japan, Korea and others have mandated the deployment of IPv6 capable devices for their networks. Additionally, some governments subsidized domestic research and/or procurement of IPv6 products. Canada was an early mover on IPv6 in the early 2000's and had several "firsts", however its technology leadership has not been sustained.

Today, Canada is clearly lagging behind its main trading partners with respect to IPv6 awareness and deployment. IPv6 expertise and awareness exists in Canada, but is concentrated in a very small number of people and organizations. Canada's largest trading partners have embraced IPv6 for their digital economy strategies. They recognize that international trade and e-commerce depend on Internet technologies, and that the Internet is moving to IPv6.

IPv6 deployment into existing networks and operations can take several years. This should be a red flag for Canada, as the last IPv4 address blocks will be depleted in *less than* two years.

To continue to be part of the global Internet and to benefit from its growth, Canadian organizations such as Governments, internet and content services providers, and enterprises need to migrate to IPv6. Most mainstream ICT products are now IPv6-capable and carrying IPv6 traffic in other countries.

This report is a call to action. Canada needs to embrace IPv6 or risk becoming non-competitive in international trading markets and in the networking technology that is vital to all segments of our digital economy.

Therefore, the ISACC IPv6 Task Group recommends:

- *Canadian governments of all levels (federal, provincial, territorial, regional, municipal) shall plan for IPv6 migration and specify IPv6 support in their IT procurements immediately;*

- *Canadian Internet Service Providers (ISPs) shall accelerate the deployment and the commercial availability of IPv6 services for business and consumer networks;*

- *Canadian internet content and application service providers shall make their content and applications reachable using IPv6;*

- *Canadian industries in all sectors shall intensify the support of IPv6 on all products that include a networking protocol stack;*

- *Canadian industry and governments shall establish a Center of Excellence to increase IPv6 awareness in Canada, by offering training and education, advice and the sharing of best practices;*

- *Governments at all levels shall review current programs to ensure eligibility of IPv6 initiatives and evaluate the creation of specific programs to enable Canadian industry to take full advantage of global IPv6 markets; and*

- *the CRTC shall ensure that relevant telecommunications and broadcasting decisions and policies support IPv6 deployment.*

Acknowledgements

The ISACC IPv6 Task Group (IITG) was formed by a subset of interested members of the ICT Standards Advisory Council of Canada (ISACC) after its 40th Plenary meeting (April 2009).

The first meeting of the IITG was held in July 2009. The focus was on organizing the work, establishing working methods, and building momentum. A lot of people and organizations were represented at the kick-off meeting. The Task Group acknowledges the significant efforts of J.C.P. Jourdeuil and Marc Lemoine (both from Defence R&D Canada) who provided a collaboration portal to serve as a document repository during the IITG's first few months of operation.

From August to October 2009, the IITG analyzed the state of IPv6 deployment around the world, and developed a set of interim recommendations for ISACC. The recommendations were presented during the 41st Plenary meeting of ISACC in November 2009.

From December 2009 to March 2010, the IITG resumed work to investigate new developments and to finalize its recommendations for the adoption of IPv6 in Canada.

The following members of the IITG participated in the work:

Name	**Affiliation and/or IITG Role**
Jim MacFie	Microsoft Canada, and ISACC Chair
Yves Poppe	Tata Communications, and Task Group Chair
Marc Blanchet	Viagénie, and Task Group Vice-Chair
Ed Juskevicius	TrekAhead, and Secretary for the Task Group
Marcelo Ferme	Industry Canada, and ISACC Secretariat
Faud A. Khan	Alcatel-Lucent ALU Ventures – Bell Labs
Douglas Kwong	Bell Canada
Erone Quek	Bell Canada
Brian Smith	Bell Canada
Cory Wishak	Canadian Radio-television Telecommunications Commission
Eric Bernier	CANARIE
Thomas Tam	CANARIE
Brian Hanson	Cisco Systems
Stephen Orr	Cisco Systems
Chris MacFarlane	Cogeco Cable
Lewis Robart	Communications Research Centre Canada
Eric Tsang	Communications Research Centre Canada
Mikael Lind	gogo6
David Gibson	Industry Canada
Tara Hennessy	Industry Canada
Colman Ho	Industry Canada
Jacqueline Jones	Industry Canada
Bill Munson	ITAC
John Hopkinson	Chairman of CAC-JTC-1/TCIT
Eric Beauchesne	Microsoft Canada

Name	Affiliation and/or IITG Role
John Weigelt	Microsoft Canada
Anurag Jain	Polynate
Mario Boisvert	Public Works and Government Services Canada
Jonathan Sau	Research in Motion
Vino Vinodrai	Research in Motion / Vinodrai Associates Inc.
Richard Thomas	RJT Solutions Group Inc.
George Babut	Rogers
Jean-Yves Bernard	Rogers
George Hart	Rogers
Gerry Thompson	Rogers
Michael Richardson	Sandelman Software Works
Mukesh Gupta	Tata Consultancy Services
Percy Lee	TELUS
Ken Nguyen	Treasury Board of Canada Secretariat
Jean-François Tremblay	Vidéotron
Francois Menard	Xittel Communications
John Visser	Private Consultant
Joe Zebarth	Private Consultant

In addition, the Task Group acknowledges the efforts and contributions of the following individuals:

- Jim MacFie for convening a drafting group which developed much of the text for the proposed Terms of Reference for a Canadian IPv6 Centre of Excellence included in Annex D of this report; and
- Tony Hain (Cisco Systems) for sharing his insights into the current status of IPv6 profiles and interoperability testing in the U.S. and other countries, many of which are included in Annex E of this report.

Finally, the IITG acknowledges the leadership, meeting facilitation, report writing and editing efforts of Yves Poppe, Marc Blanchet, Ed Juskevicius, and Marcelo Ferme.

Table of Contents

1. Introduction

1.1. Internet Protocol version 4 (IPv4)

Typically the Internet and most enterprise networks use the same underlying technology to transport information and e-commerce, viz. Internet Protocol version 4, known as IPv4 [RFC791], designed in 1981. All traffic carried on the Internet uses the Internet Protocol and devices that connect to the Internet (e.g. computers, servers, mobile browsers) are identified by an IP address.

IPv4 uses 32-bit addressing. IPv4 can address 2^{32} or approximately 4.3 billion devices. Only a few per cent of the IPv4 address space was used in 1990 when the Internet was still young. Today, only a few per cent of the IPv4 address space is left. More than 90% of the IPv4 address space has been allocated.

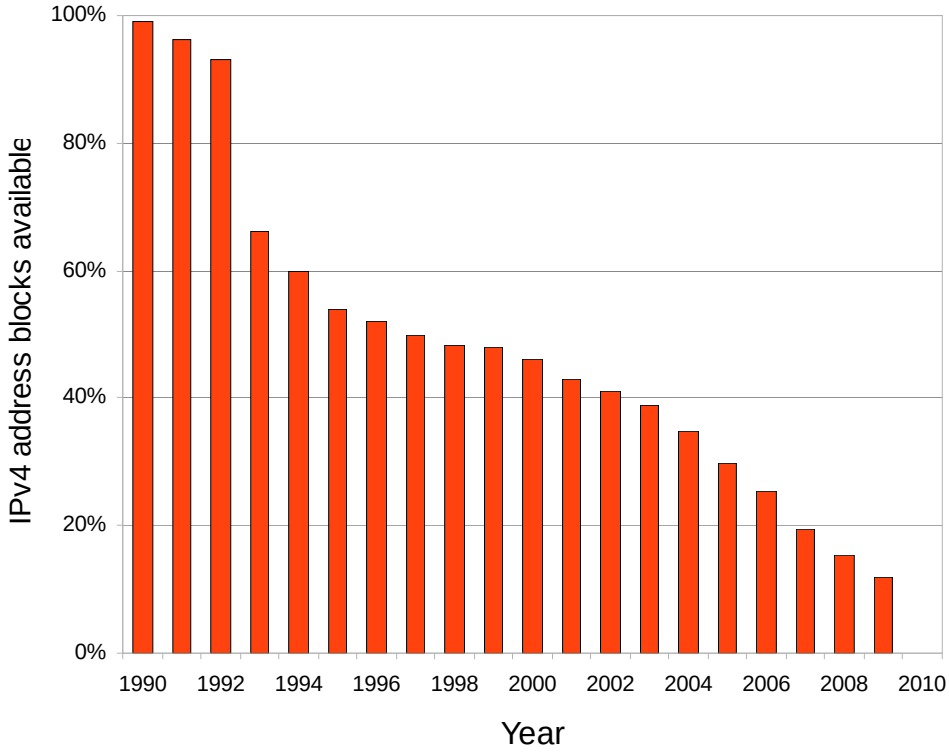


Figure 1: Consumption of IPv4 addresses over time (viz. 1990 to 2009)

Over the last two decades, IPv4 addresses have been freely allocated to growing public and private internetworks. Figure 1 illustrates the rate of IPv4 address space allocation over time. On average, approximately 5% of the total IPv4 address space has been consumed every year since 1990. **Note**: Figure 1 does not show data for 2010; the year is not yet over.

In January 2010, only 10% of the IPv4 address space was left [NRO10]. In February 2010, that number had shrunk to 8.5%. The days of IPv4 are numbered. Complete exhaustion of all remaining IPv4 addresses is expected within two years [IPv4ADDREP].

1.2. Internet Protocol version 6 (IPv6)

The engineering and computer science community started investigating how to alleviate the address limitations of IPv4 more than fifteen years ago. In 1993, the Internet Engineering Task Force (IETF) formally started work on a new version of IP. The outcome was consensus on a set of new standards which collectively defined Internet Protocol version 6 (IPv6).

One of the features of IPv6 is a vastly expanded addressing capability compared to that of IPv4. The IPv6 address space is 128 bits long (versus 32 bits in IPv4). In practical terms this means IPv6 can support 10 billion billion billion ***times*** more addresses than IPv4.

Unfortunately IPv6 was not designed to be backward compatible with IPv4. As a result:

- IPv6 devices can only communicate with other IPv6 devices;
- IPv4 devices can only communicate with other IPv4 devices; and
- current IPv4-only devices, networks and applications must be upgraded to communicate with new IPv6-only devices.

Table 1 shows a summary of the compatibilities.

	IPv4-only	IPv6-only	Dual-stack (IPv4 and IPv6)
IPv4-only	Compatible	***Not Compatible***	Compatible
IPv6-only	***Not Compatible***	Compatible	Compatible
Dual-stack (IPv4 and IPv6)	Compatible	Compatible	Compatible

Table 1: Compatibility matrix between IPv4 and IPv6 devices

One method to connect an IPv4 device with an IPv6 device is to upgrade one of them to run both IPv4 and IPv6 (i.e. to have a "dual-stack" configuration). However an issue with dual-stacks is that devices with dual-stacks need both IPv6 and IPv4 addresses. After the last IPv4 addresses are used, dual-stacks will cease to be a viable interworking technology. All new devices and networks will have no choice but to run IPv6-only (single-stack).

In recognition of the impending depletion of IPv4 address space, a global migration to IPv6 is underway.

Many nations and regions started planning for IPv6 several years ago, and are driving the adoption of IPv6 within their borders, as described in section 4. In particular it should be noted:

- the United States [USOMB], Canada's largest trading partner and defence ally, has adopted IPv6 for all federal government civilian agency networks and for U.S. Department of Defense (DoD) networks;

- other regions and countries are aggressively deploying IPv6 including the European Union, China, Korea, Japan, Australia and India; and
- Canada's adoption of IPv6 is lagging.

In order to maintain global competitiveness, Canadians need to urgently accelerate planning and procurement of IPv6 products, services, applications, content and networking.

1.3. Goals of this report

The overall goals of this report are:

- to present a set of recommendations for migrating Canadian organizations in the private and public sectors to IPv6 in a timely fashion; and
- to impart a sense of urgency that Canada must accelerate its transition to IPv6 or else risk adverse economic and social consequences.

This report contains up to the minute information about the status of IPv6 adoption in Canada's largest trading partners, and within our own borders. It explains the reasons for moving to IPv6, and it describes the benefits for public and private sector organizations to make the transition.

Section 6 provides a set of recommendations to help Canadians accomplish their transition to IPv6 in an orderly and efficient way.

IPv6 is inevitable. Not migrating to IPv6 is not an option.

2. The Rationale for IPv6

IPv4 has been a foundation of the Internet and many enterprise networks since the early 1980's. Two studies [SOLENSKY] [RFC1752] in the early 1990's projected that IPv4 address space would be exhausted around 2010. Those studies launched the work that created IPv6.

IPv6 can solve the impending problems of global IPv4 address space exhaustion. IPv6 can also enable many new features needed to cost reduce existing networks (e.g. auto-configuration of customer premises devices) or to enable new networking applications (e.g. sensor networks [ARCHROCK], smart buildings and smart grids [OECDSG]) and mobility applications for 3G and post-3G networks.

2.1. The solution for IPv4 address exhaustion

Section 1.2 introduced the most well known attribute of IPv6 – its enormous address space compared to IPv4. The expanded address capacity of IPv6 will allow the Internet to continue growing and evolving without service interruption. IPv6 has enough address space for each person on Earth to have their own network as large as today's (global) Internet, with a lot of addresses to spare. In fact, if IPv6 addresses were to be assigned in such a fashion, less than one-trillionth of 1% of the total IPv6 address space would be consumed.

There is no alternative to IPv6 for solving the expected depletion of IPv4 addresses by 2012. This fact must be accepted by Canadian stakeholders as an urgent call for pro-active deployment of IPv6 networks and services in Canada.

2.2. A platform for business continuity and growth

In addition to having a larger address space, IPv6 has many default features built-in which are essential to the continued stability and growth of communications and commerce over the Internet. These include:

1. Improved and/or cost reduced network management for large enterprises and providers suffering from dwindling IPv4 private address space;
2. Simpler and more efficient peer-to-peer and VoIP communications;
3. New protocol mechanisms (e.g. "auto-configuration") to ease the deployment of devices on networks without a priori configuration. Sensors, smart grids, small devices, mobile and adhoc networks can all be deployed more readily and in a large scale way with IPv6;
4. Embedded security at the transport level for secure end-to-end communications, and a higher (default) level of security on public networks;
5. Enhanced Quality of Service (QoS) enabling consumers, enterprises and providers to use experience superior QoS for delay sensitive services and traffic; and
6. Embedded support for mobility for existing and future client devices (e.g. smart phones, vehicles, aircraft in flight, sensors and sensor networks).

Among all of the features of IPv6, its gigantic address space is the primary trigger for deployment today. However, once IPv6 is deployed in a network, its additional features as listed above become immediately available, and enable additional benefits that can be used to create an increase in the return on investment.

2.3. A foundation for future research and innovation

Section 4.2 and Annex C discuss how other countries have invested research and development to leverage IPv6 and some of the results (e.g. new applications and classes of solutions).

One area of current research involves using ICT technologies to reduce society's carbon footprint. Large office buildings, industrial campuses, factories and the like can have thousands (or millions) of energy consuming devices (e.g. light bulbs, doors, heaters, air conditioners, cameras, computers, servers) that are "always on." Researchers in Japan and the Middle East have found that using IPv6 to individually address (and control) each of these devices can result in significant energy cost savings, which in turn will reduce greenhouse gas emissions. One study claimed a payback of less than five years for a new office tower with over 300,000 smart devices controlled via a private IPv6 network.

Smart Grids are another area where IPv6 may play an important role. Electricity grids around the world are being modernized and redesigned to use ICT capabilities to provide utilities and consumers with "smart" ways to access information on power usage in real-time, and to control and optimize the management of their demands for electricity in unprecedented ways.

In May 2009, U.S. President Barack Obama declared that the American electricity grid is a strategic national asset and that his Administration will provide stimulus money (on a one for one matching basis) to modernize the U.S. grid. Nearly eight billion dollars have been committed for Smart Grid projects in the U.S. since May 2009 [OBAMAGRID].

In November 2009, the American Registry for Internet Numbers (ARIN) sent a letter to the U.S. National Institute of Standards and Technology (NIST), which is developing U.S. standards and requirements for Smart Grids, to urge NIST to focus on IPv6 rather than IPv4 for Smart Grids.

3. Key IPv6 Considerations

IPv6 is a new protocol and different from IPv4. IPv4-enabled devices, operating systems and applications cannot communicate directly with IPv6-enabled devices, as previously summarized in Table 1, and as illustrated in Figure 2 below.

IPv6 was not designed to be backward compatible with IPv4. As a result:

- IPv6 devices can only communicate with other IPv6 devices;
- IPv4 devices can only communicate with other IPv4 devices; and
- current IPv4-only devices, networks and applications must be upgraded to communicate with new IPv6-only devices.

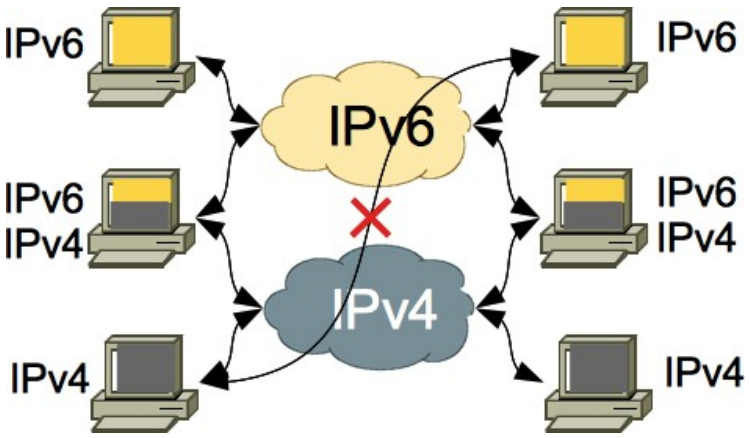


Figure 2: IPv4 and IPv6 networks

Current IPv4-only devices may be upgraded to be dual-stack (IPv4 and IPv6 enabled) or to be IPv6-only depending on the upgrade path supported by the manufacturer. For most devices and applications, IPv6 is a software upgrade. In a few devices (e.g. backbone routers in ISP networks), new hardware may be required such as additional memory or new forwarding processors.

IPv6-capable systems are generally available in the marketplace today and in sufficient quantities and diversity to facilitate global migration to the new protocol:

1. Cisco [CISCO], Juniper [JUNIPER], Apple, BSD [FREEBSD4], Linux [LINUX], and Microsoft [MICROSOFT] have IPv6-ready products.
2. Most personal computers have IPv6 capabilities, and are just waiting for IPv6 from access providers and/or Internet Service Providers (ISPs);
3. Wired network access technologies including cable systems [DOCSIS3] [COMCAST] and DSL systems [BBF177] are IPv6-capable;

4. Third generation (3G) cellular devices require an IP address for data and Internet access and are IPv6-capable [3GPP99] [3GPP5] [TMOBILEUSA] ; service providers are issuing statements that IPv6 will be required for Long Term Evolution (LTE) [VERIZON], WiMAX [RFC5121] and other post-3G networks;
5. Content providers such as Google [GOOGLE] [YOUTUBE], Limelight Networks and Netflix support IPv6 today; and
6. Global ISPs including AT&T, Cogent, Global Crossing, Level3, NTT, Tata Communications, and Verizon are providing IPv6 transit services.

In addition to the above, new applications are being designed to leverage the expanded addressing capabilities (and other new features) of IPv6. Two examples are Cloud Computing and Sensor Networks.

Before two devices can benefit from all the capabilities of IPv6, network components, computer operating systems, applications, services, and network security devices need to be upgraded to use IPv6. For example, a provider may offer an application over IPv6 with some unique mobility features only available on IPv6. If the IPv6-enabled application server is only reachable by devices which have implemented IPv6, then the application holds no value for users who operate using IPv4.

If an application does not require any IPv6-specific features and if the application and service provider have deployed it over the current IPv4 Internet, they will have no incentive to add IPv6 support (and incur associated deployment costs) unless it will increase their customer base.

To date, very few IPv6-only applications requiring unique IPv6 capabilities have become mainstream enough to drive the deployment of IPv6 in the general networking market.

Since the start of IPv6 deployment in 1999 [IANARIR], the recommended migration strategy has been to upgrade all devices, services and applications to be dual-stack (IPv4 and IPv6). A global upgrade to dual-stack has not yet happened because of the issues above. As a result, the deployment of IPv6 on the Internet and in enterprise networks has been minimal up to now.

3.1. Internet IPv4 becomes less reliable?

Internet routing was designed in the early years of the Internet based on the assumption that everyone was trustworthy, and would cooperate using generally understood (but non-written) rules. Issues were addressed and problems were fixed as they arose (e.g. routing). This still remains mostly the case, however there are very few guards in place to block an organization from using and announcing someone else's IP address space [WKPDIPH] [HUSTRTNG]. This issue of wrongly announcing IP address space has happened many times in the past, such as in 2002 [NET69], 2006 [CONED] and 2008 [RIPEYT]. For example, a large Asian provider made a configuration error which caused their network wrongly announce [RIPEYT] the popular YouTube IP address space. That error resulted in a major global outage for YouTube.

While engineering and standard efforts are undertaken to secure Internet routing [HUSTCERT], they will take time to be fully deployed (e.g. possibly longer than full deployment of IPv6). IPv6 networks will benefit from this work, but IPv4 routing may not.

Many organizations require large address spaces for their networks, where most of the traffic is routed privately within their networks. At the same time, they peer privately with others where the addresses used should be different. Because the private IPv4 address space available is often too small, and because the supply of IPv4 addresses is running out, some organizations have started using someone else's IPv4 address space or as yet not allocated address space.

When the unallocated address space used by these organizations becomes allocated [IPJALL], then reaching the new networks with this new address space will become impossible. This has happened many times in the past [NET69]. Therefore the new networks connecting to the Internet shall encounter more unreachability than older, previously addressed networks.

Evidence [CAIDA] [RIPEPOL] [HAMACHI] [ANONET] has shown that most of the remaining IPv4 address space is already in use by organizations. Within the few remaining IPv4 address blocks available as of January 2010, 90% of that address space [DIRTY] contains prefixes[1] which have been identified [CAIDA] as already in use by some organizations, resulting in decreased reliability. Therefore, the recipients of these prefixes, when allocated, will see unwanted traffic to their networks and many organizations will not be able to reach these recipients' networks.

In other words, the remaining address space will be less reliable to use than the IPv4 address space already in use. As the remaining address space approaches zero, it is likely that people will experience unreachability of sites and networks as well as more instability in IPv4 routing.

Reliability and stability issues in the IPv4 Internet and within enterprise IPv4 networks will have no effect on IPv6 networks. In fact, IPv6 networks should experience improved reliability and performance as more IPv6 is deployed.

Whether IPv6 networks will in fact enjoy increasing reliability or whether IPv4 networks will suffer from decreased reliability remains to be seen. However as IPv4 address space becomes more scarce, these trends and their impacts on reliability become more probable.

3.2. Secondary market?

As IPv4 address space becomes scarce, a secondary market (white or grey) for trading unused IPv4 addresses may begin to emerge. If this should happen, it may impact the overall reliability and stability of the Internet and private networks. Unclear ownership of some IPv4 addresses plus a lack of tools to block wrong addresses could lead to instability of the routing system [OPsREALITY].

1 As of January 2010, twenty-four prefixes of length /8 were still available for allocation. Twenty-two of those prefixes (i.e. 90%) were identified as used by other organisations in the [CAIDA] study.

The concern is that market forces (viz. the economics of supply and demand) will drive the secondary market for IPv4 addresses. As the supply of available IPv4 address blocks (e.g. from the RIRs) becomes scarce, demand for the remaining blocks will increase because people will perceive them to be increasingly valuable. Given that the supply of IPv4 addresses is finite and bounded, enterprises and providers requiring new or additional IPv4 address space after 2012 may incur significant costs, while IPv6 addresses will be free. The higher cost of new IPv4 address space may well become a driving factor for many organizations and force them to transition to IPv6.

4. IPv6 Deployment Status

This section provides a summary of information about IPv6 deployments in Canada's largest trading partners, and Canadian work on IPv6 to date. More details are in Annex C.

Canada's largest trading partners have embraced IPv6 for their digital economy strategies. They recognize that international trade and e-commerce depend on Internet technologies, and that the Internet is moving to IPv6. Trade accounts for most of the capital moving in and out of Canada, however Canada is lagging its trading partners on IPv6.

4.1. Global IPv6 Deployment: 2000 to 2010

From 2000 to 2008 the global uptake of IPv6 was slow for three main reasons:

- IPv6 is "on the wire" incompatible with IPv4; this means two devices which could communicate using IPv4 (e.g. clients, servers) would lose the ability to exchange data if only one of them transitioned to IPv6; the only way to avoid this was for one of the devices to run both IPv4 and IPv6 (dual-stack) or use transition mechanisms such as Network Address Translation (NAT) or tunnelling technologies.
- Corporate back-office software systems and mission-critical business applications were designed for use with IPv4-based networks, and might not work with IPv6 unless upgraded or rewritten; and
- Most organizations could not develop a business case to support implementation of IPv6. For example, Internet service providers required incremental investment if they wished to deploy IPv6, however such an investment could not guarantee incremental revenues (or cost savings) to recover to costs of the migration.

The situation began to change in 2009. The impending exhaustion of IPv4 addresses entered the consciousness of many organizations and as a result it became newsworthy. Many organizations (e.g. the OECD, ARIN, RIPE, APNIC, ISOC, IETF, ITU) focussed on raising global awareness [OECD] on the need to support IPv6:

- IPv6 support was included in almost every new computer operating system;
- IPv6 traffic doubled during 2009 [TRAFFICx2]; and
- Large industry players are deploying IPv6; Google enabled IPv6 access to YouTube in February 2010 [YOUTUBE] and created a 30:1 increase in IPv6 traffic in at least one global ISP [30xSPIKE].

As of February 2010, more than 915 million "/48" sized IPv6 address blocks were allocated.[2] Each "/48" can support 2^{80} IPv6 addresses, which is many <u>many</u> *times* more addresses than all of IPv4. Note: all of the IPv6 addresses allocated to date equal just 0.0033% of the total IPv6 space.

2 This number is derived from the count of allocated IPv6 "/48" addresses blocks, per the IPv6 distribution reports at: http://bgp.potaroo.net/iso3166/v6cc.html

Further evidence that IPv6 is now ramping up globally can be seen in Figure 3. It shows the growth of IPv6 address space actually "in use" on the Internet from 2005 until March 10, 2010.

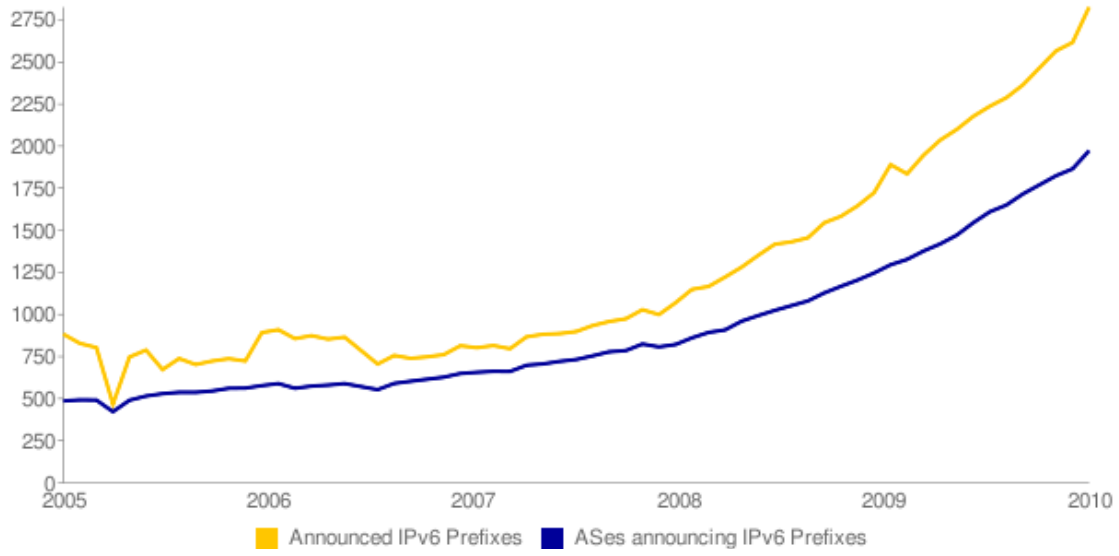


Figure 3: IPv6 addresses in use on the Internet, as seen by RIPE NCC's Routing Information Service, as of March 10, 2010 [V6ACTNOW]

The growth of announced (on the Internet) IPv6 and AS address prefixes[3] grew at a steady rate until 2008, and then the growth ramped up. The upward ramp started in 2008 because of the imminent exhaustion of the IPv4 address space. The prefixes plotted in Figure 3 are typically advertized by ISPs and large enterprises. Organizations which are downstream of an ISP are not included in the graph. Note the clear acceleration starting in 2008 and continuing through 2009 and today.

4.2. Status of IPv6 Deployment by Canada's Trading Partners

International trade represents more than 60% of Canada's GDP.

Canada trades with countries all over the world however its main trading partners are the U.S., the European Union, China, Japan and South Korea. During 2008 and 2009, trade with these partners accounted for:

- 90.1 % of all exports from Canada; and
- 79.5 % of all imports to Canada

Internet technologies provide a foundation for international trade and e-commerce, and the Internet is moving to IPv6. As can be seen from the table below, Canada's largest trading partners have accepted the need for IPv6 within their digital economy strategies, and are already transitioning their digital economies to IPv6.

[3] An Autonomous System (AS) is a group of IP networks run by one or more network operators with a single, clearly defined routing policy. An AS is also sometimes referred to as a routing domain. [ASDEFN]

	Canadian Trade with Partners, January 2008 to December 2009	Share of Total Exports	Share of Total Imports	Share of IPv6 '/48s' Allocated To Date	Share of IPv6 '/48s' Allocated Per Capita
1	United States	76.53%	51.82%	10.76%	4.32
2	European Union *excluding* the UK	4.86%	9.67%	18.40%	4.01
3	China	2.57%	10.30%	0.05%	0.01
4	Japan	2.30%	3.46%	5.97%	5.72
5	UK	2.96%	2.76%	0.90%	1.76
6	South Korea	0.87%	1.49%	3.71%	9.08
~15	India	0.54%	0.53%	0.02%	0.03
~20	Australia	0.47%	0.41%	5.92%	31.70
	Total	**91.1%**	**80.4%**	**45.7%**	
	Canada	*n/a*	*n/a*	0.06%	0.21

Sources of Data: Statistics Canada and the Regional Internet Registries (RIRs)
Report Date: 23-Feb-2010
http://www.ic.gc.ca/eic/site/tdo-dcd.nsf/eng/Home
http://bgp.potaroo.net/iso3166/v6cc.html

With the exception of China, all of Canada's most significant trading partners already have many more IPv6 addresses reserved for use in their digital economies, both in absolute terms and per capita. Canada's overall awareness of IPv6 and general state of readiness to transition to the new protocol is lagging.

Detailed information about the status and history of IPv6 deployment initiatives by Canada's main trading partners is provided in Annex C. A subset of Annex C is summarized below.

United States:

- In June 2003, the U.S. Pentagon's chief information officer directed that all new equipment procured by the Pentagon must be IPv6-compliant starting in 2008 [DOD].
- In August 2005, the U.S. Office of Management Budget (OMB) issued Memorandum 05-22, "*Transition Planning for Internet Protocol Version 6 (IPv6)*", which outlined a strategy for all civilian USG agency backbone networks to be capable of carrying both IPv4 and IPv6 traffic by June 30, 2008 [USOMB] [USFAQ].
- In May 2009, a U.S. Federal CIO Council published a *"Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government"* [USGCIO]. The document directed USG CIOs, chief architects and other government IT leaders to:
  - Develop IPv6 migration plans for their agencies by December 2009; and
  - Execute their IPv6 transition plans between January 2010 and December 2011.

- In December 2009, the U.S. Government issued a Federal Acquisition Regulation which elevated NIST's IPv6 profile into a hard requirement for ICT procurements [USGv6FAR].

Europe:

- In May 2008, the EC announced consensus on an "Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe". [ECPLAN]
- The goal is for 25% of EU users to be able to access to the IPv6 Internet and their most important content and service providers without noticing a major difference compared to IPv4, by the end of 2010. [EUPLAN]

China:

- In December 2009, China Telecom announced their timetable for commercial IPv6 services as follows [CHINATEL]:
    - 2009: IPv6 trial begins;
    - 2012: IPv6 becomes available for large scale commercial use; and
    - 2015: IPv4 is retired.

Japan:

- Japanese Prime Minister Yoshiro Mori made a statement about the importance of IPv6 research in a policy speech at the start of the 150th Session of the Diet in September 2000. He said:
    - *"We shall aim to provide a telling international contribution to the development of the Internet through research and development of state-of-the-art Internet technologies and active participation in resolving global Internet issues in such areas as IP version 6 (IPv6)."* [DIET]
- NTT launched commercial IPv6 services in 2003 spanning Asia, Europe, North America and Australia, and a domestic High Definition IPTV service using IPv6 in 2008 [HIKARITV].

Republic of Korea:

- The Korean government published a *"Plan for accelerating adoption of IPv6"* that required research networks to adopt IPv6 by 2008, and to provide IPv6 as a test bed network for communications equipment vendors and ISPs. The plan mandated that public sector networks and systems support both Internet Protocol version 4 (IPv4) and IPv6 by the end of 2010.
- Korea Telecom is working to transition Korean public sector e-Government services to IPv6, in support of the Korean Government's IPv6 deployment plan produced by the National Internet Development Agency of Korea [NIDA].

4.3. Status of IPv6 Deployment in Canada

In the first years of IPv6 deployment, Canada had some global IPv6 leadership. Today, much work is needed for Canada to regain the IPv6 initiative.

4.3.1. Early Innovators

CRC, CANARIE , Viagénie, Teleglobe, and Hexago and were some of Canada's early pioneers in the development of IPv6.

CRC first installed an IPv6 router in their BADLab in September 1998, and by mid-2000 had deployed an IPv6 network for CRC researchers and its GigaPop clients [GIGAPOP], including the Canadian Space Agency, the Department of National Defence (DND) and the Ottawa Center for Research and Innovation (OCRI).

Starting in October 1998, production native IPv6 (over ATM) interconnections were established between **CANARIE**, ESnet, Internet2/vBNS, Cairn and WIDE using testing IPv6 address space from the IETF's 6bone project [6REN]. In 1999, **CANARIE** helped the U.S. DoE's ESnet to design and deploy a common connection and peering point for all worldwide IPv6 research networks [ESnet] called the IPv6 Transit Access Point (6TAP) in Chicago [6TAP].

Viagénie created the Freenet6 service in 1999. Freenet6 is an IPv6 access service using IPv6-over-IPv4 tunnel broker technology, which has enabled many thousands of users to experience IPv6. Freenet6 moved from experimental status to real deployment in February 2003 [FREENET], and **Teleglobe** (now Tata Communications) began hosting the service in October 2005. The service is still in operation today [GOGO6].

The Federal GigaPOP was the first Internet eXchange (IX) of any kind in Canada to provide IPv6, starting in July 2002. That was soon followed by OttIX, the first public IX in Canada, and then by TorIX (the largest IX in Canada).

OttIX supplied 6to4 tunnel services to all of its members in July 2002, and extended their services to the CANARIE network in 2005. OttIX was completely IPv6 and IPv4 (dual-stack) in 2002, and still is today.

In 2002, the Government of Canada committed $110 million to **CANARIE** for the design, deployment, and operation of CAnet 4 [GOC]. CA*net 4 deployed IPv6 in a production environment by the end of 2002. Since then, all versions of the CANARIE network have provided partial IPv6 reach for Research and Education (R&E) traffic only. This has been a great benefit to researchers on the forefront of IPv6 innovation in Canada.

Hexago provided IPv4-IPv6 tunnel broker technology into the U.S. Defense Research and Engineering Network (DREN) - the U.S. DoD's first IPv6 pilot network in July 2003.

- In July 2005, DREN carried IPv6 traffic between 200 end-user sites including supercomputing sites, advanced research sites, universities, and Internet2, but only a few of sites were IPv6-enabled;

- "IPv6 connectivity from anywhere" was a key Enterprise-level challenge;
- Connectivity was complicated by the variety of operating systems on the users' desktop computers, many of which had no IPv6 capabilities at the time; and
- DREN solved their Enterprise connectivity challenge by installing a pair of **Hexago**4 Gateway6 tunnel brokers, one for users at IPv4-only DREN sites, and one for users on the Internet [DREN].

The National Research Council of Canada operates a national backbone, NRNet II, which has been running IPv6 and IPv4 (dual-stack) since February of 2007. The same is true in the NRC's Ottawa campus although most institutes have not yet adopted IPv6. NRC very recently started obtaining IPv6 global connectivity via TorIX.

4.3.2. Service Providers Offering IPv6 in Canada

It is worth noting that major Canadian ISPs such as Allstream, Bell, Rogers, Shaw, Telus and Videotron among others, already have IPv6 address space. None of them are offering IPv6 services on a large scale basis. However, they acknowledge that large scale adoption of IPv6 is imminent and are currently preparing and experimenting in view of commercial development of IPv6 for their business and consumer customers. It is also anticipated that IPv6 support will be an essential feature in their LTE and post-3G networks development as stipulated in the associated standards. Appendix C contains a list of Canadian service providers with IPv6 address space.

CANARIE is currently augmenting its IPv6 service by making full IPv6 routing available over the CANARIE network. In order to achieve that goal, CANARIE will add transit connections to a number of IPv6 suppliers. This implementation will alleviate the consequences of partial routing created by insufficient presence of IPv6 providers in Canada. The most common issues experienced by institutions are bottlenecks, policy bypass, and inability to connect properly to international colleagues. CANARIE also plans to provide technical assistance to provincial networks so the Canadian R&E community makes full and faster use of the new service.

Tata Communications (formerly Teleglobe) as a Tier-1 international provider offers global IPv6 transport services today, on a wholesale basis (e.g. to "retailers" including Canadian ISPs) today. A number of other IPv6 service providers suppliers (e.g. Hurricane Electric, NTT) also have points of presence in Canada.

A number of Canadian cities have public and private local Internet eXchanges (IXs). The largest public IXs are Torix.net in Toronto with 128 members and 36Gb/s+ of traffic, Ottix in Ottawa, and CANIX/QIX in Montreal. Torix began interconnecting IPv6 traffic in 2006; Ottix started in 2003. There are also a number of IXs in the Research & Education world, in addition to the Federal Gigapop.

Many of the regional R&E networks such as Quebec's RISQ have been IPv6 enabled for some time, but this connectivity does not reach the research labs in the campuses in Quebec without the active action of overworked IT people at the actual universities. The same has typically been the case in other R&E networks across Canada and the U.S.

At this point, a number of smaller ISPs including teksavvy.net, ncf.ca, storm.ca, and egate.com have deployed IPv6 into parts of their networks using combinations of tunnelling, local peering, and the purchase of transit at torix.net. Some are advertising it, while others are providing it on a request basis, with best-effort support. Reports are that there remain some issues with suppliers and some missing gaps in technology. One such example is spam filters that are IPv6 aware.

4.3.3. Quebec Government Network

The Quebec Government issued an RFP for its next generation network, named "Réseau intégré de télécommunications multimédia" during April 2008. The RFP included context on why IPv6 was needed.

> *"La problématique potentielle réside dans l'utilisation de la même plage d'adresses 10.X.X.X par plusieurs réseaux clietns et par les établissements hospitaliers pour accéder à des services partagés tels que la téléphonie IP, la visioconférence et autres applications."* [QCGOVRFP]

The RFP stated clearly that the IPv6 service shall be at par with IPv4 service.

> *"Le niveau de service du service IPv6 doit être identique ou supérieur au service IPv4. Le niveau de sécurité du service IPv6 doit être identique ou supérieur au service IPv4."* [QCGOVRFP]

5. Time for Action on IPv6 in Canada

The imminent exhaustion of IPv4 addresses makes it necessary to proactively transition to IPv6. IPv6 will alleviate IPv4 address space depletion, solve key scalability issues (e.g. auto-configuration of customer premises equipment), and improve network security and device mobility.

Despite a lot of early, pioneering work on IPv6 by Canadians (as described in section 4.3), very few Canadian ISPs, enterprise networks or other internet stakeholders have started their transition to IPv6. Canadian IPv6 expertise is held by a few organizations and people in Canada today.

Given that IPv4 addresses will run-out within the next 24 months, there is a clear need to multiply the small base of IPv6 expertise that exists in Canada in 2010, in order to assist Canadian organizations to transition to IPv6 by 2011-2012.

As discussed in section 4.1, the imminent exhaustion of IPv4 address space has become news and is triggering increased deployment of IPv6, especially IPv6-only networks and products. IPv6-only networks will result in applications, services and end-users reachable only by IPv6. Therefore, as shown in Table 1, current IPv4-only devices, networks and applications must be upgraded in order to reach the new IPv6 Internet. This market will be a growth market in the next years, as IPv4 deployment is flattening given the address exhaustion.

Therefore, urgent action on IPv6 support and implementation is required by Canadian ICT suppliers and service providers, government and private sector CIOs, content owners and distributors, software designers, applications developers, and trainers.

5.1. Migration Plan

A lot of mainstream networking products are IPv6-capable and ready: IPv6 just needs to be activated in order to use it, or a software upgrade. Not every networking product is IPv6-capable, but mainstream routers, network devices, operating systems and applications are.
Careful advanced planning has shown to significantly lower the cost of the migration to IPv6. As stated by Google engineers [IETFJ] about the migration of the Google services to IPv6:

> *"It costs less than you think it would. You don't have to spend much money on it if it's part of your upgrade process."*

A typical first step in these plans is to require IPv6-compliant products in all the future purchasing, to ease the upgrade process as IPv6 deployment starts.

Canadian content from governments of all levels, such as federal, provincial, territorial, regional and municipal, as well as content providers such as CBC/Radio-Canada should plan now to offer their content over IPv6. This will become soon a requirement to reach the end-users served only over IPv6.

John Curran, CEO of the American Registry for Internet Numbers (ARIN) stated [CURRAN]:

> *"Corporations and government agencies must IPv6-enable their public-facing Web sites in the next 24 months or risk upsetting a growing number of visitors with*

lower-grade connectivity. ... The drop-dead deadline for external Web sites to support IPv6 is January 1, 2012."

As well, Canadian enterprises shall plan to deploy IPv6 to be able to communicate with IPv6-only users coming online soon.

5.2. Expertise and Awareness

Because of the minimal IPv6 deployment up to now, the knowledge on how to migrate networks to IPv6, including costs, impacts, risk assessments, technology, security and planning is concentrated in a too low number of individuals and organizations.

The consciousness of the imminent IPv4 address exhaustion has not yet reached all sectors of the ICT industry or other Canadian industry segments. Therefore, the Canadian marketplace has to be made aware of the need to transition their products and services to be IPv6-ready for domestic and international communications and e-commerce.

5.3. Growth is in IPv6 market

The recent changes in the dynamics of the industry caused by the imminent exhaustion of IPv4 address space requires that Canadian products to be IPv6-compliant, to serve these growing markets. As discussed in section 4, other countries and governments have been active in pushing IPv6 products and deployments. These initiatives create requirements for products and services to be IPv6-capable. The Canadian industry has to be aware of the opportunities and consequences if its products are not IPv6-compliant in time.

Major network operators such as China Telecom [CHINATEL] are not only deploying IPv6, but also planning to deprecate IPv4 by 2015. In these networks, a product which is IPv4-only cannot be sold.

Over time, the delay of delivering IPv6-capable products may hinder the Canadian ICT industry. Canada's largest trading partners have embraced IPv6 for their digital economy strategies. They recognize that international trade and e-commerce depend on internet technologies, and that the Internet is moving to IPv6. Trade accounts for most of the capital moving in and out of Canada, however Canada is lagging its trading partners on IPv6.

5.4. Certification and Interoperability Testing

While developing IPv6-ready products, the Canadian ICT industry needs a way to certify and verify the interoperability of its new IPv6 products. As discussed in Annex C and Annex E, other countries have facilitated the creation of testing facilities to enable the validation, testing and certification of newly developed IPv6 products for their domestic markets, and for export. Similar facilities are needed for the Canadian ICT industry.

5.5. Universal Transport

The Internet Protocol is becoming the universal networking layer for the transport of media, video content, and telephony, in addition to e-mail and e-commerce. As a result, telecom regulation borders are blurring: IP is at the edge of regulation. Therefore, any regulation regarding content or telecommunications should take both IPv4 and IPv6 into account. As IPv6-only networks, services, applications and end-users are deployed, more content will be distributed over IPv6 transport.

We are now watching the entire global networking and ICT industry move to deploy IPv6 networks and services.

5.6. Consequences of Not Acting

As the overall economy relies so much on telecommunications and Internet, an organization, government or enterprise cannot afford to be late in connecting to the new version of the Internet. Opportunities will be missed.

Experience has shown that transitioning to IPv6 can take several years. This should be a red flag for Canada, as the last IPv4 address blocks will be depleted in *less than* two years.

As of February 19th 2010, just 8% of all IPv4 address blocks were left. At the current rate of consumption, the last block of IPv4 addresses will be allocated in September 2011. After that, there will be no more new IPv4 addresses. Future assignments will have to use IPv6 addresses.

Urgent action on IPv6 support and implementation is required by Canadian ICT suppliers and service providers, government and private sector CIOs, content owners and distributors, software designers, applications developers, and trainers.

6. Recommendations

Based on the assessment of the situation in Canada and in the world described in the previous sections, the ISACC IPv6 Task Group concluded with a series of recommendations for Canadian governments, Internet service providers, content and application service providers, industry (all sectors) and CRTC. These recommendations are detailed in this section.

6.1. Governments

Canadian governments, as owners of large IT infrastructures, need to protect their own investments by carefully planning for the migration to IPv6.

As broadband and wireless networks users will soon use IPv6, the public content of the governments shall be available by IPv6. As the world is moving to IPv6, including Canada's trading partners and defence allies, the internal and external networks, computers and applications of governments shall be migrated to IPv6.

An IPv6 migration plan includes requiring IPv6-capable products in procurement, IPv6 training of IT staff, and IPv6 capabilities as part of the ongoing life-cycle management of infrastructure. Careful and in-advance planning and preparation has shown much lower costs than a last minute migration.

Therefore, the ISACC IPv6 Task Group recommends that:

- *Canadian governments of all levels (e.g. federal, provincial, territorial, regional, municipal) shall plan for IPv6 migration and specify IPv6 support in their IT procurements immediately.*

6.2. Internet Service Providers

Canadian ISPs are delivering Internet services to Canadian enterprises and citizens. A delay in offering IPv6 Internet service will result in Canadian enterprises and citizens to be disadvantaged in accessing Internet IPv6 services, applications and content worldwide. The Canadian businesses needing IPv6 to communicate with their international and regional partners and customers will be at a disadvantage. If this happens, then the Canadian networks would be in a fractured position against other countries.

Therefore, the ISACC IPv6 Task Group recommends that:

- *Canadian Internet Service Providers (ISPs) shall accelerate the deployment and the commercial availability of IPv6 services for business and consumer networks.*

6.3. Content and Application Service Providers

The Canadian content and applications will be hurt if their services are not accessible to the new users and enterprises using IPv6. Content and applications shall be available to the whole Internet, now IPv4 and IPv6, instead of a fraction of it. For example, Radio-Canada/CBC should deliver all its content over IPv6 in the near future.

Therefore, the ISACC IPv6 Task Group recommends that:

- *Canadian internet content and application service providers shall make their content and applications reachable using IPv6.*

6.4. Industry

Not only the electronics market, but also an increasing number of household and industrial devices are becoming intelligent and networked. Industry segments which do not have networking and Internet as their core business, are most likely not paying attention to the migration to IPv6. Many will be surprised when their customers require IPv6 support in their products. Therefore the Canadian industry, as a whole, should be made aware of the upcoming migration to IPv6 in order to upgrade their products in time.

Therefore, the ISACC IPv6 Task Group recommends that:

- *Canadian industries in all sectors shall intensify the support of IPv6 on all products that include a networking protocol stack.*

6.5. Canadian IPv6 Center of Excellence

As discussed in sections 4.3 and 5.2, Canadian expertise on IPv6 currently resides in a small number of organizations and people. Therefore, there is a clear need to multiply that expertise to help all organizations to migrate to IPv6.

An industry-led Canadian Center of Excellence (CoE) for IPv6 is needed to increase awareness, to create a community of subject matter experts, to share best practices about adoption of IPv6, to facilitate discussion and collaboration with other agencies in U.S. and elsewhere for education and training purposes, and to create focus groups to recommend mechanisms to encourage the deployment of IPv6 and facilitate the establishment of an IPv6 conformity and interoperability testing lab for hardware and software which is open to both governments and industry.

Terms of Reference for a Canadian IPv6 Center of Excellence have been drafted and are included in Annex D.

Therefore, the ISACC IPv6 Task Group recommends that:

- *Canadian industry and governments shall establish a Center of Excellence to increase IPv6 awareness in Canada, by offering training and education, advice and the sharing of best practices.*

6.6. Government Support Programs

Current government programs such as the federal and provincial Scientific Research and Experimental Development (SRED) program, the National Research Council's Industrial Research Assistance Program (IRAP) and Industry Canada's "Broadband Canada: Connecting Rural Canadians" programs are intrinsically dependent on IPv4 and the current Internet. These programs should be reviewed to ensure that IPv6-related initiatives are eligible and supported. Without such reviews, it is possible that new investments will be made on legacy technologies (e.g. IPv4), which would not be money well spent.

As discussed in section 4.2, the governments in many countries have been actively helping their industries to create IPv6-capable products for their domestic markets, and to have a competitive edge for exports. Canadian governments at all levels should actively assist Canadian industries to compete on the same level in the global market by creating or adapting programs to support growth in the IPv6 market.

Therefore, the ISACC IPv6 Task Group recommends that:

- *Governments at all levels shall review current programs to ensure eligibility of IPv6 initiatives and evaluate the creation of specific programs to enable Canadian industry to take full advantage of global IPv6 markets.*

6.7. CRTC

The Internet is increasingly being used to transport telecommunications and broadcasting content to end-users, replacing traditional media networks such as cable, satellite and air waves.

Therefore, the IPv4 Internet is on the edge of the CRTC mandate. Since the Internet is moving to IPv6, any CRTC policies or work that relates to the IPv4 Internet, directly or indirectly, must also take into account the upcoming IPv6 Internet. Current and future regulatory decisions have the potential to either support or deter the deployment of IPv6 in Canada.

Therefore, the ISACC IPv6 Task Group recommends that:

- *The CRTC shall ensure that relevant telecommunications and broadcasting decisions and policies support IPv6 deployment;*

7. Conclusion

The ISACC IPv6 Task Group met fifteen times from July 2009 to March 2010, and reached consensus that:

- IPv6 is inevitable, and a global migration to IPv6 has begun;
- Not migrating is not an option;
- All of Canada's largest trading partners are actively transitioning to IPv6; and
- Canada is lagging in this transition.

Canada's migration to IPv6 will require action by governments and private sector members of the economy, after a sufficient level of awareness and understanding is instilled in Canadian stakeholders about the need for IPv6.

To facilitate the creation of awareness in Canada, and perhaps to aid Canadians in the move to IPv6, the IITG believes that one of the next steps required is the formation of a Canadian Centre of Excellence on IPv6, per the draft Terms of Reference contained in Annex D.

Canadian governments and/or organizations wishing to become more familiar with IPv6 in the short term should review the references cited throughout this report (as summarized in Annexes A and B), and study publicly available IPv6 reports, planning guides and other documents recently published by the US Government, many of which are described in Appendix B.

Annex A - References

[30xSPIKE] "YouTube support of IPv6 seen in Dramatic Traffic Spike", Carolyn Duffy Marsan, NetworkWorld, February 1, 2010, http://www.networkworld.com/news/2010/020110-youtube-ipv6.html

[3GPP5] "General Packet Radio Service (GPRS); Service description", 3GPP TS 23.060 version 5.1.0 (release 5).

[3GPP99] "General Packet Radio Service (GPRS); Service description; Stage 2", 3GPP, TS 23.060 V4.1.0

[6REN] 6REN Overview Information, Bob Fink, ESnet, January 29, 1999, http://mailman.isi.edu/pipermail/6bone/1999-January/001905.html

[6TAP] "Operational Experience with IPv6", Bob Fink, June 2000, http://www.nanog.org/meetings/nanog19/presentations/fink.ppt

[ANONET] Wikipedia, "AnoNet", http://en.wikipedia.org/wiki/AnoNet

[ARCHROCK] "Wireless vendor simplifies IPv6 sensor networks", John Cox, NetworkWorld, March 2008, http://www.networkworld.com/news/2008/033108-arch-rock-ipv6.html

[ASDEFN] Definition of Autonomous Systems and AS Numbers, RIPE NCC, March 2010, http://www.ripe.net/rs/as/

[BBF177] "Migration to IPv6 in the context of TR-101", Broadband Forum, WT-177.

[CAIDA] "Searching for Evidence of Unallocated Address Space Usage in DITL 2008 Data", Duane Wessels, June 4, 2008, https://www.dns-oarc.net/files/dnsops-2008/Wessels-Unused-space.pdf

[CHINATEL] "China Telecom Issues Complete IPv6 Schedule, Commercial Launch Set for 2012", CircleID, December 23, 2009, http://www.circleid.com/posts/china_telecom_issues_complete_ipv6_schedule_commercial_launch_2012/

[CISCO] http://www.cisco.com/ipv6

[COMCAST] "Preparing for the IPv6 Transition", Jason Livingood, January 27, 2010, http://blog.comcast.com/2010/01/preparing-for-the-ipv6-transition.html

[CONED] "Con-Ed Steals the 'Net", Todd Underwood, January 22, 2006, http://www.renesys.com/blog/2006/01/coned-steals-the-net.shtml

[CONTENT] "Google's leading, but where do other Web giants stand on IPv6?", Carolyn Duffy Marsan, Network World, February 4, 2010, http://www.networkworld.com/news/2010/020410-ipv6-web-sites.html

[CURRAN] "Web sites must support IPv6 by 2012, expert warns", Carolyn Duffy Marsan, Network World, January 21, 2010, http://www.networkworld.com/news/2010/012110-ipv6-warning.html

[DIET] "Policy Speech By Prime Minister Yoshiro Mori To The 150th Session Of The Diet", September 21, 2000, http://www.kantei.go.jp/foreign/souri/mori/2000/0921policy.html

[DIRTY] "Remaining IPv4 /8 prefixes are dirty", Marc Blanchet, February 7, 2010, http://marcblanchet.blogspot.com/2010/02/remaining-ipv4-8-prefixes-are-dirty.html

[DOCSIS3] "CableLabs Issues DOCSIS® 3.0 Specifications Enabling 160 Mbps", CableLabs, August 7, 2006, http://www.cablelabs.com/news/pr/2006/06_pr_docsis30_080706.html

[DOD] "Briefing on New Defense Department Internet Protocol", John Stenbit, June 13, 2003, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2747

[DREN] "DREN Helps Transition to IPv6", U.S. DoD High Performance Computing Modernization Program, http://gogoware.gogo6.com/4105/file.asp?file_id=826

[ECPLAN] "Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe", Commission of the European Communities, EC Document, 2008, http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/comm-ipv6-final_en.pdf

[ESnet] "Next-Generation Internet Protocols Debut at ESnet", January 26, 2000, http://www.lbl.gov/Science-Articles/Archive/esnet-ipv6.html

[EUPLAN] "Action Plan for the deployment of IPv6 in Europe", EC Slide Presentation, P.9, March 2009, http://www.ogf.org/OGF25/materials/1503/action-plan-ipv6.pdf

[FREEBSD4] "FreeBSD 4.0 Release Notes", FreeBSD Project, March 2000, http://www.freebsd.org/releases/4.0R/notes.html

[FREENET] "Get IPv6 now with Freenet6", Linux Journal, January 1, 2003. http://www.linuxjournal.com/article/5988

[GIGAPOP] "IPv6 Operational Experience at CRC", William F. Maton, June 2000, http://www.nanog.org/meetings/nanog19/presentations/maton.ppt

[GOC] "Industry Canada and CANARIE Inc. Partner to build CA*Net4", April 29, 2002, http://www.ic.gc.ca/eic/site/ic1.nsf/eng/02787.html

[GOGO6] "About gogo6", http://gogoware.gogo6.com/4105/about.asp

[GOOGLE] "Access Google services over IPv6", Google, March 2008, http://www.google.com/intl/en/ipv6/

[HAMACHI] "Hamachi", http://en.wikipedia.org/wiki/Hamachi

[HIKARITV] "NTT details IPv6-powered IPTV Service", Carolyn Marsan Duffy, Network World, January 8, 2009, http://www.networkworld.com/news/2009/010809-ntt-ipv6-tv.html

[HUSTCERT] "Resource Certificates", Geoff Huston, December 2008, http://www.potaroo.net/ispcol/2008-12/resourcecertificates.html

[HUSTRTNG] "Tubular Routing", Geoff Huston, March 2008, http://www.potaroo.net/ispcol/2008-03/routehack.html

[IANARIR] "Delegation of IPv6 address space", IANA, July 1999, http://www.iana.org/reports/1999/ipv6-announcement.html

[IETFJ] "Google: IPv6 Is Easy, Inexpensive", Carolyn Marsan Duffy, January 20, 2010, IETF Journal, Volume 5, Issue 3, http://www.isoc.org/tools/blogs/ietfjournal/?p=1515#more-1515

[IPJALL] "Awkward /8 Assignments", Leo Vegoda, Internet Protocol Journal, Volume 10, No. 3, September 2007, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-3/103_awkward.html

[IPv4ADDREP] "IPv4 Address Report", Geoff Huston, February 2010, http://ipv4.potaroo.net

[JUNIPER] https://www.juniper.net/us/en/company/press-center/press-releases/2001/pr-011128.html

[LINUX] "The history of IPv6 in Linux", Peter Bieringer, December 2009. http://tldp.org/HOWTO/Linux+IPv6-HOWTO/basic-history-ipv6-linux.html

[MICROSOFT] http://www.microsoft.com/ipv6

[NET69] "The 69.0.0.0/8 Problem", April 2003, http://puck.nether.net/~jared/papers/69-paper.htm]

[NIDA] "IPv6 Transition Status in Korea", Joonhyung Lim, National Internet Development Agency of Korea (NIDA), 9 July 2009, http://www.apan.net/meetings/kualalumpur2009/proposals/IPv6/IPv6%20Status%20of%20Korea.pdf

[NRO10] "Less than 10% of IPv4 Addresses Remain Unallocated", Number Resource Organization, January 2010, http://www.nro.net/media/less-than-10-percent-ipv4-addresses-remain-unallocated.html

[OBAMAGRID] "Obama's Smart Grid Game Plan", BusinessWeek, October 27, 2009, http://www.businessweek.com/technology/content/oct2009/tc20091027_594339.htm

[OECD] "Internet Address Space: Economic Considerations in the Management of IPv4 and in the Deployment of IPv6", OECD, June 2008, http://www.oecd.org/dataoecd/7/1/40605942.pdf

[OECDSG] "Smart Sensor Networks: Technologies and Applications for Green Growth", OECD, December 2009, http://www.oecd.org/dataoecd/39/62/44379113.pdf

[OPsREALITY] "IPv6 Transition & Operational Reality", Presentation to AFNOG by Randy Bush, June 2008, http://www.afnog.org/afnog2008/conference/talks/IPv6_Transition.pdf

[QCGOVRFP] Centre de services partagés, Gouvernement du Québec, "Infrastructure de services de transmission de données pour le Réseau intégré de télécommunications multimédia, Appel d'offres 999101702", 25 avril 2008.

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981, http://www.ietf.org/rfc/rfc791.txt

[RFC1752] Bradner, S. and A. Mankin, "The Recommendation for the IP Next Generation Protocol", RFC 1752, January 1995, http://www.ietf.org/rfc/rfc1752.txt

[RFC1883] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 1883, December 1995.

[RFC5121] Patil, B., Xia, F., Sarikaya, B., Choi, JH., and S. Madanapalli, "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", RFC 5121, February 2008.

[RIPEPOL] RIPE, "Pollution in 1/8", February 3, 2010, http://labs.ripe.net/content/pollution-18

[RIPEYT] RIPE, "YouTube Hijacking: A RIPE NCC RIS case study", http://www.ripe.net/news/study-youtube-hijacking.html]

[SOLENSKY] "Continued Internet Growth", Proceedings of the 18th Internet Engineering Task Force, August 1990, http://www.ietf.org/proceedings/prior29/IETF18.pdf

[TMOBILEUSA] "IPv6-only UE -- beta deployment report", Cameron Byrne, February 23, 2010. http://www.ietf.org/mail-archive/web/3gv6/current/msg00269.htm

[TRAFFICx2] "Hurricane Electric's IPv6 network doubles", NetworkWorld, November 20, 2009, http://www.networkworld.com/news/2009/112009-hurricane-electric-ipv6.html

[USFAQ] "Federal Government Transition, IPv4 to IPv6 Frequently Asked Questions", U.S. Government, February 15, 2006, http://www.cio.gov/Documents/IPv6_FAQs.pdf

[USGCIO] "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government", USG CIO Council, May 2009, http://www.cio.gov/Documents/Planning_Guide-Roadmap_Toward_IPv6_Adoption_in_USG_May-2009.zip

[USGv6FAR} U.S. Government IPv6 Federal Acquisition Regulation, December 2009, http://edocket.access.gpo.gov/2009/pdf/E9-28931.pdf

[USOMB] Executive Office of the President – Office of Management and Budget, "Transition Planning for Internet Protocol Version 6 (IPv6)", M-05-22, August 5, 2005, http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf

[V6ACTNOW] IPv6 address space in use on the Internet, seen by RIPE NCC's Routing Info Service (RIS), March 12, 2010, http://www.ipv6actnow.org/info/statistics/

[VERIZON] "Device Requirements, LTE 3GPP Band 13 Network Access Version 1.00", Verizon Wireless, December 2009, https://www22.verizon.com/opendev/index.aspx

[WKPDIPH] Wikipedia, "IP Hijacking", http://en.wikipedia.org/wiki/IP_hijacking

[YOUTUBE] "YouTube Calls on IPv6", Lorenzo Colitti, Steinar H.Gunderson, February 5, 2010, http://youtube-global.blogspot.com/2010/02/youtube-calls-on-ipv6.html

Annex B - Links to Additional IPv6 Reference Information

ARIN's IPv6 wiki:
http://www.getipv6.info/index.php/First_Steps_for_ISPs

Geoff Huston's pages:
http://www.potaroo.net/

Internet Society (ISOC) IPv6 pages:
http://www.isoc.org/educpillar/resources/ipv6.shtml

IPv6 Forum:
http://www.ipv6forum.com/

ITU's IPv6 pages:
http://www.itu.int/net/ITU-T/ipv6/

OECD Ministerial Background report about IPv4 and IPv6:
http://www.oecd.org/dataoecd/7/1/40605942.pdf

RIPE's IPv6 resource page:
http://www.ipv6actnow.org/info/statistics/#alloc

SIXXS, for their prefix visibility tool and ULA tool:
https://www.sixxs.net/tools/grh/dfp/

Annex C - IPv6 Deployment by Canada's Trading Partners

This Annex describes the status of IPv6 deployment initiatives in Canada's largest trading partners plus two other countries (viz. Australia and India).

Canada trades with countries all over the world however its main trading partners are the U.S., the European Union, China, Japan and the Republic of Korea. During 2008 and 2009, trade with these partners accounted for:

- 90.1 % of all exports from Canada; and
- 79.5 % of all imports to Canada

	Canadian Trade with Partners, January 2008 to December 2009	Share of Total Exports	Share of Total Imports	Share of IPv6 '/48s' Allocated To Date	Share of IPv6 '/48s' Allocated Per Capita
1	United States	76.53%	51.82%	10.76%	4.32
2	European Union *excluding* the UK	4.86%	9.67%	18.40%	4.01
3	China	2.57%	10.30%	0.05%	0.01
4	Japan	2.30%	3.46%	5.97%	5.72
5	UK	2.96%	2.76%	0.90%	1.76
6	Republic of Korea	0.87%	1.49%	3.71%	9.08
~15	India	0.54%	0.53%	0.02%	0.03
~20	Australia	0.47%	0.41%	5.92%	31.70
	Total	**91.1%**	**80.4%**	**45.7%**	
	Canada	*n/a*	*n/a*	0.06%	0.21

Sources of Data: Statistics Canada and the Regional Internet Registries (RIRs)
Report Date: 23-Feb-2010
http://www.ic.gc.ca/eic/site/tdo-dcd.nsf/eng/Home
http://bgp.potaroo.net/iso3166/v6cc.html

C.1. IPv6 in the United States

> *"The capabilities of IPv6 will provide many advantages beyond IPv4 (e.g. infrastructure management, wireless networking and mobility, information assurance, interoperability, and convergence)." - Office of Enterprise Architecture Management, U.S. Department of Veterans Affairs, January 2006* [4]

4 http://www.ea.oit.va.gov/apps/eas/4_3/extDocs/ea/IPv6/EA%20Guidance%20for%20Transition.pdf

"We can't keep operating in an IPv4 world when we're talking about sensor networks, wireless communications and mobile networks. We need more IP addresses - globally unique IP addresses - and that's what IPv6 provides. We need a target network architecture that's scalable, secure and stable." - Pete Tseronis, Federal IPv6 Working Group Chair and Deputy Associate CIO of the U.S. Department of Energy, June 2009

C.1.1. History of IPv6 in the U.S. Public Sector

The U.S. Government (USG) was an early sponsor of IPv6 deployment in the United States. The USG began its support for IPv6 research, testing and standardization in the 1990's. The USG also directed their Department of Defence and all USG civilian agencies to implement IPv6 capability in their backbone networks by mid-2008.

- In 1998, the very-high-performance Backbone Network Service (vBNS), sponsored by the National Science Foundation for use by researchers and engineers, pioneered the first production deployment of IPv6 in the U.S.[5]
- In 1999, Lawrence Berkeley National Laboratory designed and built the Energy Sciences network (ESnet) for the U.S. Department of Energy (DoE). ESnet provided thousands of scientific researchers across more than thirty DoE sites with IPv6 operating capability, and is still operating today.
- Also in 1999, ESnet partnered with Canada's advanced Internet development organization (CANARIE) to create a common connection and peering point for early IPv6 research networks[6] called the IPv6 Transit Access Point (6TAP) in Chicago.[7]
- In June 2003, the Pentagon's chief information officer directed that all new equipment procured by the Pentagon must be IPv6-compliant starting in 2008.[8]
- In August 2005, the U.S. Office of Management Budget (OMB) issued Memorandum 05-22, *"Transition Planning for Internet Protocol Version 6 (IPv6)"*, which outlined a strategy for all civilian USG agency backbone networks to be capable of carrying both IPv4 and IPv6 traffic by June 30, 2008.[9]
- In coordination with OMB, the National Institute of Standards and Technology (NIST) developed new standards and testing infrastructures to support agency plans for IPv6 adoption. One of NIST's key initiatives was the creation of *"A Profile for IPv6 in the U.S. Government (USGv6)"* for vendors to implement and against which their products could be tested.[10]

The USG's focus on IPv6 may have accelerated IPv6 service availability from three of the world's largest service providers: AT&T, Sprint-Nextel, and Verizon. All three were awarded contracts

5 http://en.wikipedia.org/wiki/VBNS
6 http://www.lbl.gov/Science-Articles/Archive/esnet-ipv6.html
7 http://www.nanog.org/meetings/nanog19/presentations/fink.ppt
8 http://www.commsdesign.com/showArticle.jhtml?articleID=52601556
9 http://www.cio.gov/Documents/IPv6_FAQs.pdf and http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf
10 http://www.antd.nist.gov/usgv6/profile.html

under the USG's $20B "Networx" program in March 2007.[11] Networx was one of the largest federal communication contracts in U.S. history, with an estimated $20 billion to be shared amongst the awardees over ten years.

Soon after the USG's civilian agencies met the June 2008 deadline to add IPv6 support to their backbone networks, planning was started to transition USG client devices, servers and software applications to IPv6 while maintaining IPv4 for continuity purposes.

In May 2009, the Federal CIO Council published a *"Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government"*.[12] The document directed USG CIOs, chief architects and other government IT leaders to:

- Develop IPv6 migration plans for their agencies by December 2009; and
- Execute their IPv6 transition plans between January 2010 and December 2011.

In December 2009, the U.S. Government issued a Federal Acquisition Regulation (FAR) which elevated NIST's IPv6 profile into a hard requirement for ICT procurements. As of July 2010, all USG information technology purchases will need to comply with NIST's USGv6 profiles.[13] Annex E of this report contains more information about IPv6 profiles.

Appendix A provides some insight into IPv6 migration planning and cost consideration, from the perspective one USG agency which has already completed its transition. Appendix B contains a list of useful USG reference documents on IPv6 including policies, standards, deployment planning guides and other reports. The information in many of those documents may be applicable to IPv6 deployment planning in Canada.

C.1.2. Current Status of IPv6 Readiness and Deployment in the U.S. Private Sector

Many U.S. private sector organizations are far ahead of their Canadian counterparts with respect to IPv6 today.

A number of top tier U.S service providers offer commercial IPv6 services to USG agencies and to private sector enterprises including:

- AT&T: http://www.corp.att.com/gov/solution/network_services/data_nw/ipv6/
- Comcast: http://www.comcast6.net/
- Google: http://www.google.com/intl/en/ipv6/
- Hurricane Electric:http://ipv6.he.net/
- Sprint-Nextel: http://newsreleases.sprint.com/
- Verizon: http://www.verizonbusiness.com/us/govt/overview/press_release/2007

Many US-based ICT vendors offer IPv6 capabilities in their products. The list of companies includes:

- Apple: http://www.apple.com/server/macosx/technology/networking.html

11 http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=16100

12 http://www.cio.gov/Documents/Planning_Guide-Roadmap_Toward_IPv6_Adoption_in_USG_May-2009.zip

13 http://edocket.access.gpo.gov/2009/E9-28931.htm

- HP: http://h10026.www1.hp.com/netipv6/Ipv6.htm
- IBM: http://www-01.ibm.com/software/info/ipv6/compliance.jsp
- Microsoft: http://technet.microsoft.com/en-us/network/bb530961.aspx
- Oracle: http://www.oracle.com/technology/products/oraclenet/pdf/oracledatabase_ipv6_sod.pdf
- Cisco: http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html
- Juniper: http://www.juniper.net/us/en/solutions/public-sector/federal-government/ipv6/

Several large U.S. content and network providers have announced IPv6 within the past year including:

- Limelight Networks: June 2009 announcement
- Netflix: July 2009 Status Report
- YouTube: February 2010 news report

C.2. European Union (EU)

The European Commission (EC), which is the executive function that operates the European Union, has invested more than €180 million to support more than forty IPv6 research projects on the continent to date.[14]

- In 2001, the EC funded a joint program between two major Internet projects—6NET and Euro6IX—to foster IPv6 deployment in Europe.[15] The EC committed €17 million over three years to enable interoperability testing, network interconnection, and the deployment of advanced services.
- In January 2004, the EC hosted a global IPv6 service event in Brussels. The conference celebrated the launch of world-wide native IPv6 connectivity into IPv6-enabled National Research and Education Networks (NRENs) including GÉANT, Euro6IX and 6Net in Europe, Abilene in the U.S., WIDE in Japan, and CA*net 4 in Canada.[16]
- In 2006, the EC funded a study of the expected impact of IPv6 on fifteen different market vertical sectors.[17] A comprehensive report was produced in 2007. It included recommendations that the government should play a coordinating role and partner with industry to catalyze IPv6 deployment.[18]
- In May 2008, the EC announced consensus on an "Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe". The IPv6 action plan is tightly integrated with the EC's "i2010 initiative". The goal is for 25% of EU users to be able to access to the IPv6 Internet and their most important content and service providers without noticing a major difference compared to IPv4, by the end of 2010.

14 http://usipv6.com/6sense/2004/jun/june.htm#palet
15 http://www.euro6ix.org/press/Joint_Press_Release_v12.pdf
16 http://www.global-ipv6.net/agenda.htm
17 http://www.zaltablog.com/2010/02/impact-of-ipv6-on-vertical-sectors/
18 http://www.g6.asso.fr/images/3/31/20080701-IPv6-TFF-Camp-Study-FClari.pdf

- In the past 18 months, several EU countries, including, Denmark, Germany, Ireland, and Luxembourg, have launched national action and/or deployment plans for IPv6 in support of the i2010 initiative. In contrast the UK government has decided to take a different approach, as described in section C.4.

C.3. China

"China is the only country that has more people than IPv4 addresses," said Jun Murai, a Japanese IPv6 expert, nicely summing up the quandary of this fast-developing country, largest in the world with 1.3 billion people.

In December 2003, the Chinese government issued licenses and allocated $170 million for the construction of the China Next Generation Internet (CNGI), with the goal of having that network fully operational by the end of 2005 in partnership with major providers.

- IPv6 was selected as a key technology for the CNGI because IPv4 could not satisfy China's addressing needs beyond the short term.

By October 2009, the CNGI connected more than 100 Chinese universities, 200 governmental and industrial sites, and 400,000 researchers using IPv6.[19] The network was comprised of six nationwide backbones and 39 GigaPOPs, reaching more than 20 major Chinese cities. Five of the backbone networks are commercially operated (viz. by China Telecom, China Unicom, China Netcom/CSTNET, China Mobile, and China Railcom). The sixth backbone network is an academic research network operated by CERNET. The CNGI also has exchange points in Beijing and Shanghai to interconnect the Chinese backbones and to enable international communications via links to APAN, GÉANT, and Internet2.[20]

China showcased IPv6 on the CNGI during the 2008 Olympics in Beijing via www.beijing2008.cn. A wide range of devices were networked using IPv6 including security cameras, Olympic events cameras and Taxis.

In December 2009, one of the CNGI backbone operators, China Telecom, announced their timetable for commercial IPv6 services as follows:

- 2009: IPv6 trial begins;
- 2012: IPv6 becomes available for large scale commercial use; and
- 2015: IPv4 is retired.

C.4. United Kingdom

In contrast to government policies in the United States, Asia, and the rest of Europe, the British government has decided to rely on a market led approach for IPv6. A presentation delivered in

19 http://www.cs.jhu.edu/~bkhabs/v4v6/xing-ivi-20081002.pdf, slide #3
20 http://en.wikipedia.org/wiki/China_Next_Generation_Internet

March 2009 by the British Government's Department for Business Enterprise & Regulatory Reform (BERR) asserted that: [21]

- The (British) government will not fund an IPv4 – IPv6 migration;
- Suitable products and services are (already) available from the market;
- Businesses should lead the adoption of IPv6; and
- Public sector uptake will proceed in tandem with UK industry/business.

In keeping with the above, the British Government published a "Digital Britain Report" on June 16th, 2009.[22] The report was positioned as a "strategic vision for ensuring that the UK is at the leading edge of the global digital economy", however it made no mention of IPv6. That prompted a call for government action on IPv6 from regional stakeholders.

In December 2009 a follow-up document called "Digital Britain - Implementation Update"was released. It too had no mention of IPv6.

C.5. Japan

Japan has been involved in the development of IPv6 since the 1990s via a variety of public and private initiatives. Japanese Prime Minister Yoshiro Mori made a statement about the importance of IPv6 research in a policy speech at the start of the 150th Session of the Diet in September 2000. He said:

> *"We shall aim to provide a telling international contribution to the development of the Internet through research and development of state-of-the-art Internet technologies and active participation in resolving global Internet issues in such areas as IP version 6 (IPv6)."*

In 1984, the Widely Integrated Distributed Environment (WIDE) project was launched as a research consortium among Japanese industry and academia.[23] In 1996, WIDE installed and operated Japan's first inter-city IPv6 connection. Shortly thereafter, researchers associated with WIDE contributed to:

- the creation of IPv6 protocol stacks for BSD UNIX, and for Linux;
- numerous proposals for IPv6 standardization; and
- IPv6 test and evaluation specifications and tools.

Today the WIDE project involves more than four hundred researchers from 140 private companies and universities on several networking and IPv6 topics.

21 http://www.ripe.net/ripe/meetings/ripe-58/content/presentations/berr-ipv6.pdf
22 http://www.culture.gov.uk/what_we_do/broadcasting/5631.aspx/
23 www.wide.ad.jp

Nippon Telephone and Telegraph (NTT) began operating an IP network in 1996 which has grown into one of the world's largest networks today.

- NTT launched commercial IPv6 services in 2003 spanning Asia, Europe, North America and Australia. The services included native IPv6 transport, tunneling (across their older IPv4 network and though other provider's IPv4 networks), and dual-stack gateway services.
- In March 2008, NTT announced an IPv6-based IPTV service called "Hikari TV" for Japanese subscribers. It provides standard and high definition TV programming over a dedicated IPv6 network, as well as 10,000 video-on-demand and 13,000 karaoke titles. NTT reported having "hundreds of thousands" of paying subscribers for this service within its first year (i.e. by January 2009). [24]

In 1999, Internet Initiative Japan (IIJ) launched Japan's first commercial IPv6 trial service for high-end Enterprise customers. IIJ operates one of Japan's largest domestic Internet backbones and provides networking between Japan and the U.S.

- In March 2009, IIJ announced the "IIJ (IPv6) Transition Support Solution" to help customers move to IPv6. The solution consists of consulting and training services.[25]

In 2001, an "IPv6 Promotion Council" was established by the Japanese government and industry stakeholders to coordinate IPv6 planning for the government's e-Japan initiatives, R&D programs, applications development, and product and services trials involving carriers and ISPs, CPE and infrastructure equipment vendors. This council remains active today.

In September 2008, a stakeholder group was concerned that IPv6 adoption in Japan was taking too long. That led to the creation of a new "Task Force on IPv4 Address Exhaustion in Japan" with members from the Japanese government, telcos, internet providers and researchers. [26]

- In October 2009, the Task Force published an "*Action Plan and Milestones Toward IPv4 Address Exhaustion*" to raise awareness of the current status and plans for IPv6 in content providers, applications providers, ISPs and consumer electronics suppliers. The Task Force recommended that full IPv6 services be deployed across all of Japan by April 2011. [27]
- Most Japanese ISPs including start ups and rural providers, and IX providers (viz. NSPIXP6 and JPIX) are now deploying IPv6.

The Japan Approvals Institute for Telecommunications Equipment (JATE)[28] hosts one of the six global facilities certified by the IPv6 Forum under their 'IPv6 Ready' logo testing program.[29] Most domestic Japanese router vendors (e.g. Hitachi, Fujitsu, NEC, Furukawa Electric, Yamaha) have been tested and are 'v6-ready'.

24 http://www.networkworld.com/news/2009/010809-ntt-ipv6-tv.html
25 http://www.iij.ad.jp/en/news/pressrelease/2009/0317.html
26 http://www.ipv6.or.kr/summit2009/data_pdf/3rd_keynote_4.pdf
27 http://www.kokatsu.jp/blog/ipv4/en/data/091005_v4exh_actionplan_en.pdf
28 http://www.jate.or.jp/english/index.html
29 http://www.ipv6ready.org/?page=faq#q4

C.6. Republic of Korea

In 2001, the Korean Ministry of Information and Communication announced their country would adopt IPv6. This was the start of publicly funded ICT research that would provide $150 million for the development of IPv6 routers, digital home services, applications, and other activities to the end of 2007.

Prior to the above, the government assisted in the creation of an IPv6 Forum in Korea. The Forum was launched in March 2000 and attracted 61 member organizations including industrial corporations, research institutes and universities. The mission of the Forum was to promote IPv6 in Korea, via activities such as dialogue on domestic IPv6 standards issues, hosting IPv6 conferences and summits, and developing policy advice for the government.[30]

In 2006, the Korean government shifted resources from research to implementation. They published a *"Plan for accelerating adoption of IPv6"* that required research networks to adopt IPv6 by 2008, and to provide IPv6 as a test bed network for communications equipment vendors and Internet service providers (ISPs). The plan also mandated that public sector networks and systems support both Internet Protocol version 4 (IPv4) and IPv6 by the end of 2010. Korean ISPs are expected to adopt IPv6 for their major transport network during 2010 and for their access networks by 2013. [31]

In July 2009, the National Internet Development Agency of Korea (NIDA) reported:[32]

- 61% of the hardware in domestic carrier backbone networks was dual stack IPv4/IPv6;
- 43% of the hardware in public sector networks was dual stack IPv4/IPv6;
- four of Korea's ten .kr DNS servers were fully serviced with IPv6;
- two IPv6 internet exchanges were operating (viz. 6NGIX and 6KANet); and
- one major ISP had enabled IPv6 on its backbone for a public sector customer.

Korea Telecom is working to transition Korean public sector e-Government services to IPv6 [33], in support of the Korean Government's IPv6 deployment plan produced by the National Internet Development Agency of Korea (NIDA).[34]

C.7. Australia

The Australian Ministry of Communications sponsored a national IPv6 summit in 2005, which subsequently became an on-going annual initiative. The most recent summit was held in December 2009.

In February 2005, the Australian Government mandated that their Department of Defence transition to IPv6 by 2013.[35]

---

30 http://www.ipv6-es.com/02/docs/yongjin_kim.pdf
31 http://www.idrc.ca/en/ev-140957-201-1-DO_TOPIC.html
32 http://www.ipv6.or.kr/summit2009/data_pdf/1st_AD2_2.pdf
33 http://www.apan.net/meetings/newzealand2008/presentations/ipv6/apan20080806ipv6-djkwak.pdf
34 http://www.apan.net/meetings/kualalumpur2009/proposals/IPv6/IPv6%20Status%20of%20Korea.pdf
35 http://www.ipv6.org.au/07ipv6summit/talks/Paul_Pappas_IPv6.pdf

In 2006, the Chief Information Officer Committee (CIOC) directed the Australian Government Information Management Office (AGIMO) to develop an IPv6 transition strategy. AGIMO, under the Department of Finance and Deregulation, published an initial strategy in October 2006, which was endorsed by the Australian CIOC. The strategy was widely disseminated during 2008, and reviewed with industry stakeholders.

In November 2008, an AGIMO presentation to the fourth annual Australian IPv6 Summit suggested the government planned to accelerate their IPv6 transition strategy. Whereas the original timeline called for IPv6 adoption between 2013 and 2015, the new target for IPv6 transition in Australia was set for the end of 2012.[36]

C.8. India

Only 22 entities (viz. ISP's and Research & Education networks) have obtained IPv6 address blocks from the Asia Pacific Network Information Center (APNIC). However only Ernet (India's R&E network, equivalent to CANARIE), Sify, HNS and Tata Communications have deployed and announced their IPv6 routes.

India still has a long way to go in its development including the telecommunications sector. In this sector, the size of the market and the anticipated continuation of very rapid growth, encouraged by an enlightened liberalization policy by the Federal Government, has attracted investments and participation by a number of foreign telecommunications companies including AT&T, BT, C&W, FT Orange, and Verizon. NTT Docomo of Japan bought a stake in TTSL, Tata's mobile telephony operator in India. The Indian software development departments of some major telecomm equipment manufacturers and software houses have participated actively in the development and testing of IPv6 features and functionalities creating a growing pool of local IPv6 expertise.

References

- http://www.trai.gov.in/Default.asp
- http://www.mit.gov.in/
- http://www.dot.gov.in/
- http://www.tec.gov.in/

36 http://www.ipv6.org.au/08ipv6summit/talks/Dale_IPv6Summit08.pdf

Annex D - Proposed Terms of Reference for a Canadian IPv6 Centre of Excellence

This Annex contains draft Terms of Reference (ToR) for a Canadian IPv6 Center of Excellence.

I. OFFICIAL NAME

The official name of the Centre of Excellence is to be determined; the *working name* used throughout this Annex is the "Canadian IPv6 Centre of Excellence (C6CoE)".

II. CONTEXT

Canada's largest trading partners have embraced the need for IPv6 within their digital economy strategies. Internet technologies provide a foundation for international trade and e-commerce, and the Internet is moving to IPv6.

The imminent exhaustion of IPv4 addresses makes it necessary to proactively transition to IPv6. IPv6 will alleviate concerns about internet address space run out, solve key scalability issues (e.g. auto-configuration of customer premises equipment), and improve network security and device mobility.

Despite a lot of early, pioneering work on IPv6 by Canadians (as described in section 4.2 of the IITG's Final Report to ISACC), very few Canadian ISPs, enterprise networks or other internet stakeholders had started their transition to IPv6 by March 2010. Canadian IPv6 expertise is held by a very few organizations and people in Canada today.

IPv4 addresses will run-out within the next 24 months.

There is a clear need to multiply the small base of IPv6 expertise that exists in Canada in 2010, in order to assist Canadian organizations to transition to IPv6 by 2011-2012.

III. MISSION and GOALS:

One of the highest priority tasks for the C6CoE is to start an urgent familiarization program for industry and governmental senior managers, educators, trainers, and technical advisors about the need to transition Canada's digital economy infrastructure to IPv6.

Members of the C6CoE should provide assistance and share their IPv6 expertise with Canadian ICT product development, network engineering, planning and operational staff. In addition, expert review and guidance on key IPv6 technical specifications (e.g. to be included in requests for tender for IPv6 services, hardware or software) may be offered.

If time and resources permit, the C6CoE may also establish subgroups to help articulate Canadian positions in specific application domains such the role of IPv6 in Smart Grids, sensor networks, wireless communications, green IT, and any other domain where C6CoE expertise could contribute to new ICT innovations.

IV. PRIMARY RESPONSIBILITIES:

- Develop and maintain a world class repository of knowledge and expertise to assist Canadian governments, enterprises, and other stakeholders to transition to IPv6;
- Raise awareness about the need for IPv6 in Canada; and
- Disseminate IPv6 knowledge and best practices.

V. DESIRED OUTCOMES:

- Attract, develop, and retain Canadian expertise on IPv6 from domestic sources and abroad;
- Improve Canada's position as a producer and consumer of advanced telecommunications equipment and services;
- Contribute to the sustainability of Canadian ICT research and innovation by engaging with researchers, knowledge workers, venture capitalists and entrepreneurs;
- Increment capital and strategic investment for the telecommunications sector; and
- Modernize Canada's internet infrastructure to secure Canada's position in relation to her trading partners.

VI. JURISDICTION:

- The scope of operations for the C6CoE should encompass all of Canada;
- The creation of new IPv6 standards is out of scope; the C6CoE is not intended to be a Standards Development Organization (SDO);
- Notwithstanding, C6CoE participation in standards development activities may be pursued (e.g. by authoring and submitting contributions to existing SDOs such as the IETF);
- IPv6 Profiles for Canada may be required; if the C6CoE becomes involved in the creation of original IPv6 profiles for Canada, it should do so in partnership with an existing Canadian SDO (i.e. BNQ, CGSB, CSA, ULC).

VII. TIMEFRAME:

- The C6CoE should be established as soon as possible (e.g. during 2010), and plan to operate for at least two years.
- The costs and benefits of the C6CoE to Canada should be reviewed annually, and serve as one input to the C6CoE's goals and priorities for the following 12-24 months.

VIII. RESOURCES:

An adequate budget and cadre of IPv6 experts will be required to launch the C6CoE in a meaningful and sustainable way.

IX. RELATIONSHIP WITH OTHER GROUPS:

- **ISACC**: Formation of the C6CoE was approved in principle at the November 5th 2009 Plenary meeting of the ICT Standards Advisory Council of Canada (ISACC). It is therefore recommended that the C6CoE liaise periodically with ISACC on topics of mutual concern or benefit.
- **Canadian Accredited SDOs**: The C6CoE is not intended to become an SDO. If the C6CoE wishes to become involved in the development of Canadian Standards (e.g. Profiles for IPv6 in Canada), it should partner with an existing Canadian SDO (i.e. BNQ, CGSB, CSA, ULC).

X. GOVERNANCE, POLICIES, BYLAWS:

Governance (e.g. policies and bylaws) for the C6CoE is to be determined.

XI. STRUCTURE:

Six structural options for constituting the C6CoE were examined by the ISACC IPv6 Task Group (IITG) during January and February 2010. A preferred structural model for the C6CoE was not identified.

They options examined were:

1. **New Not-For-Profit**
   This option calls for the incorporation of a new not-for-profit entity. The financial model would presumably be sponsorship from interested parties in government and industry. The entity would have dedicated staff. A champion (the President) with a strong desire to lead the C6CoE would be required to launch this option. The advantage is that the C6CoE would be largely independent. The disadvantage is that preparing a business case and starting the company from scratch may be more difficult and time-consuming than other options, and the new corporation might have to contend with established not-for-profit companies which have comparable capabilities. The overhead of incorporation may be an issue if the lifetime of the C6CoE is short (e.g. one or two years). All of the possible work program elements could be undertaken, although development of IPv6 profiles could only be in partnership with an SDO or Treasury Board, who publish Treasury Board Information Technology Standards http://www.tbs-sct.gc.ca/pol/index-eng.aspx?tree=standard.

2. **New For-Profit**
   This option calls for the incorporation of a new for-profit entity. The financial model would presumably be fee-for-service from customers in government and industry. The entity would have dedicated staff. A champion (the President) with a strong desire to run

the C6CoE would be required to launch this option. The advantage is that the C6CoE would be independent. The disadvantage is that preparing a business case and starting the company from scratch may be more difficult and time-consuming than other options, and the newly incorporated entity might have to contend with established not-for-profit companies which have comparable capabilities. The overhead of incorporation may be an issue if the lifetime of the C6CoE is short (e.g. one or two years). Most of the possible work program elements could be undertaken, although development of IPv6 profiles could only be in partnership with an SDO or Treasury Board. Representing Canada's views internationally is not generally within the scope of a for-profit company.

3. **Existing Not-For-Profit**
   This option calls for the C6CoE to reside as a division or office or program within an existing not-for-profit organization. Variants are that the existing not-for-profit organizations could be a university, an industry association, a research organization or a standards development organization. This option is similar to #1 above, except that expanding an existing organization to include the C6CoE work program would obviously be easier than starting from scratch. Contact should be made with at least CANARIE, ITAC and BCNET. Note that BCNET lists as its partners all the universities in BC. http://www.bc.net/

4. **Existing For-Profit**
   This option calls for the C6CoE to reside as a division or office or program within an existing for-profit organization. This option is similar to #2 above, except that expanding an existing organization to include the C6CoE work program would obviously be easier than starting from scratch. Obviously this option does not introduce a new competitor. It is possible, however, that more than one existing for-profit company may be interested in undertaking some of the work program and competing with each other. A disadvantage of this option is that some mechanism would be necessary to hand off the C6CoE to an interested company or companies in a fair and non-discriminatory manner. Representing Canada's views internationally is not generally within the scope of a for-profit company.

5. **Subtending from ISACC**
   Under this option, the C6CoE would be a volunteer Working Group of ISACC. The financial model would be sponsorship from interested parties in government and industry to offset expenses. The entity would not have dedicated staff. The advantage is that this model would be the easiest to launch. The disadvantage of a volunteer organization is that its capabilities would be limited. All of the possible work program elements could be undertaken, although development of IPv6 profiles could only be in partnership with an SDO or Treasury Board. Representing Canadian views internationally would be easier than in any of the previous models, because ISACC does that now.

6. Distributed

This option would split the work program of the C6CoE among multiple organizations. One obvious variant would be to separate the profile development and place it with either an accredited Canadian SDO or Treasury Board. The balance of the C6CoE could then follow any one of the five options already described. Another variant would be to split the international representation and place it with an organization that already has an international mandate. Another variant would be to distribute the work program among members of the ISACC IPv6 task group who have the requisite interest and knowledge, with a light-weight umbrella organization.

The first four options were judged by the IITG as being very similar with respect to enabling the execution of the work items proposed for the C6CoE (viz. section XII below). An important consideration for Options 1 to 4 is that a Champion will be required to develop the business case and to lead the C6CoE, either in a new corporate structure (the first two Options) or within an existing corporate structure (the second pair of Options):

1) Form a new not-for-profit company;
2) Form a new for-profit company;
3) Extend an existing not-for-profit company;
4) Extend an existing for-profit company.

The other two options were judged to be less well-suited for a C6CoE:

5) Form an unincorporated volunteer committee sub-tending from ISACC;
6) Distribute the work items across multiple organizations.

Option #5 would suffer from a total reliance on volunteers and an inability to handle financial transactions (e.g. obtain funding, solicit dues from members, sell services 'for hire'). Option #6 could become defocused – a Centre of Excellence without a center.

XII. PRIORITY TASKS and WORK ITEMS:

The IITG identified a list of tasks and work items for the C6CoE and then prioritized the list. The prioritized list is:

1. <u>Highest Priority Tasks for the C6CoE in 2010-2011</u>:
   - Survey and report on, or facilitate doing a survey and report on, the IPv6 readiness of various sectors in Canada;
   - Actively assist in the creation of industry/government working groups:
     - help in, or catalyze, the creation of IPv6 deployment working groups in government and in industry
     - nominate experts (knowledge leadership) to contribute to the work of working groups in various government branches, verticals industry segments, and/or in industry associations (e.g. send an IPv6 expert into the

first meeting of a fledgling working group, and offer to facilitate subsequent meetings).

2. High Priority Tasks for the C6CoE in 2010-2011:
   - Actively promote IPv6 awareness in industry:
     - create a uniform slide deck to be used by the C6CoE speakers;
     - develop a list of certified speakers who would be available to speak at various industry conferences; “certified” in this context means "pre-screened and approved";
     - Seek speaking opportunities at various industry conferences on topics including Information Technology, safety, electrical industry, banking, etc.
   - Actively promote IPv6 awareness in all level of governments:
     - create a uniform (for government) slide deck to be used by C6CoE speakers;
     - have a list of “certified" speakers who would be available to speak to various government levels (federal, provincial, municipal, agencies);
     - seek speaking opportunities at various government ICT conferences including Information Technology, safety, electrical industry, banking etc.

3. Medium Priority Tasks for the C6CoE in 2010-2011:
   - Liaise with Academia:
     - actively facilitate engagement and commitment to IPv6 by Canadian academics;
     - identify challenging IPv6 research topics for grad students;
   - Training and Seminars: develop (or facilitate development of) Canadian expertise and talent on IPv6;
   - Select and make available a cadre of experts able to assist government and industry in the specification of IPv6 requirements and evaluation of compliance of response;
   - Create a web site and communications tools to provide linkages to new and/or existing information about IPv6, and to enable discussion and communications with the C6CoE;
   - Facilitate access for the Canadian industry to an IPv6 interoperability and compliance testing environment;
   - Facilitate exchange of information about IPv6 deployment, best practises, market conditions, products and applications with IPv6 interest groups in other countries (e.g. create and populate C6CoE website with good content).

4. Medium to Low Priority Tasks for the C6CoE in 2010-2011:
   - International Representation:
     - Speak (and listen to gather intelligence) at various international events, including meetings of ISOC or Internet Registries;
     - Develop and communicate Canadian positions for international consumption via existing Canadian national coordination processes;
     - Liaise with selected international organisations.

5. Low Priority Tasks for the C6CoE in 2010-2011:
   - Assist people who want help on their IPv6 needs, on a for-hire basis (e.g. to write a specific profile);
   - Determine what, if any, IPv6 profiles are required in Canada (e.g. say "the NIST profile is good for Canada", or "Canada should just use IPv6 Forum "v6-ready" products):
     - If there is a need for a Canadian IPv6 profile, then facilitate the creation of one or more IPv6 profiles for Canada as required.

Annex E - Standard IPv6 Profiles

The information contained in this Annex was compiled during the twelfth working meeting of the IITG, held January 19, 2010. Most of the text herein is copied from the approved Minutes of that meeting.

More information on IPv6 Profiles is also available on-line at:
http://www.antd.nist.gov/usgv6/usgv6-v1-faq.htm and
http://csrc.ncsl.nist.gov/cyber-md-summit/documents/posters/iip-ipv6-poster.pdf

---

IITG-12 Discussion: IPv6 Profiles and Certification Testing

Marc Blanchet and Mario Boisvert thanked Tony Hain and Stephen Orr for agreeing to talk to the IITG about industry standards profiles for IPv6, and their experiences from IPv6 interoperability and conformance testing.

Tony Hain is a technical leader for IPv6 at Cisco, an IPv6 Forum Fellow, and a former co-Chair of the IETF's (now concluded) ngtrans working group. Both he and Stephen Orr (also from Cisco) were in Ottawa during the week of January 18th 2010, and made time to speak to the IITG. They summarized the current status of IPv6 profiles and certification testing in the United States and other countries as follows:

IPv6 Forum Profiles:
The IPv6 Forum is the home of the "IPv6 Ready Logo Program" (http://www.ipv6ready.org/), a conformance and interoperability testing program intended to increase user confidence by demonstrating that IPv6 is available now and ready to be used. An "IPv6 Ready Logo Committee" defines test specifications for IPv6 conformance and interoperability testing, and provides access to self-test tools which can be used to:

- Verify protocol implementation and validate interoperability of IPv6 products, and
- Prepare for IPv6 Ready Logo testing in laboratories across the globe.

Most of the focus on the IPv6 Ready Logo Program is outside of the United States today.

U.S. Government and DoD Profiles for IPv6:
IPv6 profiles have not been a hot topic in U.S. to date, except in the U.S. Government:

- The U.S. Department of Defense (DoD) has developed a technical and standards based definition of interoperability requirements for IPv6-capable products designed for use in DoD networks (viz. the "DoD IPv6 Profiles"); and
- NIST maintains similar but not identical IPv6 profiles for equipment to be deployed in civilian agency networks.

Version 4.0 of the "IPv6 Standard Profiles for IPv6 Capable Products" (for use in DoD networks) was published in July 2009, as part of an update to the Defense Information Technology Standards

Registry (DISR) Baseline Release, Version 09-2.0. The new IPv6 Profiles updated and replaced the DoD Version 3.0 Profiles from 2008, which were themselves updates to earlier profiles. The first DoD IPv6 Profiles were published in 2006.[37]

[Note: Wikipedia has more information about U.S. DoD IPv6 profiles at http://en.wikipedia.org/wiki/DoD_IPv6_Product_Certification. The italicized text below is excerpted from Wikipedia.]

> The DoD IPv6 Standards Profiles for IPv6 Capable Products (DoD IPv6 Profile) *is the singular "IPv6 Capable" definition in DoD. It is a document that lists the six agreed upon product classes (Host, Router, Layer 3 Switch, Network Appliance, Security Device, and Advanced Server) and their corresponding standards (RFCs). It lists each standard according to its level of requirement:*
>
> - *MUST: The standard is required to be implemented in the product now.*
> - *SHOULD: The standard is optional, but recommended for implementation.*
> - *SHOULD+: The standard is optional now, but will be required within a short period of time.*

The National Institute of Standards and Technology (NIST) published "A Profile for IPv6 in the U.S. Government – Version 1.0" in 2008, after more than two years of work and industry consultation. The document specifies a standards profile to support government agencies as they implement IPv6. The profile recommends technical standards for common network devices, such as hosts, routers, firewalls and intrusion detection systems. It also outlines the compliance and testing programs that NIST will establish to ensure that IPv6-enabled federal information systems work securely with existing IPv4 systems.

NIST also posted a document called "USGv6 Version 1 Frequently Asked Questions" about the scope and purpose of the NIST IPv6 profile, and how it relates to other profile and test efforts, including those of the DoD and the IPv6 Forum.

NIST's profiles are largely based on the IPv6 Forum's IPv6 Ready Logo Program. This means that any product that carries the "IPv6-ready" logo should have a good chance of satisfying NIST profile requirements; NIST recommends many of the same tests and testing suites that are used for "IPv6 ready" testing, however NIST does not accept an IPv6-ready logo as proof of compliance. Instead, NIST insists that vendors must re-certify the compliance of their products (i.e. against the NIST profile) at a NIST accredited testing facility.

Product testing against U.S. DoD IPv6 Profiles has evolved beyond verifying compliance against profiles. IPv6 has been integrated IPv6 into the DoD's system level architecture.

The following explanatory note is (again) taken from Wikipedia:

37 See http://fcw.com/Articles/2009/08/24/WEB-DOD-releases-IPv6-profile.aspx?p=1 for more information.

> *The Department of Defense (DoD) Internet Protocol version 6 (IPv6) product certification program … mandates the Joint Interoperability Test Command (JITC) in Fort Huachuca, AZ, to test and certify IT products for IPv6 capability according to the Request For Comments (RFCs) outlined in the DoD's IPv6 Standards Profiles for IPv6 Capable Products. Once products are certified for special interoperability, they are added to the DoD's Unified Capabilities Approved Products List (UC APL) for IPv6. This list is used by procurement offices in the DoD and the U.S. Federal agencies for ongoing purchases and acquisitions of IT equipment.*

Unfortunately there is no transitive trust between the DoD and NIST. The DoD goal is to have equipment that is "IPv6 operational" (in DoD applications) whereas the focus of NIST is to get equipment certified as IPv6-ready.

NIST has standardized just three categories of equipment in their IPv6 profile (viz. Hosts, Routers, and Network Protection Devices) whereas the DoD Profiles cover six categories. Interestingly the IPv6-ready logo program (which NIST used to create their profiles) has more than three equipment categories.

The problem with having not enough equipment categories in IPv6 profiles is that many networks are complex. For example, consider evolving an Enterprise Network to Unified Communications (UC). Existing voice and data networks, e-mail, IVR and/or instant messaging systems may need to be integrated to create a UC network solution. Dozens of different product types may be involved. How can vendors certify UC products as "IPv6 capable" if the NIST profiles only specify tests for three different types of products?

Q: How must effort did NIST invest to develop their IPv6 profile?

A: It wasn't trivial. NIST has had five people working on their IPv6 profile for more than a year, and some of their review meetings (with stakeholders) involved more than 30 people.

Q: Can you comment on the role of the University of New Hampshire (UNH)?

A: Equipment can be tested for compliance with the IPv6 Forum's IPv6-ready specifications in Japan or at the UNH. UNH is not (as of yet) certified for testing against the NIST profile. Verizon has the only lab that is certified for NIST testing to date.

Q: Are the tests straightforward?

A: Testing may involve 3 to 4 weeks per device, per software load. Labs are heavily backlogged already, and they do not include testing against FIPS or Common Criteria.

Q: What about NATO? Will there be a NATO Profile for IPv6? If yes, will it be different from NIST and U.S. DoD profiles?

A: Good questions. The support for IPSec and IKEv2 are the two main places where NIST and DoD profiles diverge today. NIST has mandated that, as of July 2010,

both IPSec and IKEv2 must be supported, whereas the DoD profiles do not require them.

Q: Is there one IPv6 Profile, that is a superset of the others?

A: No. The key thing to understand is the operational context drives requirements, and the requirements, in turn, drive the content of IPv6 profiles.

Q: What are U.S. Carriers doing about IPv6 profiles?

A: Large Carriers typically do not publish profiles. They usually procure equipment against their own requirements, and they usually bring equipment into their own labs to testing against their needs.

Q: What Enterprise customers and IPv6 profiles?

A: Enterprises have yet to look “IPv6-ready” products, and then ask themselves if that level of capability is sufficient for their needs.

Q: Would it be useful to list the approved labs for IPv6 testing, across the U.S., Europe and Japan?

A: Knowing about labs is useful. Having more labs could be better. It might be useful to have a Canadian University take on IPv6 testing, to offload UNH when they are backlogged.

Appendix A - Sample IPv6 Migration Plan

The contents of this Appendix are based on the experiences of the U.S. Department of Veterans Affairs during their transition to IPv6, from 2006 to 2009.[38]

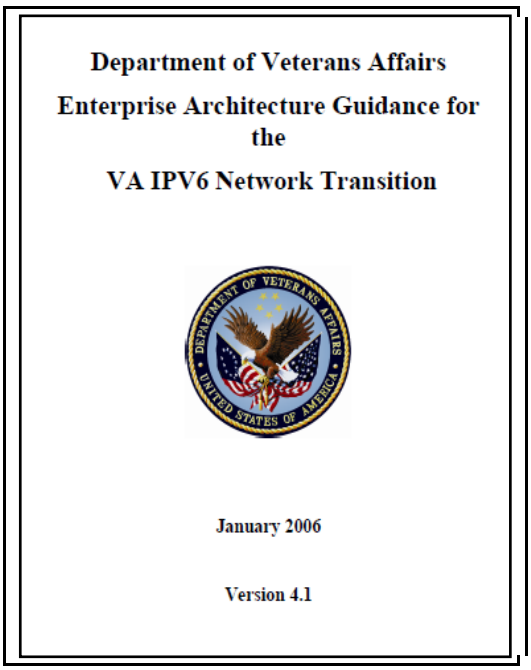
The first steps in the VA's transition to IPv6 were as follows:

1. An official leader for their IPv6 transition project was assigned to:
    - conduct an inventory of routers, switches and hardware firewalls for IPv6 compatibility;
    - conduct an inventory of all other network IP devices for IPv6 compatibility;
    - analyze fiscal and operational impacts and risks.
2. The IT organization produced, completed and reported on the following:
    - a requirements analysis to determine the target scope of IPv6 deployment into the existing network infrastructure, and to identify challenges with maintaining communications with older IPv4 devices;
    - a sequencing plan for implementing IPv6 across the organization;
    - the development of training material for stakeholders;
    - the development and implementation of a test plan for IPv6 compatibility and interoperability;
    - the deployment of IPv6 using a phased approach;
    - maintenance and monitory of networks; and
    - updates to IPv6 requirements and the target architecture on an ongoing basis.

After completing the transition, the VA summarized the major cost elements as follows:

> **VA-wide Network Planning and Design:** Costs associated with project planning and network design for IPv6 Implementation.
>
> **Networking Engineering:** Costs incurred to augment networks specifically to support IPv6.
>
> **Nodes and Peripherals:** Costs for workstations, printers, and data storage devices etc. that are currently IPv4 capable and would eventually become IPv6 capable as well as the cost of other devices that do not current require an IP address, but may in the future.
>
> **Infrastructure Development:** Those costs derived from modifications to the infrastructure based upon the configuration needs associated with the IPv6 protocol suite, versus the IPv4 protocol suite.

38 http://www.ea.oit.va.gov/apps/eas/4_3/extDocs/ea/IPv6/EA%20Guidance%20for%20Transition.pdf



Application Development: Costs associated with modifying existing applications to work with the IPv6 stack, as well as the costs to develop new applications that would be impacted by the IP stack and require IPv6 specific coding.

Network Operations (O&M): Additional costs, above standard O&M, necessary to implement, manage, and maintain a dual stack IP network, or a future-centric network running the single IPv6 protocol.

Training: Costs associated with training network engineers, technicians, developers, and managers to support a dual stack network, or a future-centric network running the single IPv6 protocol as well as the cost of communicating the impact and value of the program to users, clients and other stakeholders.

Appendix B - Useful U.S. Government IPv6 Documents

DoD IPv6 Standards Profiles for IPv6 Capable Products - Version 4.0
Date Effective: July, 2009 Adobe Acrobat Reader is required to view file

This document provides the engineering-level definition of “IPv6 Capable” products necessary for interoperable use throughout the U.S. Department of Defense (DoD). The term “IPv6 Capable Product” as used in this document, means any product that meets the minimum set of mandated requirements, appropriate to its Product Class, necessary for it to interoperate with other IPv6 products employed in DoD IPv6 networks.....

Planning Guide / Roadmap Toward IPv6 Adoption in the U.S. Government
Date Effective: May 20, 2009 ZIP is required to view file

On behalf of the Federal CIO Council, OMB is pleased to announce the release of the "Planning Guide/Roadmap toward **IPv6** Adoption within the US Government". This document defines the Federal Government's Internet Protocol version (**IPv6**) direction, building upon requirements set forth in OMB Memorandum ...

Federal CIO Council Transition Guide
Date Effective: January 12, 2009 Adobe Acrobat Reader is required to view file

The Federal Chief Information Officers Council Transition Guide is provided for newly designated Agency heads and other senior leaders during this time of transition to both understand the role of the Federal CIO Council and to begin the conversation of identifying additional opportunities to share ...

Architecting Next-generation Internet Technologies
Date Effective: October 22, 2008 MS PowerPoint is required to view file

This presentation made was at the 2008 Federal IT Summit by Peter Tseronis, Chair, Federal **IPv6** Working Group. It was presented on October 22, 2008, at the Department of Commerce to more than 500 federal IT workers. The event was co-sponsored by the Office of Management and Budget's Office of E-Government ...

A Profile for IPv6 in the U.S. Government - Version 1.0
Date Effective: July, 2008 Adobe Acrobat Reader is required to view file

This document contains recommendations by the *National Institute of Standards and Technology* with respect to a technology acquisition profile for common IPv6 devices to be procured and deployed in operational (civilian) U.S. Government IT systems. This profile has been prepared for use by Federal agencies. It can be used by other organizations on a voluntary basis and is not subject to copyright ....

IPv6 Demonstration Plan
Date Effective: January 30, 2008 Adobe Acrobat Reader is required to view file

The purpose of this document is to provide guidance and describe procedures for Agencies to demonstrate **IPv6** compliance - to show that **IPv6** traffic has been successfully transported (i.e., received, processed, forwarded) through all **IPv6** devices in an Agency's operational core backbone network. The ...

Requirements for Enterprise Architecture and IPv6 Progress Reports
Date Effective: November 21, 2007 Adobe Acrobat Reader is required to view file

Since June 1, 2006, scorecard agencies have been required to submit Quarterly EA/**IPv6** Progress Reports to OMB. This quarterly reporting process is part of OMB's responsibility to oversee the development of agencies' enterprise architectures as part of the E-Government initiative on the President's Management ...

IPv6: The Next Generation Internet
Date Effective: January 17, 2007 MS PowerPoint is required to view file

This presentation called "**IPv6**: The Next Generation Internet" was delivered by Peter Tseronis from the Department of Education. He is a co-chair of the Federal **IPv6** Working Group. This is one of three presentations made during a Quarterly IT Forum co-hosted by the IT Workforce Committee of the CIO Council ...

U.S. General Accountability Office Report on IPv6
Date Effective: June, 2006 Adobe Acrobat Reader is required to view file

Federal agencies have taken steps in planning for the transition to IPv6, but several have not completed key activities. Much remains to be accomplished. Specifically, as of February, only 9 of the 23 agencies that reported having begun an impact analysis had developed preliminary costs for the transition as required as part of this analysis. These costs ranged from $960,000 to more than $20 million ...

IPv6 Transition Guidance
Date Effective: May 03, 2006 MS Word is required to view file

The Office of Management and Budget (OMB) has directed agencies to implement Internet Protocol version 6 (**IPv6**) within their infrastructure by June 2008. **IPv6** is an enterprise transformation driven by business, environmental, and technology factors, the scope and impact of which extend well beyond ...

IPv6 Frequently Asked Questions
Date Effective: February 15, 2006 Adobe Acrobat Reader is required to view file

In August of 2005, the Office of Management Budget issued Memorandum 05-22, establishing the goal of transitioning all Federal government agency network backbones to the next generation of the Internet Protocol Version 6 (**IPv6**), by June 30, 2008. OMB Memorandum 05-22 identifies several key milestones ...

Integrating IPv6 into Agency EA Planning
Date Effective: December 22, 2005 MS Word is required to view file

Abstract: In an effort to facilitate the transition to **IPv6**, the Architecture and Infrastructure Committee (AIC) and the Federal Enterprise Architecture Program Management Office (FEAPMO) have developed guidance titled **IPv6** Guidance: Implementing **IPv6** into Agency EA Planning to assist agencies in their ...

Transition Planning for Internet Protocol Version 6 (IPv6)
Date Effective: August 02, 2005 Adobe Acrobat Reader is required to view file

June 2008 is set as the date by which all agencies' infrastructure (network backbones) must be using **IPv6** and agency networks must interface with this infrastructure. This memorandum and its attachments provide guidance to the agencies to ensure an orderly and secure transition from Internet Protocol ...

Appendix C - IPv6 Allocations to Canadian Organizations

The following table lists the owners that have received IPv6 routable address space directly from ARIN. Most of these entities listed in this Appendix are Internet Service Providers which may further allocate address space to their customers and/or other organizations.

Note that downstream organizations are not included in this listing. Therefore this list does not identify **all** Canadian organisations that have IPv6 address space (e.g. DND).

This list was generated from a snapshot of the ARIN database taken on March 8, 2010. [39]

1	ACTIVO INC
2	ADVANCED KNOWLEDGE NETWORKS
3	Afilias Canada, Corp.
4	Allstream Corp.
5	Bcnet
6	Beanfield Technologies Inc.
7	Bell Aliant Regional Communications, Inc.
8	Bell Canada
9	Blink Communications
10	Cable VDN Inc.
11	CANARIE Inc
12	ccROUTE Inc.
13	CIRA Canadian Internet Registration Authority Autorit Canadienne pour les enregistrements Internet
14	Clear View Communications Canada Corp.
15	COGECO Cable Canada Inc.
16	Cogeco Cable Inc.
17	Connect One
18	Corporation of the City of Windsor
19	Dalhousie University
20	DATA CENTERS CANADA INC.
21	EAGLE.CA
22	EastLink

39 Only routable (/48 or less) prefixes are shown.

23	E-Gate Communications Inc.
24	E. I. Catalyst
25	Epik Networks, Inc.
26	Fibrenoire Internet Inc.
27	Fidalia Networks Inc.
28	Fusepoint Managed Services
29	Futureway Communications Inc.
30	GloboTech Communications
31	GONET
32	Gossamer Threads Inc.
33	Gouvernement du Quebec (Government of Quebec)
34	Greater Sudbury Telecommunications Inc.
35	Hexago
36	HL HOSTING LOGISTIC INC
37	Huron Telecommunications Cooperative Limited
38	Internet Light and Power Inc.
39	isoHunt Web Technologies, Inc.
40	iWeb Technologies Inc.
41	Legislative Assembly of Ontario
42	Le Groupe Videotron Ltee
43	Lexicom Ltd.
44	Magma Communications Ltd.
45	McGill University
46	Mega Quebec
47	Memorial University, NF CAnet 2 gigaPOP
48	MERLIN
49	Mountain Cablevision LTD.
50	MRNet
51	MTO Telecom Inc.
52	National Research Council of Canada
53	Network Connection
54	Neutral Data Centers Corp.
55	New Brunswick Department of Education

56	Nexicom Inc.
57	Nortel Networks, Inc
58	Nucleus Information Service, Inc.
59	Openface Inc.
60	ORANO
61	PERSONA COMMUNICATIONS INC.
62	Priority Colo
63	Public Works and Government Services Canada
64	PwC Management Services LP
65	Q9 Networks Inc.
66	Radiant Communications Canada Ltd.
67	Radiant Communications Ltd.
68	Research In Motion Limited
69	Reseau d'Informations Scientifiques du Quebec (RISQ Inc.)
70	RipNET Limited
71	River East Transcona School Division
72	Rogers Cable Communications Inc.
73	Rogers Wireless Inc.
74	Saskatchewan Telecommunications
75	Scratch Telecom
76	Seaside Communications, Inc.
77	Sentex Communications Corporation
78	Shaw Communications Inc.
79	Shaw Telecom G.P.
80	Skyway West
81	SPD NETWORK
82	Storm Internet Services
83	Tata Communications
84	TekSavvy Solutions, Inc.
85	Teleglobe Inc.
86	TELUS Communications Inc.
87	TELUS MOBILITY
88	Tera-byte Dot Com Inc.

89	TeraGo Networks Inc.
90	ThinkTel Communications Ltd.
91	Trail Networks, Inc.
92	Tucows.com Co.
93	Universite Laval
94	University of Manitoba
95	University of New Brunswick
96	University of Prince Edward Island
97	ViaGenie Inc.
98	VIF Internet
99	Westman Communications Group