IGF2015

Best Practice Forum
on

Creating an Enabling Environment for IPv6 Adoption

Version 3
31 October 2015

Draft for discussion at the IGF2015

João Pessoa, Brazil

Comment at http://review.intgovforum.org/?p=3987
1. Introduction and Background

1.1. About the Best Practice Forum on Creating an Enabling Environment for IPv6 Adoption

1.1.1. What we mean by “practices”
1.1.2. Methodology
1.1.3. Contributors

1.2. About IPv6 adoption

1.2.1. Internet Protocol addresses
1.2.2. IPv4 exhaustion
1.2.3. Network Address Translation
1.2.4. IPv6 development
1.2.5. IPv6 and IPv4 compatibility
1.2.6. IP address management

1.3. Why is it better to adopt IPv6 now?

1.3.1. IPv4 is running out
1.3.2. “Stopgap” measures are inadequate

1.3.2.1. Problems with the IPv4 “market”
1.3.2.2. The downsides of NAT and CGN

1.3.3. The benefits to IPv6 adoption (per stakeholder)

1.3.3.1. For content providers and publishers
1.3.3.2. For network operators
1.3.3.3. For end users
1.3.3.4. For mobile carriers and their customers

1.4. Hurdles to IPv6 adoption

1.4.1. Managing network configuration
1.4.2. Wholesalers providing IPv4-only bitstream services to retailers
1.4.3. Hardware and software compliance
1.4.4. Slow adoption by content and application providers
1.4.5. Training people and expanding capacity building

2. IPv6 Task Forces: A platform for best practices

2.1. Different Task Force models

2.1.1. Geographic scope
2.1.2. Organizational type
2.1.3. Membership composition and participation

2.2. Task Force activities
   2.2.1. Creating a space for collaboration
   2.2.2. Raising awareness
   2.2.3. Providing advice to businesses
   2.2.4. Making policy recommendations to governments

2.3. Common challenges identified by Task Force leaders

3. Capacity building
   3.1. Providers of IPv6 capacity building programmes
   3.2. Capacity building for non-technical stakeholders

4. Lessons from the private sector
   4.1. Review existing infrastructure
   4.2. Determine whether vendors are IPv6-ready
   4.3. Provide employees with training and knowledge
   4.4. Deploy IPv6 for public-facing services
   4.5. Migrate to IPv6 on internal networks
   4.6. Set internal deadlines
   4.7. Reach out to customers
   4.8. Consider different approaches to pricing (for ISPs)
   4.9. A case study: Japan
      4.9.1. IPv6 deployment plan
      4.9.2. Starting point of IPv6 deployment
      4.9.3. Confirming IPv6 readiness of network equipment vendors
      4.9.4. Staff skill-up with IPv6
      4.9.5. Setting internal deadlines toward the IPv6 deployment plan
      4.9.6. Preparing for unexpected events

5. Research and Education Networks, and Universities

6. Government initiatives
   6.1. Procurement policies
      6.1.1. Germany - Developing “IPv6 Profiles”
      6.1.2. United States - Requiring vendors to themselves use IPv6
   6.2. Deployment strategies
      6.2.1. The Kingdom of Saudi Arabia
      6.2.2. Finland
      6.2.3. India
      6.2.4. Japan - IPv6 Study Group - A platform to identify issues and actions for industry players
   6.3. Providing guidance
   6.4. Collaboration with Industry and other stakeholders

7. The role of the end user / consumer in IPv6 adoption
   7.1. The developing market for the Internet of Things
   7.2. Consumer awareness
   7.3. Certification
1. Introduction and Background

1.1. About the Best Practice Forum on Creating an Enabling Environment for IPv6 Adoption

The Internet Governance Forum (IGF) at the United Nations is an open, global forum where different participants from various stakeholder groups – governments, the technical community, civil society, academia, and the private sector – discuss Internet Governance and policy issues, on equal footing. The Best Practice Forums (BPFs) at the IGF seek to collect, discuss, and share different “best practices” used around the world for Internet Governance and policy issues. The BPFs help us to learn from each other by sharing our experiences – our successes as well as not so successful efforts.

The 2015 BPFs focus on six different areas: 1) regulating spam; 2) establishing and supporting Computer Security Incident Response Teams (CSIRTs); 3) establishing and supporting Internet Exchange Points (IXPs); 4) developing multistakeholder participation mechanisms; 5) Countering the abuse of women online; and 6) creating an environment that encourages the widespread adoption of Internet Protocol version 6 (IPv6) by those currently using Internet Protocol version 4 (IPv4). These actors include, for example, wired and mobile access ISPs, content owners, CDN operators, web hosting providers, residential gateway makers, VPN service providers, and corporate IT networks.¹

1.1.1. What we mean by “practices”

By “practices,” we mean the actions that different people and organizations take to create an enabling environment for IPv6 adoption in their locality, region, industry, or network. Practices can come in the form of case studies, examples, or anecdotes supported by evidence, and they describe the activities, policies, or other measures taken by stakeholders to encourage IPv6 adoption.

¹ Contribution on IGF review platform, Ross Chandler.
1.1.2. Methodology

The 2015 BPF on *Creating an Enabling Environment for IPv6 Adoption* (BPF on IPv6 Adoption) [was] an open discussion, with an open participation policy. This **outcome document** (document) is the result of an iterative discussion process conducted on the BPF’s open mailing list, over several calls, during an in-person session at the IGF2015, and by incorporating comments provided by the community at large on the IGF public review platform. We hope this document will assist others in their own efforts to support IPv6 adoption in their locality, region, industry, or network.\(^2\)

Best practice examples were collected by means of a public survey that launched mid-July 2015 and closed mid-November 2015. Organisers also collected content through email correspondence and mailing list discussion. The compilation of survey submissions is available in the Appendices Section at the end of this document.

1.1.3. Contributors

This document is the result of a combined effort involving many people. It would not exist without the volunteerism and expertise of a handful of core contributors. In lieu of adding citations to every contribution from the individuals below, we wish to thank and acknowledge them as a group:

*Alejandro Acosta, Olivier Crepin-Leblond, Glenn Deen, Miwa Fujii, Aaron Hughes, Marco Hogewoning, Hascall “Chip” Sharp, Sander Steffan, Nathalie Trenaman and Paul Wilson.*

We wish to thank all survey respondents and contributors, whose submissions are referenced throughout the text, for their involvement.\(^3\) We have made every effort to accommodate all submissions based upon their relevance to the text, as it developed.

The BPF on *Creating an Enabling Environment for IPv6 Adoption* was coordinated by IGF Multistakeholder Advisory Group (MAG) members Izumi Okutani and Susan Chalmers, and supported by the work of Wim Degezelle. Special thanks to Michael Oghia for his editing assistance.

---

2 The BPF mailing list [was] open to all who wish to participate. The list archives are publicly available here: http://mail.intgovforum.org/mailman/listinfo/bp_ipv6_intgovforum.org.

3 We have made every effort to accommodate all submissions based upon their relevance to the text.
1.2. About IPv6 adoption

1.2.1. Internet Protocol addresses
Devices connect to the Internet through Internet Protocol addresses (IP addresses). An IP address is a unique numerical address used to identify devices on the Internet (e.g., 69.65.11.25). Currently, almost all devices use the Internet Protocol version 4 (IPv4) address system to connect to the Internet, which was developed in the mid-1970s. The IPv4 address system has approximately 4 billion possible address combinations, defined by its address length of 32 binary digits, or bits.

1.2.2. IPv4 exhaustion
Since the 1970s, the Internet has undergone a rapid degree of growth and expansion that those involved in creating the early IP address systems could not have foreseen. As the number of online devices continues to grow, the available pool of IPv4 addresses, naturally, shrinks. A recent forecast by Cisco projects that by 2019, “the number of devices connected to IP networks will be three times as high as the global population.” This is almost six times the number of available IPv4 addresses. Simply put, we need more IP addresses to accommodate the growing number of Internet connections.

1.2.3. Network Address Translation
Network Address Translation (NAT) is a technique that was developed to save IPv4 address space. NAT also simplifies address management for consumer Internet connections by allowing multiple devices inside of a network to share one or more exterior, public IP address(es). For example, an ISP assigns an IPv4 address to a residential customer and then, via the NAT function, that single IPv4 address is used by a number of different computers and devices in the customer's home, which each use internal or “private” IP addresses.

A NAT can be thought of as an old-style PABX (Private Automatic Branch Exchange), which has one public phone number but internal office phones that use private extension numbers.

---

4 This definition is simplified for the purposes of this paper. As one contributor said, “Technically, an IP address identifies an interface on a device, not the device itself.”
5 To see statistics on what remains of the IPv4 address pools, see the personal site of computer scientist Geoff Huston, available at: http://www.potaroo.net/tools/ipv4/.
7 Note that there are public IP addresses and private IP addresses. “A public IP address is an IP address that can be accessed over the Internet. Like a postal address used to deliver mail to your home, a public IP address is the globally unique IP address assigned to a computing device. Your public IP address can be found at http://whatismyipaddress.com. Private IP addresses, on the other hand, are assigned to computers within a private space, without letting them directly connect to the Internet. See IPlocation.net, available at: https://www.iplocation.net/public-vs-private-ip-address.
Like a PABX, a NAT prevents full connectivity between internal devices and the public Internet. In the case of Internet connectivity, this introduces additional complexity for Internet applications. While this particular disadvantage is localized to NAT users and applications designers, the total aggregate cost of NAT on the Internet is very large.8

1.2.4. IPv6 development
IPv4 exhaustion may be a novel issue for the general public, but it has been a concern of the Internet engineering community since the 1990s. By the end of 1995, the community had already specified a new version of the Internet protocol – IPv6. IPv6 specifications were published by the Internet Engineering Task Force (IETF) in a document called Request for Comments 1752 (RFC 1752).

Similar to how we create more phone numbers by adding digits to them, the engineers who developed IPv6 made the addresses longer (128 bits as opposed to 32-bit IPv4 addresses).9 IPv6 theoretically increases the number of unique IP addresses to $2^{128}$ which means 340,282,366,920,938,463,463,374,607,431,768,211,456 unique combinations.10 The practical size of IPv6 address space could be equated roughly to 32 billion times that of the current IPv4 Internet.

1.2.5. IPv6 and IPv4 compatibility
IPv4 and IPv6 are two different protocols. IPv6 is not backward compatible with IPv4 because of the additional complexity that this would have entailed. Devices that communicate using only IPv6 cannot communicate with devices that communicate using only IPv4. Only when all services are able to support IPv6 can one really begin to switch off IPv4.11

1.2.6. IP address management
The Internet Assigned Numbers Authority (IANA), a function housed within the Internet Corporation for Assigned Names and Numbers (ICANN), manages the global pool of IP addresses. IANA allocates IP addresses to the Regional Internet Registries (RIRs).

8 Contribution, Paul Wilson, APNIC, Australia.
9 An IPv6 address is represented by 8 groups of hexadecimal values, separated by colons (:). The IPv6 address size is 128 bits. A bit is a digit in the binary numeral system and the basic unit for storing information). The preferred IPv6 address representation is: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where each x is a hexadecimal digit representing 4 bits. “X” ranges from “0-9” or from “a-f.”
10 In real-world terms, for example, the number of IPv6 addresses available amounts to approximately $5 \times 10^{28}$ addresses for each person alive today, or $2^{52}$ addresses for every observable star in the known universe. See: Ivy Wigmore, IPv6 Addresses: How Many is that in Numbers? (January 2009), IT Knowledge Exchange, available at: http://itknowledgeexchange.techtarget.com/whatis/ipv6-addresses-how-many-is-that-in-numbers/.
11 Techniques are now emerging that allow IPv4 to be moved to a service layer at the edge, which can thereby reduce the overall IPv4 footprint and smooth the migration towards the sunset of the legacy protocol.
There are five RIRs, each of them responsible for a specific geographic region:

- **AFRINIC** African Region
- **APNIC** Asia-Pacific Region
- **ARIN** Canada, USA, and some Caribbean Islands
- **LACNIC** Latin America, including some Caribbean Islands
- **RIPE NCC** Europe, the Middle East, and Central Asia

The [Number Resource Organization (NRO)](https://www.nro.net) is the coordinating body for the RIRs.\(^\text{12}\)

The RIRs further allocate smaller blocks of IP addresses to National Internet Registries (NIRs), Local Internet Registries (LIRs), or to ISPs within their regions. As discussed in-depth below, many RIRs conduct important outreach on IPv6 by providing training and education to the community. Such efforts are crucial to promoting IPv6 adoption.

Deploying IPv6 is a crucial investment to make in order to sustain the growing Internet. In the next section, we address the primary reason for IPv6 adoption, that is, IPv4 exhaustion. Then we discuss a few stopgap measures that were developed to help tide the Internet over until IPv6 is widely adopted – measures that are ultimately unsustainable. We then emphasize some of the many benefits that different stakeholders stand to gain by adopting IPv6.

### 1.3. Why is it better to adopt IPv6 now?

IPv6 is crucial to the Internet's sustainable growth, especially in light of the forthcoming Internet of Things (IoT), which will require much more IP address space than is. As one contributor explained:\(^\text{13}\)

*Projects that interconnect devices to reduce power consumption, increase efficiency and traceability, and generally make better use of the world's existing resources will require the allocation of vast numbers of IPv6 addresses. Ubiquitous connectivity of these devices using IPv6 is paramount to a simple roll-out in consumer markets, from inter-connected cars, home automation (light bulbs, refrigerators, power meters, [etc.]), and industrial settings, as well as the logistical back-end cloud services that are needed to service this high growth, high innovation ecosystem.*

---


The availability of IPv4 addresses is limited. The demand for IP addresses will only increase as time goes on, as the Internet expands, as more devices are connected, and as more people come online. The availability of IPv6 addresses is, with proper management, effectively limitless.

This set of circumstances, in and of itself, should be a major motivation for businesses, governments, and all others invested in the Internet to embrace IPv6, but the new protocol’s adoption rate has been more sluggish than the technical community had hoped. Today, the global uptake of IPv6 compared to the number of IPv4 addresses is still relatively low.\(^4\) This likely due to the cost associated with making a transition that includes reconfiguring networks, providing training, purchasing new equipment, and so on. Despite the fact that more than one-half of the end-user equipment deployed on the Internet is capable of supporting IPv6, less than 10% of this same equipment connects via an ISP that provides IPv6.

### 1.3.1. IPv4 is running out

The availability of IPv4 addresses is now extremely limited. As of June 2015, all RIRs, except for AFRINIC, had exhausted the supply of available IPv4 addresses allocated to them by IANA. They can continue to distribute the IPv4 addresses that have been allocated to them, but cannot ask IANA for new ones. While some RIRs have policies to supply limited quantities of IPv4 addresses to new network operators, the demand for addresses, created by the continuing rapid expansion of the Internet, will eventually exhaust this remaining supply.

### 1.3.2. “Stopgap” measures are inadequate

The BPF mentioned two “stopgap” measures that developed in response to the impending exhaustion of IPv4. First, a new “market” emerged, where IPv4 addresses are bought and sold between private parties. Second, techniques like NAT are used to enable multiple devices to share a single IP address, a temporary solution that comes with additional drawbacks.

#### 1.3.2.1. Problems with the IPv4 “market”

In 2011, in light of the growing scarcity of IPv4 addresses, private “markets” for the sale and acquisition of IPv4 addresses developed. It is important to note that these types of commercial transactions take place outside of IANA. IPv4 addresses and address blocks are bought and sold in direct transactions between users, or with the help of so-called “IPv4 address brokers.”

These sales are private. Prices vary and are not always made public, but some sources mention prices of 9 USD – 10 USD per address.\(^5\) Large amounts of money are being paid to acquire

---

\(^4\) See, for example, Google’s collection of statistics about IPv6 uptake, presented on a country-by-country basis, available at: [https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption](https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption)

IPv4 addresses. For example, Microsoft paid Nortel 7.5 million USD for IPv4 Addresses in 2011. More recently, governments are beginning to sell the IPv4 addresses that it no longer uses.

One contributor said that the IPv4 market is currently growing, but that some expect a downturn in transfers to begin by 2016 – speculating that its “overall viability will begin to degrade within a relatively short time frame.”

Most transfers of IPv4 addresses are free from incident, but there have been rumours of routing misbehavior and hijacks. Sometimes, IPv4 address transfers can complicate geolocation by giving errors for geolocation providers.

1.3.2.2. The downsides of NAT and CGN

Conventional NAT has been used in homes and offices for many years. Carrier Grade NAT (CGN) is a more recent development. CGN enables an ISP to provide service through an IPv4 address that can be shared not only across a number of different devices in a single, local network, but between multiple networks as well. CGN often adds an additional layer of address translation, thus another level of complexity and cost to the existing IPv4 network.

NATs and CGNs are not viewed as ideal solutions for IPv4 exhaustion; they increase the complexity of a network, incur costs for operational support, introduce complications for law enforcement, and require additional computing and memory resources. They also create a single point of failure – the NAT device – and can increase latency on the network. Extensive use of CGNs can diminish the speed and efficiency of applications, reduce network flexibility

---

19 A traditional NAT between the customer’s network and the service provider puts all devices on the customer’s network behind one public IP address. CGN adds another NAT within the service provider’s network, and assigns private IPv4 addresses to the different customers within the network rather than public and globally unique IPv4 addresses.
20 For an explanation about how NATs can impede the Internet’s global integrity and reach, see: Leslie Daigle, On the Nature of the Internet (March 2015), Global Commission on Internet Governance (GCIG) Paper Series, Paper No. 7, available at: https://www.cigionline.org/publications/nature-of-internet.
21 Latency is the time elapsed between the transmission of IP packets from the originator and reception of those IP packets at the receiver.
22 NAT uses Transmission Control Protocol (TCP) ports on the NAT gateway, of which there are only 65,535. Each outgoing connection uses a port, and this number can become exhausted quickly. In this event, the NAT gateway will be unable to allocate ports for new connections. The obvious consequence is the increase of latency on the network.
and robustness, and render Internet-based services more unstable. Additionally, CGNs and NAT have a number of security and privacy implications.\footnote{As for privacy, CGNs, for example, provide direct insight into and a complete log of the online activities of each and every customer. As for security, one contributor explained that, in his experience, ISPs that provide NAT equipment to its customers often do not take enough care of the security on the network, making the network less secure.}

Having considered the risks of avoiding IPv6 adoption, we now turn to the benefits of deploying the new standard.

### 1.3.3. The benefits to IPv6 adoption (per stakeholder)

Until recently, there has been little-to-no immediate benefit in deploying IPv6 and, in competitive terms, no “early adopter” advantage. This contributed to the slow deployment of IPv6, prior to around 2012. However, now that more Internet users are connecting via IPv6 (e.g., Google measurements indicate \textit{more than 20\% of end users} in the United States now use IPv6) and more content is being made available over IPv6 (8\% of Google’s traffic is delivered via IPv6), the immediate benefits to deploying the new protocol are gaining visibility. This should drive IPv6 adoption at a faster pace than before.

#### 1.3.3.1. For content providers and publishers

As a content provider, it is entirely possible to host and deliver all content over IPv6.\footnote{Content providers can also reach users of the legacy protocol using NAT technologies. See: T. Anderson and Redpill Linpro, \textit{SIIT-DC: Stateless IP/Internet Control Message Protocol (ICMP) Translation for IPv6 Data Centre Environments} (April 2015), IETF, available at: \url{https://tools.ietf.org/html/draft-anderson-v6ops-siit-dc-01}.} When content is made available via IPv6, a significant number of users will immediately start to receive that content through IPv6, in preference to IPv4. In many cases, performance will be improved because traffic will not be flowing through the aforementioned NAT or CGN devices, but directly to the user. Facebook, for example, directly measured a performance benefit to mobile handsets using IPv6, and “has seen users’ News Feeds loading 20 percent to 40 percent faster” on such devices.\footnote{Dan York for the Internet Society’s (ISOC) Deploy360 Blog, \textit{Facebook News Feeds Load 20-40\% Faster Over IPv6} (April 2015), available at: \url{http://www.internetsociety.org/deploy360/blog/2015/04/facebook-news-feeds-load-20-40-faster-over-ipv6/}.}

#### 1.3.3.2. For network operators

By providing end users with IPv6 services they can then, in turn, access content available over IPv6. This will remove the traffic load on CGN infrastructure and bypass NAT functions in customer NAS (network access server) devices.

#### 1.3.3.3. For end users

Provided their ISP provides IPv6 services, users with IPv6-enabled devices can access content from IPv6-ready content providers, with improved performance. IPv4 connectivity may still be
required by some software and services. In this case, an end user’s ISP will continue to provide IPv4 services, which will be used automatically by a connected device as needed.

1.3.3.4. For mobile carriers and their customers

Today, almost every mobile device is connected to the Internet via a private IPv4 address, meaning that it relies on CGN technologies within the mobile operator network. If a mobile connection is shared (whether from a smartphone, tablet, or a dedicated mobile hub), then this introduces a second layer of NAT, which adds to the complexity and inefficiency of the connection.

However, the most recent mobile phones and devices use operating systems that fully support IPv6. Some mobile service providers are now successfully providing IPv6 services as well. Deploying IPv6 reduces the complexities and inefficiencies described with NAT and CGN, above.\(^{26}\)

1.4. Hurdles to IPv6 adoption

Widespread adoption of IPv6 faces a number of challenges, which should be taken into consideration when developing IPv6-related policies, or planning to deploy IPv6. Below are examples of hurdles to IPv6 adoption provided during the BPF.

1.4.1. Managing network configuration

Deploying IPv6 is no small undertaking for an ISP. Existing devices, servers, and software used by ISPs are IPv4-based and need to be upgraded or replaced in order to comply with IPv6. While this can be done in stages and often at little direct cost due to increasing IPv6 availability in normal upgrade cycles, it certainly requires planning, particularly as most networks need to keep operating while undergoing upgrades.\(^{27}\)

1.4.2. Wholesalers providing IPv4-only bitstream services to retailers

In some cases, depending on the market, an access wholesaler might have the exclusive right to activate a fiber optic network, that is, to provide bitstream access. In the event that the bitstream access provided only supports IPv4-based services, it is impossible for the retailer (the ISP the end customer has chosen) to provide IPv6. Even if a retailer is able to support IPv6,

---

\(^{26}\) RIPE NCC provides a helpful document for these occasions. See: *Requirements for IPv6 in ICT equipment* (June 2012), available at: [https://www.ripe.net/publications/docs/ripe-554](https://www.ripe.net/publications/docs/ripe-554).

the wholesale provider might effectively block that ISP’s IPv6 deployment by only offering them a product that supports IPv4.\(^{28}\)

1.4.3. Hardware and software compliance

A number of business-level vendors continue to treat IPv6 as a “feature request” in lieu of a baseline, giving lower priority to IPv6 than it should. Hardware and software vendors should focus on providing more IPv6-capable products. Cable modems, routers, Network Attached Storage (NAS) devices, etc., sold through both online and offline retail electronics sellers should support IPv6 straight out of the box.

It is worth noting that most modern consumer devices not only support IPv6 directly, but their operating systems also enable IPv6 automatically and require IPv6 for support purposes.

1.4.4. Slow adoption by content and application providers

It took some time before big players in the ICT industry such as Microsoft and Apple made their operating systems and software IPv6 compatible, but such support now exists. Moreover, IPv6 often cannot be disabled on these platforms. Apple, for example, now requires all developers submitting applications to the App Store to support IPv6.\(^{29}\)

Websites and applications may require updating in order to support IPv6. Older sites may also have hard-coded assumptions about IP addresses and, thus, will not work with IPv6.

1.4.5. Training people and expanding capacity building

The required expertise to develop and maintain stable, efficient, and secure IPv6 services and applications is in short supply. The dearth of human resources and capacity with regards to IPv6 is a significant impediment to deployment globally, particularly in developing countries. To ensure that new generations are adept in working with the new standard, various groups such as a number of RIRs and the Network Startup Resource Center have invested in developing training materials and courses to help engineers familiarize themselves with this new technology and bridge the gap that exists in human capacity between IPv4 and IPv6. Their efforts are discussed in further detail in Section 3, which focuses on capacity building.

***

\(^{28}\) Swedish ISP Bahnhof, for example, is having issues deploying IPv6 to a customer in Sundbyberg, Sweden, as discussed by the Swedish competition authorities, available at: [http://www.konkurrensverket.se/beslut/15-0220.pdf](http://www.konkurrensverket.se/beslut/15-0220.pdf) (in Swedish).

\(^{29}\) See: Iljitsch van Beijnum, ArsTechnica, Apple to iOS devs: IPv6-only cell service is coming soon, get your apps ready (June 2015), available at: [http://arstechnica.com/apple/2015/06/apple-to-ios-devs-ipv6-only-cell-service-is-coming-soon-get-your-apps-ready/](http://arstechnica.com/apple/2015/06/apple-to-ios-devs-ipv6-only-cell-service-is-coming-soon-get-your-apps-ready/).
The long-term sustainability of the network and success of the Internet depends on IPv6 adoption. Efforts made to extend the lifespan of IPv4 (e.g. NAT and CGN) are suboptimal and risk making the Internet slower, and more expensive.

Creating an environment that encourages coordination between different actors in the Internet value chain is the key to supporting the adoption of IPv6 within the local community. In Section 2, we look at how IPv6 Task Forces encourage such coordination.

2. IPv6 Task Forces: A platform for best practices

The “IPv6 Task Force” – in and of itself – is a best practice for creating an enabling environment for IPv6 adoption. The local Task Force is also normally the best place for different stakeholders to come together to discuss and develop IPv6 deployment best practices.

Generally speaking, IPv6 Task Forces work to promote IPv6 deployment in their country or region by raising awareness, providing advice, conducting outreach, and making recommendations to government on national IPv6 policy. Task Forces are usually comprised of people from industry, government, network operator groups (NOGs), research and education networks, universities, and Internet organizations such as the Regional Internet Registries (RIRs) or the Internet Society (ISOC). People participate within Task Forces as volunteers or as part of their employment.

There is no fixed formula for an IPv6 Task Force, but they all have the same goal: to bring people and knowledge resources together in order to advance the support for and adoption of IPv6 in the local or regional ICT sector.

In this section of the document, we take a look at IPv6 Task Forces, their different models, activities, and the common challenges they face.

2.1. Different Task Force models

IPv6 Task Forces come in different shapes and sizes. They vary in terms of geographic scope and organizational type. For the most part, IPv6 Task Forces are multistakeholder in nature, meaning that the membership is composed of different stakeholders, including network operators, academia, government officials, and the private sector, among others.

2.1.1. Geographic scope

Many countries have a national IPv6 Task Force and, in the case of some larger countries, regional or state-specific Task Forces (e.g. the Rocky Mountain or Texas IPv6 Task Forces in the United States). Task Forces reach out to the broader community in order raise IPv6
awareness and engage others in IPv6-related activity. They often function as a focal point for the media and others who have IPv6-related questions.

National IPv6 Task Forces often collaborate on a regional basis, for example, at the Asia Pacific IPv6 Task Force, the LAC IPv6 Task Force in the Latin American and Caribbean region, or the North American IPv6 Task Force. Regional meetings enable participants to exchange information with members of other Task Forces who, while from different countries, may operate in similar cultural, economic, and regulatory environments. Thus, participants are able to identify and solve for common challenges.

For instance, network operators who are active in multiple or neighboring countries can discuss how to deploy IPv6 on cross-border network infrastructure. One contributor recalls seeing this happen in the Caribbean, where at the Caribbean Association of National Telecommunication Organizations (CANTO), “many Caribbean service providers were working together to connect 800+ islands and 27 countries.”

In addition to the venues and efforts described above, there is the Luxembourg-based IPv6 Forum, which was established in 1999 as an open and global consortium of vendors, industry experts, and network and service providers. The IPv6 Forum is similar to other IPv6 Task Forces, albeit with a broader geographic scope. Moreover, it served as the primary model for the early IPv6 Task Forces, and works with people in different countries to establish local IPv6 task forces. The Swiss IPv6 Council, for example, is a chapter of the IPv6 Forum that “provides a platform to support IPv6 deployment in Switzerland.”

The certification activities of the IPv6 Forum are discussed in Section 7, below.

Irrespective of geography, there is an overarching type of engagement and collaboration that occurs between individual Task Force members who participate in regional and international meetings, for example, Network Operator Groups (NOGs), RIR community meetings, and the Internet Engineering Task Force. These individuals play important roles in connecting local efforts to global and regional discussions.

Lastly, various industry consortia have established projects or begun dedicating time to IPv6 in their normal activities. One example is the Industrial Internet Consortium, which is “currently working on IPv6 issues with many hardware manufacturers.”

2.1.2. Organizational type

Some IPv6 Task Forces are organized on a formal basis, while others are less formal. In any event, Task Forces are, “by their very nature...volunteer/industry-led, hence not-for-profit. It’s

---

30 Survey, Silvia Hagen, Swiss IPv6 Council, Switzerland.
31 Contribution, Olivier Crepin-Leblonde, ICANN ALAC, United Kingdom.
already hard enough to put the message out there, it would be pretty hard to make a profit doing it. That said, there are several for-profit courses for IPv6 implementation.\textsuperscript{32}

Some Task Forces have been established and continue to be supported by their government, as is the case in Indonesia, for example.\textsuperscript{33} In the Netherlands, the Ministry of Economic Affairs established the Dutch Task Force in 2005.\textsuperscript{34}

2.1.3. Membership composition and participation

As mentioned above, Task Forces are composed of various stakeholders in the ICT sector, including network operators, government officials, academics, and software and hardware vendors. In some instances, global vendors support the participation of local staff in IPv6 Task Forces, which is useful because this enables more effective communication and collaboration with large vendors that are headquartered overseas.

Task Forces are typically initiated by people who have a technical focus (engineers, operators, developers, and Chief Technology Officers (CTOs)). There is much to be said for broadening this technical group to include participants with roles that are non-technical in nature, for example, the Chief Financial Officer (CFO) of an organization planning to deploy IPv6. Broadening the group will also allow task forces to leverage a wider range of skills and networks. As one BPF participant explained:\textsuperscript{35}

\textit{[For most organizations], migration to IPv6 or \textquotedblleft dual stack\textquotedblright is going to cost a great deal of money, including many hidden costs ... Therefore, having a CFO with the skills appropriate for managing budget and financial planning should be present, early on.}

An additional aspect of Task Forces worth noting is that, as is the case in some other Internet Governance venues, Task Force members normally participate in their individual capacities, as opposed to representing the specific positions or objectives of their employers.\textsuperscript{37}

2.2. Task Force activities

IPv6 Task Force members meet to share best practices, collaborate on new ideas, tackle deployment barriers, share updates on their own deployment efforts, and more. Many IPv6 Task Forces operate websites and mailing lists to archive and distribute information, as well as to facilitate discussions in between meetings. Some groups meet once a year, while others may meet as often as twice a month. Usually, Task Forces adhere to an open model, which means that anyone interested in IPv6 deployment is welcome to participate.

\textsuperscript{32} Ibid.
\textsuperscript{33} Survey, Satriyo Wibowo, ID-IPv6TF, Indonesia.
\textsuperscript{34} Survey, Erik Huizer, SURFnet, The Netherlands.
\textsuperscript{35} Contribution, Aaron Hughes, 6connect, USA.
\textsuperscript{36} “Dual stack” refers to the simultaneous recognition of IPv4 and IPv6 by a network.
\textsuperscript{37} Survey, Azael Fernandez Alcantra, IPv6 Forum, Mexico.
During the Best Practice Forum (BPF) discussion, IPv6 Task Force organisers identified a number of activities that they have in common. In this section, we consider these shared practices.

2.2.1. Creating a space for collaboration

In one example, the IPv6 Council in Belgium provides a space for collaboration on IPv6, where participants meet to share information on the status of IPv6 deployment, organise outreach and awareness raising activities, and share their knowledge and experience on IPv6 deployment. In its survey response, the IPv6 Council listed characteristics of its programme that have contributed to its success:

- A policy of open communication during meetings, giving the floor to anyone who wants to step up
- Having a social event after the meeting
- Hosting meetings at member venues, changing location each time
- A policy of open participation, where everyone is welcome

2.2.2. Raising awareness

IPv6 Task Forces work to raise awareness on IPv6 deployment in various ways. One example, submitted from the Swiss IPv6 Council, showed how an information-gathering exercise can also be used to raise awareness and lead to action.

The survey we did among the Top Alexa 75 websites in Switzerland gave the opportunity to call people and ask them about their plans, which again created opportunity to tell them why it could be important to them. This actually led to the dual-stacking of several major websites in Switzerland, which can again be used to convince others.

2.2.3. Providing advice to businesses

In general, the local IPv6 Task Force is a good first port of call for resources and advice on IPv6 deployment. The IPv6 Forum in Thailand, for example, is currently “working with the Government to create an IPv6 Nation[al] Roadmap,” whilst the Task Force in the Netherlands maintains a web resource for different stakeholders, including the public sector. They provide the following simple checklist for government employees planning IPv6 deployment across a network.

1. Assign a project manager

---

38 Survey, Carl Wuyts, IPv6 Council Belgium, Belgium.
39 Survey, Silvia Hagen, Swiss IPv6 Council, Switzerland.
40 Survey, IPv6 Forum Thailand.
41 Website of Nederlandse IPv6 Task Force. (Google translation).
2. Go talk to your ISP
3. Determine which network components should be replaced or upgraded
4. Identify what the project manager will need to train your team
5. Determine what the possible hardware and software replacements will cost
6. Look for qualified suppliers and consultants to conduct the transition
7. Compile a project plan
8. Submit your cost estimate to the person who is responsible for budgeting and decision-making

As discussed further in Section, some Task Forces provide IPv6 capacity building workshops. One contributor suggested that Task Forces consider “feeding the debate with case studies” in order to help illustrate in a holistic way “what can be done for this next generation protocol, e.g. network upgrades, capacity building for engineers and decision makers, etc.”

2.2.4. Making policy recommendations to governments

Government involvement in IPv6 adoption is critical, as explained further in Section 5 of this document. IPv6 Task Force members are an excellent resource for governments, because they are almost always the most knowledgeable and motivated people in the area when it comes to IPv6. Concerned about IPv4 exhaustion, the limitations of NAT and CGN, and aware of the opportunities created by IPv6, they invest time and resources into producing policy recommendations for and providing advice to governments.

For example, the IPv6 Task Force in Venezuela provided a set of recommendations to their government, suggesting that government services be required to support IPv6 (concurrently with IPv4, referred to as “dual stack technology”), and that hardware in the country, whether imported or produced domestically, be required to run dual stack technology. The Task Force offered other recommendations relating to CONATEL, Venezuela’s telecommunications regulator, suggesting that it explore ways “to encourage ISPs to deploy IPv6 … one way is to give tax discounts to ISPs [for using IPv6].”

In addition to the Task Force examples above, RIRs and other bodies provide recommendations to governments regarding IPv6. APNIC, for example, has outlined various ways in which governments can create an enabling environment for IPv6 adoption:

---

42 Survey, Vymala Thuron, AFRINIC, Mauritius.
43 For information on NATs and CGNs, see Section 1, above.
45 List, Miwa Fujii, APNIC Australia. See also: https://www.apnic.net/community/ipv6-program/ipv6-for-governments.
- Mandate for IPv6 readiness in government procurement forms for ICT goods and services
- Conduct research on IPv6 readiness in the industry
- Develop policies, guidelines, and roadmaps to enable IPv6 in government and network infrastructure
- Subsidize IPv6 skills training for industry members to support human capacity development
- Lead the industry by example in adopting IPv6
- Encourage the development of partnerships between government and industry
- Include the necessity of IPv6 deployment in ministerial statements

2.3. Common challenges identified by Task Force leaders

Many Task Force organisers cited funding and coordination as challenges to maintaining an IPv6 Task Force. In one contributor’s experience, “financing is very hard, [and] sponsorship has dropped substantially since 2010. People appreciate initiative, but nobody wants to contribute financially.”

Starting an IPv6 Task Force can be challenging as well. Speaking from experience, one contributor advised that, in order to get an IPv6 Task Force off of the ground, one needs “to find some core work people, even in a small number” who are willing to dedicate their time to the exercise. “[I]f they are good enough,” he explained, “[i]t can kick off.”

Some survey participants also cited the lack of key stakeholder participation as a challenge for their Task Force in promoting national IPv6 deployment. For example, one contributor said: “In our country, the dominance of the [two] big ISPs, and their lack of interest and promotion of IPv6 is what [has delayed IPv6] deployment.” This situation was echoed among other (though not all) survey respondents:

**ISPs are not interested in promoting [IPv6 activities], and the government does not invest in the [task force].**

When asked why this was the case, another contributor responded by explaining that, once an ISP has its infrastructure installed and running, it will seek the highest possible return on its investment. Adopting IPv6 requires major changes to the network and business operations, and these changes cost money. In the absence of a requirement in some form, by a government or an IPv6 business incentive for the ISP, the ISP will defer adopting the new standard – even

---

46 Survey, Silvia Hagen, Swiss IPv6 Council, Switzerland.
47 Survey, Rafael Ignacio Sandoval Morales, IPv6 Forum, Colombia.
48 Survey, IPv6 Forum, Mexico.
49 Survey, IPv6 Forum, Colombia.
though adoption and investment is what is required to ensure the sustainable growth of the Internet, as well as the ISP’s future business.\(^{50}\)

In light of the above mentioned challenges, one contributor suggested increased inter-networking of the IPv6 Task Forces, beginning with an understanding of “how the IPv6 TFs [are] seeded, for example. How did each of the existing TFs make people aware of their existence? … Using other/existing lists that may have overlapping interested parties [could be used] to send an ‘announce-style’ message to notify the regional group of a new TF’s existence.”

***

We elected to begin this document with an introduction to IPv6 Task Forces because they (or their members) often engage other best practices described throughout the document. A non-exhaustive list of IPv6 Task Forces is provided in the Appendix.

3. Capacity building

“Capacity development” has been described by the United Nations Development Programme (UNDP) as “the process through which individuals, organizations, and societies obtain, strengthen, and maintain the capabilities to set and achieve their own development objectives over time. Simply put, if capacity is the means to plan and achieve, then capacity development describes the ways to those means.”\(^{51}\) People also refer to capacity development as “capacity building.” In this document, we will use the latter term – capacity building – in the parlance of this BPF’s participants.

Capacity development is critical to the successful deployment of IPv6. Perhaps most important is technical capacity building for network operators, but developing an understanding of IPv6 at a non-technical level – by the CFO of a company, for instance – will help to create an enabling environment for IPv6 adoption.

In this section of the document, we explore technical and non-technical capacity building activities, which carry the capacity development process described by the UNDP above into the arena of IPv6 adoption.

---

\(^{50}\) ISPs are commercial entities where training staff on IPv6 involves cost, and “the curve of knowledge about IPv6 takes time: preparing their equipment, services, employees, and products.” Email, IPv6 Forum, Colombia.

3.1. Providers of IPv6 capacity building programmes

A number of different organizations, not-for-profit and for-profit, provide IPv6 capacity building programmes.

National Research and Education Networks (NRENs) and Regional Internet Registries (RIRs) - not-for-profit organizations - deliver IPv6 capacity building workshops. In the latter case, AFRINIC (the Internet Numbers Registry for Africa), for example, conducts hands-on IPv6 training throughout the continent. Each year, AFRINIC trains more than 600 “network engineers in at least 17 countries on practical skills required to plan and deploy IPv6 networks.” These workshops, led by AFRINIC with the participation of ISP associations, government agencies, and members of academia, are free-of-charge to participants.

Having conducted IPv6 trainings since 2010, AFRINIC offered a number of insights in its survey response, suggesting that others interested in organising their own IPv6 capacity building workshops consider the following:

- An effective IPv6 foundations training session requires at least two full days
- Participants must be pre-screened for requisite knowledge before attending
- Content must be 50:50 theory/practice
- Rigorous feedback must be put in place and used to update the content

AFRINIC’s IPv6 training courses have yielded positive results. As explained by Training Manager Mukom Akong Tamon:

Some higher-level participants have gone on to deploy IPv6 after attending the training and a few countries are doing mini-sessions based upon the content [AFRINIC] created.

RIPE NCC (Réseaux IP Européens Network Coordination Center) regularly provides two IPv6 training courses – basic and advanced – as “a standard service to promote and encourage the use of IPv6 in the western hemisphere.” The two-day advanced course teaches attendees how...
to implement IPv6 in their core network, understand the differences and similarities between IPv4 and IPv6 security, configure IPv6 on network equipment, and understand different transition mechanisms.

Over the course of her work as RIPE NCC IPv6 Program Manager, Nathalie Künneke-Trenaman has seen how many people who are new to IPv6 approach the idea of deployment. She offered the following advice:

One of the big problems with IPv6 deployment is that people think they have to do everything at once and that too much new knowledge is needed. It is of vital importance to break a deployment into smaller tasks and evaluate them step-by-step.

Another important element is ensuring that training efforts are made sustainable, by training others to train others. In 2015, together with telecom regulators in Saudi Arabia and the United Arab Emirates, RIPE NCC organised a “train the trainer” program to further embed IPv6 knowledge in the local community and expand the capacity building activities by having local trainers deliver the courses.58

***

The need for technical training is widespread. A few groups deliver training in geographic areas where engineers would otherwise have limited access to the knowledge and information required to successfully deploy IPv6.

APNIC (Asia Pacific Network Information Center) maintains an ongoing collaboration with the International Telecommunication Union’s Development Sector (ITU-D), and provides another example of IPv6 capacity building.59 Over the past five years APNIC and ITU-D have worked together to deliver IPv6 capacity building workshops for “network engineers, the technical staff of regulators, and government policymakers in developing economies in the Asia Pacific region.”60

APNIC Senior Technology Advisor Miwa Fujii summarised the trainings on the BPF discussion list:

The workshop content focuses on IPv6 transition strategies and technologies and IPv6 infrastructure security, including hands-on workshop[s] and teamwork exercises. The course is designed to provide practical and useful IPv6 knowledge and skills that participants can bring back to their home economy and apply in their networks.

58 Contribution, Marco Hogewoning, RIPE NCC, the Netherlands.
59 Opinions supporting IPv6 capacity building were issued from the ITU’s World Telecommunication Policy Forum in 2009 and again in 2013.
60 List, Miwa Fujii, APNIC, Australia. For more information on APNIC’s training programmes, visit: https://training.apnic.net/home.
In a non-RIR example, the Network Startup Resource Center (NSRC), based at the University of Oregon, "works directly with the indigenous network engineers and operators who develop and maintain the Internet infrastructure in their respective countries and regions by providing technical information, engineering assistance, training, [and] donations of networking books, equipment, and other resources."

The goal of NSRC’s work “is to make it easier for local scientists, engineers, and educators to collaborate via the Internet with their international colleagues by helping to connect communities of interest. By strategically working with universities, research institutes, Internet Service Providers, Regional Internet Registries, government agencies, supranational agencies, industry, private foundations and non-governmental organizations, the NSRC helps develop national and regional Internet infrastructure for collaborative research, education, and international partnerships.”

NSRC is mainly funded by the U.S. National Science Foundation and Google.

In addition to the trainings for network operators listed above, there are a number of commercial providers of IPv6 trainings that cater to businesses. Businesses that operate their own IT systems and/or networks require technical training for their network and IT operations staff on network design, configuration, operations, troubleshooting, support systems, and security. This technical training should include general technology training on IPv6 in addition to vendor-specific training on how to configure IPv6 on their specific equipment.

In addition to formal training, whether from a commercial provider or other entity, information should be made sufficiently available to the technical staff to allow them to make informed decisions on equipment purchases and updates (both software and hardware) to support IPv6. This includes clear documentation and support from vendors. IT support staff will need to be included in the training to support users of the business applications and network, and customer support staff will need training to manage cases that involve IPv6.

3.2. Capacity building for non-technical stakeholders

While most of the above-mentioned examples focus on network operators, IPv6 training for law enforcement officials, policymakers, and corporate-level (C-level) business decision makers (e.g., CEOs, COOs, CFOs, etc.) is also very important for creating an enabling environment for IPv6 adoption.

For business decision-makers, training and education are essential to help mitigate risk to business operations. The extent and type of training or education on IPv6 required will depend on the type and size of business. Generally speaking, businesses need to consider investment

---

61 NSRC’s website is available at: https://nsrc.org/
62 Contribution, Hascall “Chip” Sharp, Cisco, USA.
in this training as part of their business and operations plans. This requires education of business decision-makers with the information needed to develop these plans.\footnote{Ibid.}

A few recommendations from BPF contributors for business decision-makers included the following:

- \textit{Build confidence at the decision-making level that IPv6 is “proven technology” and (perceived) risks are manageable}
- \textit{Work with decision-makers directly to help them understand the importance of IPv6 deployment, at a level where they can make a meaningful risk assessment for their business}
- \textit{Ensure that non-technical staff understand the long-term, positive effect of IPv6 deployment on their business goals (for example, enabling growth and the potential for reducing costs)}
- \textit{For product developers and marketing staff, clarify the benefits for organisations that adopt IPv6}

Somewhat similar to the “train the trainer” approach mentioned above, \textbf{SURFnet}, the Dutch National Research and Education Network, documented their best practices on creating an IPv6 addressing plan. SURFnet then made this information freely available to other businesses.\footnote{See: RIPE NCC, \textit{Preparing an IPv6 Addressing Plan} (2010), available at: \url{https://labs.ripe.net/Members/steffann/preparing-an-ipv6-addressing-plan}.} Thus, businesses can learn from SURFnet’s experience. Additionally, in 2013, SURFnet published a document outlining the business case for IPv6.\footnote{SURFnet, \textit{Business case for IPv6: The Internet adds Trillions of Addresses to the Web} (2013), available at: \url{https://www.surf.nl/binaries/content/assets/surf/en/2013/rapport_201309_Business+Case_IPv6_eng.pdf}.}

Lastly, \textbf{APNIC} has a dedicated section on its website that provides IPv6 information for business decision-makers and service providers in the Internet industry.\footnote{These parties include Internet transit providers, access network providers, hosting providers, data center operators, content distribution network operators, mobile network operators, and content providers. See: APNIC, \textit{IPv6 for Decision-Makers}, available at: \url{https://www.apnic.net/community/ipv6-program/ipv6-for-decision-makers}.}

\section*{4. Lessons from the private sector}

In Section 4, we examine best practices identified within private sector organizations - namely with ISPs and content providers. During BPF discussion it became apparent that there are few case studies and best practices to share from enterprise-wide deployment of IPv6.

Approaches to deployment depend on local considerations. As with other illustrations in this document, the practices described below are offered only as suggestions.
One important point made during the BPF was that ISPs and content providers share some best practices in common. This section reviews those practices.

4.1. Review existing infrastructure

ISPs and content providers can begin planning for IPv6 deployment with a high-level review of their existing infrastructure, including software, services, support systems (including sales and customer support), and administrative processes. An evaluation like this is a significant undertaking for the team, so focusing on IPv6 training should be part of the project planning process. One contributor suggested framing the project as an opportunity for everyone to review and assess the company’s vendors, hardware, services, security, and budget. They also shared the following:

*During this process, it is common to learn a great deal about your underlying supporting infrastructure, and either establish a better relationship with existing vendors or … establish new relationships with vendors who support IPv6 and want to be your partner through this transition.*

Further advice from the BPF included assessing any and all dependence on IPv4 across the infrastructure. Describing the impact of IPv6 adoption on a departmental basis was also noted as an important step.

4.2. Determine whether vendors are IPv6-ready

One challenge identified during the BPF related to the capacity of vendors to support IPv6 products and services. According to one contributor:

*There is still a long way to go in terms of IPv6 support in a lot of the equipment out there. A lot of network gear is still IPv4 only on the management interface. Many vendor implementations are buggy.*

When working with vendors, ISPs and content providers should consider testing every aspect of equipment to ensure that it meets their needs. Based on the discussion during the BPF, IPv6 is not yet well understood by the majority of vendors. One contributor suggested that companies confirm vendor expertise in IPv6 before engaging in a contract. One contributor said “many vendors will tell you they are IPv6 ready, but this may not [necessarily] mean that parity exists for features which exist in IPv4.” Another survey response explained:

*Don’t buy any equipment that doesn’t have the IPv6 features that you need. If a manufacturer says that IPv6 is “coming,” don’t take their word for it. Make sure they at least show you a working beta.*

Vendors adept in IPv6 make a big difference for businesses. In Singapore, the ISP StarHub explained that their roll-out of IPv6 was not without challenges, but their vendors were there to assist.

---

68 Ibid.
69 Email correspondence, Seng Chye, StarHub, Singapore.
There were unexpected challenges along the way ... mostly dealing with scaling of routing tables...to deal with a larger than expected install of IPv6-capable Customer Premise Equipment. But fast turnaround and support from the vendor allowed us to identify and get back on track in a short time. The resultant IPv6 traffic growth with progressive rollout was a pleasant surprise after that.

Thus, it is important for the business to know whether its vendor works fluidly with IPv6, and if not, whether that vendor is willing to take steps to become IPv6-ready.

A related example mentioned during the BPF was that Apple now requires iPhone and iPad applications to be IPv6 compliant in order to be carried by the Apple App Store.70

4.3. Provide employees with training and knowledge

Technical and non-technical IPv6 training for employees is necessary. In terms of non-technical roles, employees who interact directly with customers, such as those in the sales, account management, and customer service departments, should receive sufficient training and be able to understand the high-level reasons for IPv6 deployment. Capacity building in IPv6 is discussed in greater length in Section 3.

4.4. Deploy IPv6 for public-facing services

ISPs and content providers should offer their end users / customers IPv6 connectivity through dual stack technology, meaning that both IPv6 and IPv4 are in use.71 Businesses can begin work on dual stack implementation by taking inventory of all outside, public-facing IPv4 services. This should help to define the steps that need be taken to enable dual stack technology. As one contributor summarised:

The simplest approach is to work from the outside in.

By offering public-facing IPv6 services to IPv6-ready end users, businesses will offer better access to their content. End users will also be able to bypass the IPv4 bottlenecks of NAT and CGN. With dual stacked, public-facing services, content providers can enrich the experience of IPv6 end users without affecting IPv4 end users.

To begin, ISPs and content providers who use Content Distribution Networks (CDNs) should contact their CDN about IPv6. Most CDN providers offer dual stack services by default, though some only enable dual stack upon request. For businesses who do not work with CDNs,


71 The Canadian ISP Communicate Freely decided to deploy IPv6 in 2011 after the company encountered problems securing IPv4 addresses. The company considered "IPv6 adoption [to be] the 'new normal' for all IP connected systems.” The company explained in its survey response that it has since made IPv6 available to 100% of its customers via dual stack technology.
enabling dual stack means ensuring that all load balancers, name servers, mail servers, web-servers, app servers, etc., are available over both IPv6 and IPv4.

Once public-facing services are dual stacked, then businesses should consider “work[ing] inwards, making sure that all back-end gear is singled stacked” – in other words, using IPv6 exclusively.\(^\text{72}\)

After deploying dual stack technology for public-facing services, Facebook saw an increase in performance for its mobile end users. In a March 2013, it was reported that certain users connecting to Facebook via IPv6 were doing so “on average … about 30% faster” than users connecting via IPv4.\(^\text{73}\) As software engineer Paul Saab explained, “This is great for our users because that means their news feed loads faster, their pictures load faster – everybody’s happier when things are faster.”\(^\text{74}\)

As of September 2015, 50% of Facebook’s 4G smartphone traffic in the U.S. was being carried via IPv6.\(^\text{75}\)

### 4.5. Migrate to IPv6 on internal networks

*Why maintain two stacks in your entire network [when it is] much easier to handle two stacks at the edge and one internally?*\(^\text{76}\)

During the 2014 v6 World Conference, Facebook presented on the company’s internal migration to IPv6.\(^\text{77}\) The case study canvasses the challenges that were encountered along the way, so it is a useful reference for more technical readers.\(^\text{78}\)

---

\(^\text{72}\) In its survey response, BDCOM, an ISP in Bangladesh, took the opposite approach, implementing IPv6 in its internal networks in 2013, and working on deploying public-facing IPv6 resources more recently. Survey, Mohammad Abdul Bashar, BDCOM, Bangladesh.

\(^\text{73}\) Paul Saab, Facebook, presentation at v6 World Conference (31 March 2015), video available at: https://www.youtube.com/watch?v=An7s25FSK0U&feature=youtu.be&t=19m, (note that this example references speeds observed on the iPhone 6. Saab provides a number of further examples in the video).

\(^\text{74}\) Ibid.


\(^\text{76}\) Ibid.


At the time, 75% of Facebook’s internal traffic was IPv6. Today, Facebook no longer builds new machines with v4 connectivity, and the small amount of IPv4 that remains in use on Facebook’s internal network will be migrated soon.79

Facebook of course maintains a very large network, but IPv6 adoption yields benefits to businesses of all sizes. Local ISP Communicate Freely, based in Ontario, Canada, said in its survey response that eliminating NAT helped with managing customer devices, and added:80

*Where possible, remove NAT and replace with IPv6 only on management networks. You will quickly find this makes management far easier.*

4.6. Set internal deadlines

Seeing that the pool of available IPv4 addresses continues to shrink, BPF contributors recommended that all businesses plan for the inevitability of no IPv4.

*Planning for the inevitable unavailability of IPv4, and the complete adoption of IPv6, with eyes wide open, will make planning for and implementation of IPv6 far easier. Importantly, it will allow for your customers to plan accordingly.*

Though simple, the phased plan outlined below was offered by a BPF contributor as one place to start:

1. Begin with IPv6 education and outreach to customers and partners
2. Support customers in their transition to IPv6
3. Require IPv6 adoption by customers, but allow for dual stacking and IPv4 support at the same time
4. When the time is right, support IPv6 only

4.7. Reach out to customers

One survey response from an ISP described how it sent an “email blast” to its business customers, “explaining the reasons for considering IPv6 adoption.”81 While the outreach effort, “did raise some level of awareness … very few people were interested” and “a few customers were confused.”82

This experience suggests that a steady and repetitive approach to distributing information about IPv6 adoption to customers may be more effective than a one-off email. Updating all customer-facing communications (e.g., invoices, maintenance notifications, marketing material, website, email signatures, etc.) with a note on IPv6 adoption or a link to education would also be useful. One participant suggested creating and maintaining a wiki as a Frequently Asked Questions page for customers:

---

79 Twitter conversation with Paul Saab, Facebook, USA.
80 Survey, Tim St. Pierre, Communicate Freely (ISP), Canada.
81 Survey, Anonymous, USA.
82 Ibid.
There is no better way to answer the same questions from all of your customers than to document them publicly in once place. Not only will you be building a repository for your customers, but you will also be educating your staff on the common issues that your customers face.

For business customers in particular, another suggestion for ISPs was to engage more directly, by inviting them to an on-site training. IPv6 education is a fantastic reason to have a “lunch and learn” with customers. This is also a useful practice for staff.

4.8. Consider different approaches to pricing (for ISPs)

The amount of IPv4 available will continue to decline, and the cost of supporting it will rise. To encourage customers to adopt IPv6 over IPv4, ISPs may want to consider passing on the cost of supporting IPv4 by charging the customer for IPv4 but not for IPv6. This approach suits ISPs with non-residential customers.\(^{83}\)

In this case, it is important to give the customer clear notice and to explain the rationale supporting the price increase. This is also an opportunity to raise awareness about IPv6 adoption.

For example, the customer could receive a notice on their invoice similar to:

_In order to support the growing Internet, we at [ISP] encourage the use of IPv6. Because IPv4 addresses are running out, the monthly cost for an IPv4 address will increase next month to [X]. However, IPv6 will be provided at no cost to you. If you would like to know more about IPv6, please click here._

The above listed practices can be applied not only to ISPs and content providers, but to other businesses as well.

Enterprise-wide IPv6 deployment, however, is a major undertaking that only a few enterprises have experienced. Few examples were identified during the BPF. Contributors suggested that, should the BPF continue, enterprise-wide IPv6 deployment be a future focus area for discussion and research into best practices.

4.9. A case study: Japan

In its submission to the BPF, a Japanese telecommunications provider, identified a number of best practices described within this section. To wrap up this section of the document, we have reproduced the case study in full, below.

4.9.1. IPv6 deployment plan

First, we considered if our customers required an additional subscription for IPv6 services, or if we should provide IPv6 services as default services by combining it to the existing services. We

---

\(^{83}\) Note that this practice is not being recommended by the BPF, but only noted in discussion as an example.
decided to provide IPv6 services as a default services in order to enable smooth IPv6 adoption in the future.

4.9.2. Starting point of IPv6 deployment
We clearly defined which services would be on IPv6. We chose to deploy IPv6 for our services on FTTH, as we expected subscription growth in this service. We also targeted services that we can provide using our own networks.

4.9.3. Confirming IPv6 readiness of network equipment vendors
We verified availability of end-to-end communication routes in order to identify equipment with limited IPv6 capability (e.g., identified equipment which could not manage IPv6 packets at the hardware level, equipment without IPv6 QoS etc). We identified work-around measures to cope with this lack of IPv6 functionalities on our equipment so that we could avoid any negative impacts on performance in forwarding IPv6 packets.

4.9.4. Staff skill-up with IPv6
We conducted staff training on IPv6 as a new service. Our staff are currently stably managing large data traffic on dual stack networks.

4.9.5. Setting internal deadlines toward the IPv6 deployment plan
We set our internal deadline of IPv6 deployment on the timing of IPv4 address exhaustion at JPNIC/APNIC. Although Japan experienced a major earthquake in March 2011, we were able to proceed and successfully launched IPv6 services in April 2011.

4.9.6. Preparing for unexpected events
We managed network equipment, servers, Home Gateway (HGW) and Customer Premises Equipment (CPE) that do not comply with RFC standards by changing parameters. We applied low cost (cost, time, required number of processes) methods for managing unexpected events.

5. Research and Education Networks, and Universities
National Research and Education Networks (NRENs), provide specialised Internet services to learning institutions inside their country. NRENs are usually pioneers in introducing and deploying new protocols and technologies.
Like many NRENs, the China Education and Research Network (CERNET) has “universities, institutions and schools” as customers. CERNET provides IPv6-enabled Internet services to the Chinese student population. In its survey response, the NREN explained that “the connectivity between IPv4 and IPv6 networks (via translation) is the way to transit[ion] the Internet from IPv4 to IPv6.”

GÉANT is the pan-European network serving Europe’s research and education community. It is co-funded by the European Commission and European NRENs. GÉANT has been running IPv6 since 2002. The organisation’s [website](#) is an excellent resource for finding information on the IPv6 work of other European NRENs.

Few contributions were provided during the BPF from universities. However, one contributor shared:

*In recent discussion with several people at UK universities, I have found out that whilst some departments...might have rolled out IPv6 as long as several years ago, they have found it very hard to have IPv6 accepted University-wide, due to the ever-increasing complexity of service level agreements and risk management at University’s management level.*

The contributor went onto explain that it is easier for a single university department to deploy IPv6 because the decisionmaking process is less formal, and the responsibility for quality of service remains within the department. University-wide deployment is seen as a different level of responsibility, considered by people who do not necessarily know what IPv6 is.

Best practices for IPv6 deployment in the university sector, in addition to enterprises, were identified as useful areas for future focus by the BPF.

### 6. Government initiatives

Governments can create an enabling environment for IPv6 adoption in different ways. As one BPF contributor explained:

*Some governments prefer a more "hands-off" approach, expressing their support but wishing the private sector take the lead. Others go a step further by mandating IPv6 compatibility for any government procurement contract, some a little further by offering all government online services over IPv6, and some go [all] the way by taking a very active role in financing research and implementation projects for IPv6 adoption.*

With the exception of the “hands off” approach, the practices mentioned above are covered in this section of the outcome document.

---

84 Survey, Xing Li, China Education and Research Network, China.
85 List, Olivier Crepin-Leblond, ICANN ALAC, U.K.
6.1. Procurement policies

When a government requires IPv6 in its ICT procurement policies, it sends a signal to the industry about the importance of IPv6 adoption and incentivizes businesses to include IPv6 in their bids for government contracts. The wide-variety of websites, Internet-based services, and networks that the public sector owns, operates, or commissions should support IPv6, requiring the vendors who tender for this work to understand and support IPv6 as well. BPF contributors mentioned a number of countries that require their public administrations to run IPv6.86 Below, we cover a few examples.

6.1.1. Germany - Developing “IPv6 Profiles”

In Germany, the Federal Office of Administration (BVA) and the Federal Ministry of the Interior led an IPv6 research project that, in 2013, culminated in the publication of set of documents designed to support IPv6 adoption by the public administration. As described in the IPv6 Transition Guide for the Public Administration (Transition Guide), “the purpose of [the IPv6] project was to define profiles for different categories of devices, and examine and document strategies for the migration to IPv6.”87

The IPv6 Profiles for the Public Administration document and the Profile Table itself facilitate the public procurement of IPv6-ready products and services by Germany’s public sector not only by providing “recommendations for the introduction and procurement of components which support IPv6,” but also by “supporting the acquisition of [IPv6-enabled devices], and [encouraging the] evaluation of existing devices for [IPv6 readiness].”88

The Profile Table distinguishes between necessary and mandatory use of IPv6 in different situations. It specifies requirements in terms of device (routers, firewalls, etc.) and use (stationary, mobile, etc.), which simplifies the public administration’s assessment of whether a tender meets the contract requirements.

The information in the documents from Germany’s IPv6 project “can be used for procurement processes of new devices, the evaluation of existing hardware and software, and in the implementation of and transition to IPv6.”89 While the IPv6 profile is not mandatory for the procurement activities of the different authorities in Germany, it is very well accepted.

English translations of the Transition Guide as well as the IPv6 Profiles document and Profile Table are available online and were published under a Creative Commons license.90

---

86 Other countries mentioned included the Netherlands and Sweden.
6.1.2. United States - Requiring vendors to themselves use IPv6

In 2010, the United States Office of Management and Budget (OMB) issued a memorandum (M-05-22) to executive departments and agencies that described “specific steps for agencies to expedite the operational deployment and use of IPv6.” Among other requirements, executive agencies had to ensure that any procurement they made of networked information technology complied with government standards for “the completeness and quality of [its] IPv6 capabilities.”

During the BPF, one contributor acknowledged that the U.S. government requires all procurements to be IPv6-ready, but some departments go even further by requiring their vendors to use IPv6 themselves.

The reasoning here is twofold. First, vendors should consider actively demonstrating their commitment to fully supporting IPv6. Second, in the long-term, vendor websites that are only accessible over IPv4 will force their customer to keep supporting IPv4 as well, thereby hindering the ultimate decommissioning of IPv4.

Governments and other public sector actors are often service providers themselves. Therefore, it is equally important for governments to deploy IPv6 in the services and infrastructure they own. Showing leadership in this area can help build confidence in other stakeholders to deploy IPv6 as well.

6.2. Deployment strategies

6.2.1. The Kingdom of Saudi Arabia

The Kingdom of Saudi Arabia’s Communications and Information Technology Commission (CITC) is responsible for the nation’s IPv6 Strategy. The objectives identified in the **IPv6 Strategy for Saudi Arabia** are to:

- Prepare for the IPv4 exhaustion by supporting IPv6 and ensure stability, business continuity, and room for continued growth of the Internet in Saudi Arabia
- Ensure a smooth adoption of IPv6 by stakeholders so as to minimize risks

---


92 Ibid. Requirements include the “USGv6 Profile and Test Program.”


94 Ibid.
• Raise overall IPv6 awareness nationwide by approaching stakeholders of both the public and private sectors, highlighting the necessity to adopt IPv6

A phased timeline, with milestones, for IPv6 deployment is a critical element of the strategy. The CITC’s own IPv6 timeline comes via an action plan of initiatives categorized into two tracks: an infrastructure track, and an awareness track.95

As described in its response to the BPF survey:96

Meeting the milestones would facilitate the deployment and further penetration of IPv6 on a nationwide basis so as to eventually realize an IPv6-ready Internet infrastructure in the Kingdom of Saudi Arabia.

Early CITC IPv6 activities focused only on ISPs. In 2013, however, the CITC expanded its IPv6 initiative to include Saudi business enterprises. As part of this effort, the CITC took practical steps to promote IPv6 deployment by implementing a set of pilot projects within selected entities in order to showcase best practices for the benefit all stakeholders.

The CITC often benchmarks the status of IPv6 deployment in the Kingdom against international trends, and assesses those regulatory and technical aspects of the national Internet ecosystem that obstruct the smooth adoption and deployment of IPv6 in the Kingdom.97

6.2.2. Finland

The Finnish Communications Regulatory Agency (FICORA) hosted Finland’s national IPv6 launch day in June 2015 in order to promote IPv6 adoption in Finland and to bring the country’s deployment rate in line with other central European countries.98 The only condition of participation in the launch was that the attendees had to have deployed IPv6 themselves.

As explained in its response to the BPF survey:99

After discussing the topic for 10 years, ISPs were rather ready to take IPv6 into use. It just needed clear goals, some leadership, and definitely marketing, publicity, and peer pressure.

The planning process for the launch began one year in advance. “Organizing a national launch takes time,” explained Klaus Nieminen from FINCORA, who led the project:100

95 Survey, Adeeb Albraidi, CITC, Saudi Arabia.  
96 Ibid.  
97 Ibid.  
99 Survey, Klaus Nieminen, FICORA, Finland.  
100 Ibid.
Make a proposal and see what response it gets. Get at least some ISPs to commit. When it is safe, [engage a] bigger audience. Try also to get broad shoulders to back you, it helps. But still a lot of marketing, talking, and there you go. Try also get some benefits for those ISPs that are taking part in the launch, or example with press releases and media contacts.

One challenge observed during the launch was the hesitance of some ISPs “to take IPv6 into use automatically” because of “security and quality of service concerns.” The organisers, however, remain optimistic:

I think that industry is just rather ready to take the step if given just a little push.

6.2.3. India

In light of IPv4 exhaustion, and “the many inherent advantages of IPv6,” India’s Department of Telecommunications (DoT) has “mandated … timelines for [a] time-bound and phased manner [of] implementation of IPv6 across all stakeholders - service providers, content and application providers, device manufacturers, end user device vendors, cloud service providers, and government organisations.” As explained in a survey response, “as IPv4 addresses are already exhausted, and in view of M2M and IoT [development] in the country, the uptake of the IPv6 will increase rapidly.

Nearly all stakeholders “have been asked to abide by the timelines of the National IPv6 Deployment Roadmap v-II (March 2013) and complete the transition by the mandated timelines. Many of the service providers, content providers, and Government organization[s] are ready right now, [and] almost all end user devices launched after June 2014 in India are IPv6-ready.” The DoT is also tracking progress and engaging with stakeholders.

In the south Indian state of Kerala, the Kerala State IT Mission (KSITM) launched an initiative aimed at upgrading the state’s core IT infrastructure, which was the first step for the transition to state-wide IPv6 deployment. As explained in a recent article:

The IPv6 migration in the initial phase involves transition of State Data Centres (SDCs), e-governance applications, portals and website services hosted in SDCs, and [the] Kerala State Wide Area Network. The remaining government offices...will be covered in the next phase and integrated with the existing national networks and infrastructure like the National Knowledge Network, National Data Centre for Disaster Recovery, and National Optical Fibre Network.

---

101 Ibid.
102 Ibid.
103 Survey, Government of India.
104 Ibid. Note that M2M is short for “machine-to-machine” communications.
105 Ibid.
6.2.4. Japan - IPv6 Study Group - A platform to identify issues and actions for industry players

In 2009, understanding that the exhaustion of the unallocated IPv4 address pool was eminent, the Ministry of Internal Affairs and Communications of Japan (MIC) established an IPv6 Study Group (Study Group) as part of its comprehensive, national effort to address IPv6 adoption.

The Study Group served as a platform for experts and key players in the industry to discuss and identify issues, including issues involving multiple industry players with different roles. The Study Group produced a report which provides a comprehensive picture of the situation to prepare for post IPv4 exhaustion. The report features expert analysis and outlines key milestones for actions to be taken.

In the course of discussions in the Study Group for producing the report, the stakeholders with action items were requested to provide a status update. If they were facing issues with the progress an explanation was needed. This initiative clarified issues where each group of industry players must address in their respective areas. If there are issues which needed to be addressed by other stakeholders, they were able to put it on the table, so other stakeholders could take it back as their action items.

The work of the Study Group succeeded in progressing IPv6 adoption to a certain level, in creating a situation where the industry players were faced to take actions to address issues identified by the study group. through regular progress tracking and updating of the issues. The MIC restarted its Study Group in July, 2015, and is currently considering an additional measure to deploy IPv6, based on the recognition that IPv6 is one of the essential elements supporting the Internet of Things (IoT).

6.3 Providing guidance
The Infocomm Development Authority of Singapore (IDA) spearheaded an IPv6 Transition Programme to address IPv4 exhaustion and facilitate a smooth transition to IPv6. The

programme promotes readiness and adoption of IPv6 in the local industry, through a series of projects.\textsuperscript{108}

As part of this programme the IDA developed the \textit{IPv6 adoption guide for Singapore}. This document sets out detailed IPv6 adoption guides, tailored to assist each stakeholder group in translating their strategic IPv6 objectives into practical implementation. The guide explains IPv4 exhaustion, takes into account the findings of the national IPv6 readiness survey for Singapore and includes technology roadmaps.

\section*{6.4. Collaboration with Industry and other stakeholders}

Government collaboration with local industry, academics, and other interested stakeholders was a commonly supported best practice during the BPF. IPv6 Task Forces, covered in Section 2, are obvious venues for government officials to collaborate.

In one example, in 2011, the Norwegian Communications Authority (\textbf{Nkom}) established a national working group on IPv6 deployment. The purpose of this working group, attended mainly by government officials and ISPs, was to “identify key issues and discussions associated with the transition to IPv6.”\textsuperscript{109} Similar to the work of the IPv6 Task Forces addressed above in Section 2, Nkom’s working group serves as a platform to help plan for IPv6 deployment. The initiative then led to further collaboration in the industry between IKT-Norge (Norway’s ICT industry representative), ISPs, and other stakeholders.\textsuperscript{110}

It is worth noting that governments can engage with local IPv6 Task Forces, not only by sharing their experiences with IPv6 deployment but also by gaining input from industry experts.

\section*{7. The role of the end user / consumer in IPv6 adoption}

End users support IPv6 adoption when, as consumers, they buy IPv6-enabled devices and sign up for IPv6 services. Growing end-user demand for IPv6-ready goods and services should, in turn, encourage upstream providers and device manufacturers to adopt IPv6.

This section considers a few different ways that consumers can encourage IPv6 adoption.

\begin{footnotesize}
\begin{footnotes}{\footnotesize
\begin{enumerate}
\item For more information on IDA’s efforts supporting IPv6 adoption, visit: https://www.ida.gov.sg/Tech-Scene-News/Technology/IPv6.
\item Survey, Ørnulf Storm, Norwegian Communications Authority, Norway.
\item Ibid.
\end{enumerate}
\end{footnotes}
\end{footnotesize}
7.1. The developing market for the Internet of Things

“Many discussions of the Internet of Things (IoT)\textsuperscript{111} appear to assume that IP address space is an unlimited resource that will scale as the IoT scales to previously unimagined proportions. But the IP address space is not unlimited. In fact, the IPv4 address space has been depleted since February 2011. And that could have been the single best reason to consider IPv6 ... for the future of [the] IoT.”\textsuperscript{112}

More “things” are coming online and the Internet is growing as a result. For example, early demand by the technically-savvy for “home automation" or the "smart house" has created a market for IPv6-enabled home appliances. BPF contributors mentioned an array of different devices, including IPv6-enabled printers, Nest thermostats, cameras made by Panasonic, and light bulbs made by Phillips. The benefits of IPv6-enabled devices should become more apparent as the IoT develops over time.

For early adopters, it is difficult as a consumer to shop for IPv6-enabled devices. For non-technical consumers, purchasing an IPv6-ready device does not mean “plug and play.” Rather, the device still must be configured. One contributor elaborated on the problem:

\textit{There are no interface standards for how configuration features are labeled [o]n setup screens, nor is there a standard or even best practice for how the device alerts the consumer that it is using IPv6. For example, there isn't an IPv6 equivalent to the 4G LTE shown on cell phones.}

A very different type of market challenge was also identified during the BPF: many low cost, low quality IPv4-only devices are “flooding the market,” which contributes to the delay of IPv6 deployment. Simply, those who have no access to IPv6 equipment cannot deploy IPv6.

7.2. Consumer awareness

BPF contributors identified consumer awareness as one area that could benefit from new best practices. It is not easy to raise and maintain the interest of an average consumer in the technical standards that their electronic devices use. As one contributor explained:

\textit{Most consumers aren't aware of IPv6; no surprise there, as consumers also aren't aware of what [quadrature amplitude modulation (QAM)] standard their TV uses or other technical details about the technology they use every day. That's very likely never to change.}

\textsuperscript{111} “The Internet of Things has been defined in Recommendation ITU-T Y.2060 (06/2012) as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.” International Telecommunication Union (ITU) Internet of Things Global Standards Initiative (IoT-GSI), available at: \url{http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx}.

It was then suggested, however, that a “buzzword like "v6 enabled" would be a good thing to provoke [the] curiosity of … end users that care about such details.” The same contributor added:

*That said, it’s one thing to put such promotional words/logo on devices, it’s another thing for it to have meaning to the buyer. At the moment, a typical end user just wants to be able to access his/her favourite services … So long as the device is tested to do that, they would be fine.*

### 7.3. Certification

A well-recognised, voluntary standard for certification of IPv6-readiness in consumer devices was raised as a best practice. During the BPF discussions, the IPv6 Forum’s “IPv6-Ready Logo Program” was identified as an example. This program focuses on IPv6 conformance and interoperability testing. Its goal is “to increase user confidence by demonstrating that IPv6 is available now and ready to be used.”

The program is managed by the IPv6 Ready Logo Committee, which is composed of representatives from vendors, service providers, academic institutions, IPv6 organisations, and others. As explained on the program’s [website](http://labs.apnic.net/measureipv6/):

*The IPv6-Ready Logo Committee’s mission is to define the test specifications for IPv6 conformance and interoperability testing, to provide access to self-test tools, and to deliver the IPv6-Ready Logo. The key objectives and benefits of the IPv6-Ready Logo Program are to:

- Verify protocol implementation and validate interoperability of IPv6 products
- Provide access to free self-testing tools
- Provide IPv6-Ready Logo testing laboratories across the globe dedicated to provid[ing] testing assistance or services*

### 8. Tracking success: Measurements

One possible future work area for the BPF on IPv6 Adoption is to examine the role of IPv6 measurements. In future work, measurements should be able to help us to track the relative success of different best practices on IPv6 adoption. Measurements can also be used to raise awareness about IPv6 adoption, including for key decision makers, when discussing IPv6 policies.

**APNIC** has done extensive work on measuring IPv6. The aim of its measurement activities “is to conduct a broad-based long term measurement of the level of uptake of IPv6 across the Internet.” APNIC’s website visualizes the data it collects, so that visitors to the website can

---

113 Email correspondence, Yannick Pouffary, IPv6 Forum, United States.
see IPv6 deployment rates on a country-by-country basis. Google also does something similar, tracking the IPv6 activity of its users on a worldwide basis.\textsuperscript{115}

For readers who are interested in knowing more about IPv6 measurement activities, one important resource mentioned during the BPF was the AMC’s Internet Measurement Conference. This annual event focuses on Internet measurement and analysis. “The aim is that papers presented at the conference contribute to the current understanding of how to collect or analyze Internet measurements, or give insight into how the Internet behaves.”\textsuperscript{116}

9. Conclusion <to be completed following the IGF2015>

10. Appendices

10.1. A: Best Practices Survey

The Best Practice Survey was launched to collect examples of practices that help to create an enabling environment for IPv6 adoption. The survey was launched mid July 2015 and was open to all via a link posted on the IGF website.

The survey remains open during the public review period and the IGF meeting. An overview of the survey responses will be added to the final outcome document. An interim survey report is available on the IGF website.

Click here to share your experiences and best practice examples by filling in the survey.

Closing date: 14 November 2015.

10.2 B: Non-Exhaustive list of IPv6 Task Forces

This non-exhaustive list of IPv6 Task Forces was compiled based on the input received during the BPF. Additional IPv6 Task Forces can be posted as comment on the review platform or submitted via the survey.

Table: Non-Exhaustive list of IPv6 Task Forces


\textsuperscript{116} See the website of ACM Sigcomm, available at: http://www.sigcomm.org/events/imc-conference.
<table>
<thead>
<tr>
<th>Organization</th>
<th>State / Country / Industry / Region</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIIPv6TF</td>
<td>Asia-Pacific</td>
<td><a href="http://www.ap-ipv6tf.org">http://www.ap-ipv6tf.org</a></td>
</tr>
<tr>
<td>IPv6 Council</td>
<td>Belgium</td>
<td><a href="http://www.ipv6council.be/">http://www.ipv6council.be/</a></td>
</tr>
<tr>
<td>IPv6 Canada</td>
<td>Canada</td>
<td><a href="http://www.ipv6canada.ca/">http://www.ipv6canada.ca/</a></td>
</tr>
<tr>
<td>IPv6 Forum</td>
<td>Chad</td>
<td><a href="https://www.facebook.com/pages/IPV6-FORUM-CHAD/34144490609204">https://www.facebook.com/pages/IPV6-FORUM-CHAD/34144490609204</a></td>
</tr>
<tr>
<td>ID-IPv6TF</td>
<td>Indonesia</td>
<td></td>
</tr>
<tr>
<td>LACTF</td>
<td>Latin America and the Caribbean</td>
<td><a href="https://mail.lacnic.net/mailman/listinfo/lactf">https://mail.lacnic.net/mailman/listinfo/lactf</a></td>
</tr>
<tr>
<td>North America IPv6 Task Force*</td>
<td>North America (Canada, US, Mexico)</td>
<td><a href="http://www.nav6tf.org/">http://www.nav6tf.org/</a></td>
</tr>
<tr>
<td>IPv6 Forum</td>
<td>Thailand</td>
<td><a href="http://www.thailandipv6.net/">http://www.thailandipv6.net/</a></td>
</tr>
<tr>
<td>IPv6 Task Force</td>
<td>The Netherlands</td>
<td><a href="http://new.ipv6-taskforce.nl">http://new.ipv6-taskforce.nl</a></td>
</tr>
<tr>
<td>IPv6 Council</td>
<td>United Kingdom</td>
<td><a href="http://www.ipv6.org.uk/">http://www.ipv6.org.uk/</a></td>
</tr>
<tr>
<td>CAV6TF</td>
<td>USA - California</td>
<td><a href="http://ca6tf.org/">http://ca6tf.org/</a></td>
</tr>
<tr>
<td>Rocky Mountain IPv6 Task Force</td>
<td>USA - Colorado, etc.</td>
<td><a href="http://www.rmv6tf.org/">http://www.rmv6tf.org/</a></td>
</tr>
<tr>
<td>IPv6 Task Force Hawai’i</td>
<td>USA - Hawaii</td>
<td><a href="http://ipv6hawaii.org/">http://ipv6hawaii.org/</a></td>
</tr>
<tr>
<td>MidAtlantic IPv6 Task Force</td>
<td>USA - New York, Pennsylvania, Delaware, New Jersey, Maryland, Washington, DC</td>
<td><a href="http://midatlanticv6tf.org/">http://midatlanticv6tf.org/</a></td>
</tr>
<tr>
<td>TXv6TF</td>
<td>USA - Texas</td>
<td><a href="http://www.txv6tf.org/">http://www.txv6tf.org/</a></td>
</tr>
</tbody>
</table>

** Task Force decommissioned