IPV6 IS HERE

KEY CONSIDERATIONS FOR DEVELOPING AND IMPLEMENTING A PHASED MIGRATION STRATEGY

NTT Communications | NTT America

AN NTT COMMUNICATIONS WHITE PAPER
APRIL 2012

Executive Summary

In February of 2011, the last remaining block of IPv4 addresses was assigned, sending a warning signal to the industry: No longer could it ignore the coming of IPv6.

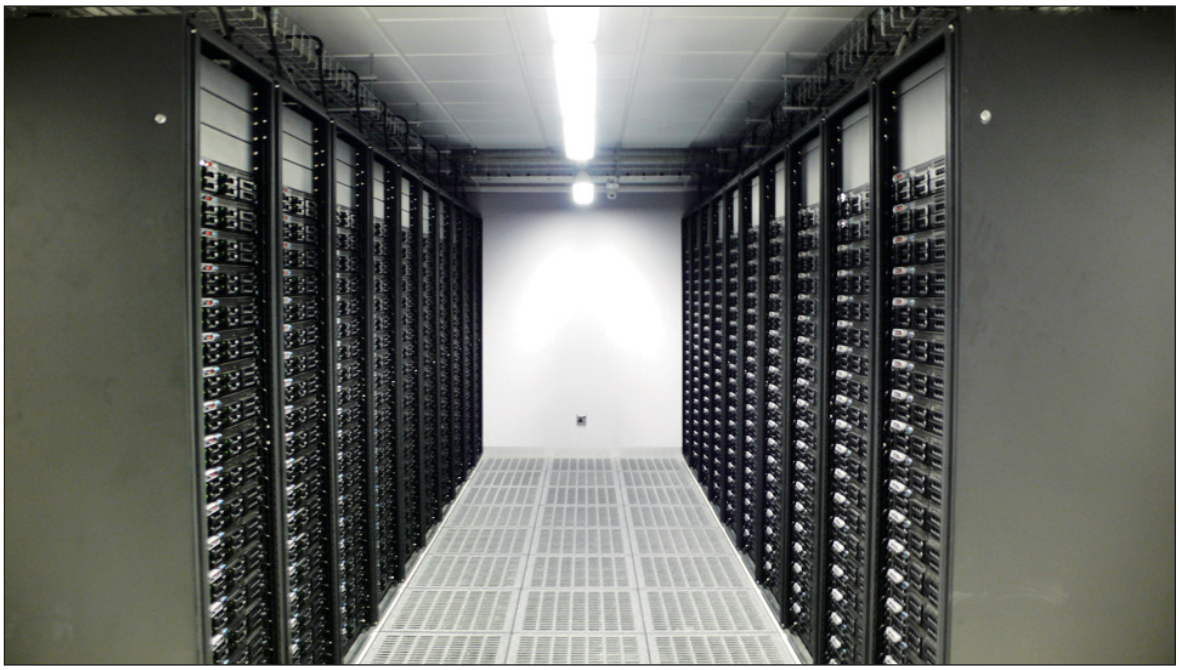
The market is ready and the infrastructure is in place. In fact, NTT America has been offering IPv6 native and dual stack services in North America since 2003 and globally since 2004. So why aren't more service providers and content networks transitioned to IPv6? For many, it's an issue of urgency. Why transition now if there's no need?

Today, enterprises, ISPs and content providers run the risk of disrupting their seamless business processes if they delay or avoid planning for migrating to IPv6 because, at a fundamental level, IPv4 and IPv6 are not compatible. And hurried, ill-planned implementations can and will likely result in business delays, negative effects on the end-user and, potentially, significant cost.

The following white paper outlines five key guidelines for creating a successful IPv6 migration strategy:

1. Save money by migrating to IPv6 now
2. Conduct an inventory of your existing network
3. Develop a technical strategy
4. Avoid NATs and tunnel infrastructure
5. Make an educated decision when choosing your service provider

Companies, service providers and content networks that integrate these considerations into their migration strategy will ultimately benefit from a smoother transition.



Yesterday's IP Can't Support Today's Demands

The business world was radically different in 1981, when the Internet Protocol version 4 (IPv4) was designed. At the time, no one envisioned the exponential growth the Internet would experience in the following decades. Today, we live in a wireless, always-on, continuously connected broadband world and have more than one Internet-connected device to facilitate it. The incredible proliferation of users and devices currently on the Internet has created a situation where IPv4 addresses are now almost completely exhausted.

In fact, the Internet Assigned Numbers Authority (IANA), which controls the global IP address pools and delegates address space to the Regional Internet Registries (RIR), released its final block of free IPv4 addresses nearly a year ago. While most RIRs still have some address space to offer end networks, their pools are dwindling. The situation is most critical in Asia where the Asia Pacific Network Information Center (APNIC) recently became the first RIR to completely deplete its pool of IPv4 addresses. According to APNIC, new companies are at most risk because remaining address space is held by incumbent network operators. In short, anyone starting a new data center, web hosting or Internet access company with the intent of using IPv4 could be in trouble.

IPv6: The New Standard

The Internet Engineering Task Force (IETF) recognized the impending exhaustion of IPv4 addresses early on and created the new protocol, IPv6, as a safeguard.

IPv6 uses 128 bits for an IP address, versus the 32 bits used by IPv4. This allows IPv6 to offer an abundance of new addresses – 340 trillion trillion trillion – a number that has been termed as "almost approaching infinity." As a result, IPv6 has the capability to support an enormous number of users and devices on the Internet to manage their needs today and long into the future.

In addition, IPv6 has a number of other benefits such as Stateless Address Auto-configuration, which simplifies address assignments for a host when connected to an IPv6 network, and improved security features with Internet Protocol Security (IPsec) built directly into the IPv6 protocol.

In 2010, the major backbone network providers began to widely deploy native IPv6 and ready their systems. In 2011, many content providers began migrating their networks and most large providers are now able to deliver content over IPv6. For example, both Google/YouTube and Netflix have made content available via IPv6. In 2012, some of the large Internet Service Providers (ISPs) or "eyeball networks" will begin moving to IPv6 and the stage will be set for more rapid customer migration. In fact, some industry experts anticipate IPv6-only content may appear as early as next year.

The incredible proliferation of users and devices currently on the Internet has created a situation where IPv4 addresses are now almost completely exhausted.

Making the Move Now

Many organizations are now actively developing strategies for IPv6 implementation and moving toward migration. Yet, even if they are not ready to make the shift to IPv6 today, it is important to develop a comprehensive strategy now and purchase the appropriate technology as part of the natural acquisition cycle. This approach will enable businesses to avoid making all the necessary IPv6 equipment purchases at one time in the future, resulting in a large capital expenditure. And because available IPv4

addresses are becoming increasingly scarce overseas, businesses that aren't IPv6 enabled also risk running into major roadblocks when trying to expand globally, potentially resulting in major lost revenue.

Additionally, an unintended consequence of the dwindling number of IPv4 addresses is the creation of a "secondary market" for selling existing addresses under the earlier protocol. Already, leading industry vendors are purchasing blocks of IP addresses from other vendors at a premium. As fewer addresses are available, the cost of once-free IPv4 addresses will skyrocket, dramatically increasing costs for those who were slow to migrate to IPv6.

If there is any doubt, the time is now for companies to plan a move to IPv6. The landscape is set and the industry is at the midpoint of this widespread migration. Below are five guidelines to consider as part of a successful IPv6 migration.

Guideline No. 1 – Save Money by Migrating to IPv6 Now

Experts believe the industry is at the tipping point for widespread IPv6 adoption – the point in time when companies and ISPs are all migrating at once. Since IPv6 does not interoperate with IPv4, users that remain on the older protocol will be unable to access the new content. When this happens, organizations that are not IPv6-enabled will be scrambling to upgrade their networks.

A major advantage for moving to IPv6 now is that the process will be simpler and the project will be less expensive than waiting until the final hour. The cost of adopting new technologies goes up when businesses wait until there is major demand for equipment and services, and they hurriedly execute on a migration plan to meet tight deadlines.
Both hardware and software technologies have come a long way in terms of IPv6 compatibility in recent years. There are few additional IPv6 functionality enhancements for networks on the horizon, so there is no real benefit in waiting for new technologies.

As fewer addresses are available, the cost of once-free IPv4 addresses will skyrocket, dramatically increasing costs for those who were slow to migrate to IPv6.

As a first step in the process, all relevant stakeholders across the organization should understand the critical nature of an upgrade to IPv6. Once there is consensus that migrating to IPv6 is a technology priority, a timeline should be developed, appropriate budget allocated and a qualified team identified to execute the upgrade.

Guideline No. 2 – Conduct an Inventory of the Existing Network

Hardware and software vendors alike have been anticipating the move to IPv6 for some time, so most network hardware and operating systems purchased in the last few years are already IPv6-enabled. For example, Microsoft has included IPv6 functionality in its operating systems since Windows XP, so all subsequent versions, including Windows Vista and Windows 7, already support IPv6 networks.

Other popular operating systems are also IPv6 compatible, including Apple OSX, many flavors of Unix and Linux, and Sun Solaris. The situation is the same regarding network hardware, as most is IPv6-enabled today. In many cases, routers purchased in the last four years will also support IPv6.

Organizations should begin by developing a checklist of all the elements in their network that will need to be IPv6-enabled. Almost all IPv6 networks in the next few years will be "dual stack," meaning IPv4 and IPv6 will be running alongside one another. Depending upon underlying hardware, this dual-stack approach

may not require much capital investment since the equipment will already be in place. When businesses are in the situation of evaluating new network and security solutions, they should select equipment that can process IPv6 packets at the same rate as IPv4 to maximize performance of their network in the future.

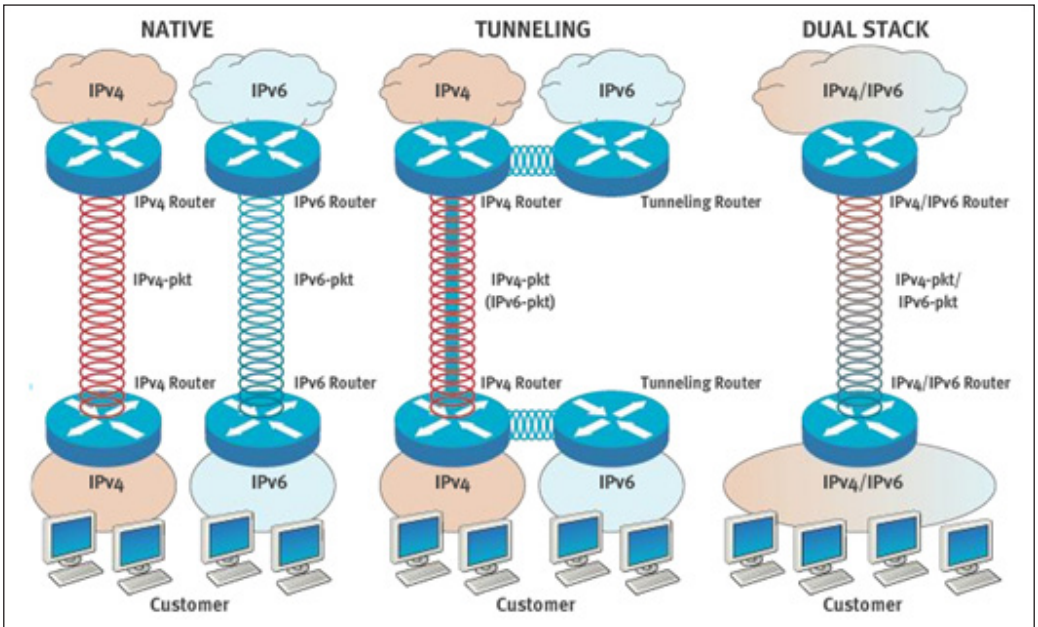
Guideline No. 3 – Develop a Technical Strategy

Once an inventory is completed, the organization should identify areas where work will be required to ensure their network is fully enabled for IPv6 and develop a work stream for accomplishing the migration. Operational costs will comprise the majority of the expenses, since much of the hardware is likely already in place. This includes doing the actual work to touch every part of the network, as much of this complexity of upgrading is at the end-user level – upgrading every desktop and client on the network.

Enterprises that are not Internet-centric will have different considerations in their migration path to IPv6 than retail ISPs. While most back-end technologies are IPv6-enabled, an exception is firewall applications in the enterprise, which have been slower to reach IPv6 parity with IPv4. In these cases, IT managers are required to upgrade security software to fully enable their networks.

In addition, IPv6 adoption can create a complex environment for addressing end users with a variety of network protocols. For example, IPv6 has an automated method for distributing addresses to end users called neighbor discovery (ND).
However, ND does not perform all the functions available with the Dynamic Host Configuration Protocol (DHCP), an automatic configuration tool that allows a server to automatically assign an IP address to a computer. As a result, a new protocol was developed called DHCPv6. Because this latter protocol is quite new, it is only available in the most recent operating systems.

Retail ISPs, such as multiple system operators (MSOs) and digital subscriber line (DSL) providers, will need to determine how to deliver IPv6 all the way to the end user. Providing a dual stack IPv4 and IPv6 network to each individual household is exponentially more difficult than



IPv6 can be run natively, through tunneling and via a dual-stack infrastructure. However, tunneling can present challenges in connectivity and speed and therefore is not an ideal solution.

NTT America provides global IPv6 capabilities via the NTT Communications Global IP Network.

providing the same network on the backbone because there is much more equipment to be upgraded.

In many cases, retail ISPs will need to determine if a tunneling infrastructure is a viable option, as this approach can bring unnecessary challenges and complexity into the system. In addition, ISPs need to be cognizant of operating systems, such as Windows XP, that are IPv6 compliant but need that functionality to be explicitly enabled on each client. This results in more work for an ISP than an enterprise where an IT manager would have control over all end user systems.

Guideline No. 4 – Avoid NATs and Tunnel Infrastructure

Establishing a dual-stack IPv4 and IPv6 network now means businesses can eliminate their investment in costly equipment needed to manage large-scale network address translation protocols (NATs). NATs are designed to obfuscate the IP addresses of end hosts to conserve address space in a process called overloading. Using NATs, a network can use a single IP address to serve many end users.

There are two NATs that are commonly used to avoid an IPv6 upgrade: NAT44 and NAT64. NAT44 allows many IPv4 end users to hide behind a single IPv4 address. This approach can help stave off IPv6 deployment by allowing networks to continue using limited IPv4 resources for a longer period of time. NAT64 is similar to NAT44, except it uses one IPv4 address to represent many IPv6 addresses. This can be done either to deliver IPv4-only content to IPv6-only users or vice-versa.

Both NAT44 and NAT64 present a high level of complexity for network managers who are responsible for maintaining NAT hardware and software. In addition, NATs introduce a new potential point of failure in the network because they are another component added to the network topology. NATs are known to be particularly fickle with the reliability of certain critical protocols such as VoIP, for example. In many cases, Application Layer Gateways (ALG) are developed and deployed to address NAT-averse protocols function that increase cost and complexity in the network even further.

NAT444, or a Carrier Grade NAT, is a common approach to IPv4 network design by service providers for traffic that has already been translated to an IPv4 address by the end-user. In most cases, the user will have a residential router that acts as a gateway between themselves and the ISP. Traffic from a user's computer is translated once by a personal router and then translated to another IPv4 address again by the ISP before sending it on to the Internet. NAT444 creates problems when a user sends traffic to another user because the traffic is required to go through the NAT device to be translated to an IPv4 address and then go

back through the same device to the customer's public IP address. In some cases, a customer's traffic would pass through three different IPv4 addressing domains using NAT44.

One temptation for businesses is to adopt IPv6 externally to manage IPv6-only content on the Internet, but continue on IPv4 internally within their organization. This is a suboptimal situation because it still requires the maintenance of complex technologies on the network. In particular, this creates problematic extranet scenarios. As companies work more and more in an online capacity with partners and customers, extranets will continue to gain popularity and see additional traffic, which will result in even more NATs for networks that still use IPv4. The best approach is to develop a native IPv6 network both internally and externally.

Another measure that is commonly used to avoid IPv6 deployment is tunneling. Networks use tunneling protocols to carry certain IP traffic within other IP traffic. This allows customer to carry IPv6 protocols over an incompatible IPv4 network. Tunnels are problematic because they result in a reduction in the Maximum Transmission Unit (MTU), or the largest packet that can be sent at one time. In addition, a reduced MTU can break connectivity when communicating with hosts that do not support Path MTU Discovery. Generally, the MTU on the

OUR IPV6 SERVICE HISTORY

1996: NTT Communications' labs start one of the world's largest global IPv6 research networks

1998: Verio begins participation in PAIX native IPv6 IX

1999: NTT Communications begins IPv6 tunneling trial for Japanese customers

2000: Verio obtains IPv6 sTLA from ARIN

2001: NTT Communications pioneers the world's first IPv6 connectivity services on a commercial basis

2002: World Communications Awards (WCA) gives NTT Communications the "Best Technology Foresight" award for its IPv6 global products

2003: NTT/Verio launches IPv6 Native, Tunneling, and Dual Stack commercial service in North America

2003: Communications Solutions magazine names NTT/Verio IPv6 Gateway Services "Product of the Year"

2004: NTT Communications' IPv6 Native and Dual Stack services become available around the globe

2004: NTT Communications wins the World Communications Awards "Best New Service" award for IPv6/IPv4 Global Dual Service

2005: Dual stack Virtual Private Server released, making NTT Communications the first ISP to offer an IPv6 Managed Firewall service

2006: NTT Communications launches the IPv6 Transition Consultancy

2007: NTT Communications is awarded GSA Schedule 70 contract for IPv6 IP transit

2008: NTT America demos IPv6 at ICAC at U.S. Senate

2008: IDC names NTT America Top 20 IPv6 Influencer working with the U.S. Government

2008: NTT Communications named Best Wholesale Carrier at the Telecom Asia Awards for its Global IP Network Service incorporating IPv6 and advanced security technologies

2008: European Commission invites NTT America to speak at European IPv6 Day

2009: NTT America demos IPTV over IPv6 at ICAC at U.S. Senate

2011: NTT America participates in World IPv6 Day sponsored and organized by ISOC to demonstrate readiness for the transition to IPv6

Internet today is 1500 bytes; however, a "tunnel overhead" can dramatically reduce the size of permissible packets and increase lag time on the network.

Guideline No. 5 – Make an Educated Decision when Choosing Your Service Provider

Another critical step in the process of upgrading to IPv6 is choosing the right service provider for your backbone network. There are several providers on the market that offer IPv6 expertise for a global IPv6 network, so it can be a daunting task to determine which provider will best meet a customer's business needs.

Experience and a proven record are key factors to take into consideration. NTT America has been an IPv6 service provider since setting up the largest test lab of its kind in 1996. In 2001, the company launched its first IPv6 transit services and the first IPv6 managed firewall solution in 2005. In 2004, NTT America was one of the first providers to run a global network carrying native IPv6 traffic. Today, NTT America has the highest quality global Tier-1 backbone, offering its customers a fully redundant network backed by industry leading service level agreements (SLAs).

No provider has a longer record in offering commercial IPv6 than NTT America. In addition, the company is involved with some of the most advanced IPv6 projects worldwide. NTT America's IPv6 services enable businesses to run dual IPv4 and IPv6 stacks, allowing them to make the transition to IPv6 at their own pace. The company's award-winning IPv6 transit service provides unprecedented performance with no bottlenecks between network segments.

Ready, Set, Migrate

There is no way around it, IPv4 addresses are nearly depleted and IPv6 is the future of the Internet. Now that most backbone providers have fully upgraded their networks to IPv6, companies and ISPs are anticipated to begin migrating to IPv6 at an increasing rate. Content that is only accessible on IPv6 networks is on the horizon and once this happens the floodgates will open and the industry will experience a massive rush to IPv6.

Moving to IPv6 before this watershed moment is smart business that will allow enterprises and ISPs to save money and also ensure their migration goes smoothly. Experts agree, the time is now to start planning this essential move and develop a work stream for IPv6 migration throughout the organization. Unlike many other upgrades in the technology industry, IPv6 enablement shouldn't be considered an incremental value-add to a network. Rather, migrating to IPv6 should be approached as an imperative investment to basic network functionality to ensure businesses are prepared for the next era of computing.