Share this with your peers.

How Will IPv6 Impact your Network?

The transition to IPv6 protocol is officially under way. The global top-level repository of IPv4 addresses expired, and just a few quickly dwindling pools of addresses remain at the world's five regional Internet registries.

Going forward, your network will have to accommodate a growing population of IPv6-enabled devices: new equipment is shipping with IPv6 simply because there are so few unused IPv4 addresses left.

The American Registry for Internet Numbers (ARIN), one of the remaining registries suggests that all Internet servers be prepared to serve IPv6-only clients by January 2012. And in September 2010, the U.S. Obama administration issued a directive requiring all U.S. government agencies to upgrade their public-facing Web sites and services to support native IPv6 by September 30, 2012.

Start with the Internet

As these deadlines suggest, the first place that the IPv6 transition will affect your network is in the public Internet segment. You'll want to upgrade your Web-facing content and mail servers to IPv6 first so all users can access content on your Web site, regardless of which network protocol their devices support. Otherwise, there might be some mismatches and lack of interoperability between Web resources and users.

Newer IPv6-only mobile devices, for example, might not be able to locate IPv4 Web sites. Similarly, e-commerce sites that run only IPv4 or IPv6 (not both) might be unable to receive orders from user access devices running the protocol that the site doesn't support.

Dual Stack Interoperability Approach

Preparing equipment to "speak" either protocol involves using a standard dual-stack IP addressing approach to IP interoperability. Running this implementation in the operating system of network equipment, servers and client devices enables network infrastructure components to communicate with either IPv4 hosts or IPv6 hosts in their native language.

Fast Fact

In 1995, the Institute of Electrical and Electronic Engineers (IEEE) global standards body specified a whole new Internet Protocol, called IPv6, which adds several services to the protocol and lengthens the address space from 32 bits to 128 bits. The greater address space means there are many, many more possible combinations of bits, resulting in an almost an infinite number of IPv6 addresses.

Some newer industries may run only IPv6 from the start. Consider a utility company monitoring IP-enabled smart meters or a home-appliance company monitoring and servicing IP-enabled refrigerators, washers, dryers and other equipment over the network. These enterprises will probably need to communicate with these remote devices, machine to machine, using IPv6. That's because the forthcoming avalanche of IP-enabled smart home devices and sensors will be assigned only IPv6 addresses.

The transitional issues associated with enabling millions of existing IPv4-based devices to communicate with IPv6 Web sites and devices (and vice versa) mean that dual-stack IP addressing will need to be in place for a long time.

Another interoperability approach that can be deployed among components in the enterprise private WAN is tunneling. Tunneling is used in exceptional cases where running dual-stack IP software isn't feasible, such as on older equipment. It involves encapsulating IPv6 packets within IPv4 so that two islands of IPv6 can interconnect using an IPv4 network in the middle.

Figuring out what network elements are candidates for each type of transition requires a well-thought-out planning process (see figure on top of page 2).

at&t

Planning Process for IPv6

Program Governance and Communication

- Create IPv6 transition timelines, sequencing and interdependencies
- Identify governance team to oversee plan
- Develop review and program management aspects of overall plan, timelines and assigned transition teams
- Execute plan

Infrastructure Readiness

- Quantify infrastructure readiness and understand transition impacts
- Categorize Components for Readiness

Strategy and Architecture

- Research IPv6 technologies utilized for transition (tunnels, translation mechanisms)
- Develop IP Addressing Plan
- Develop a thorough transition strategy

Design and Engineering

- Develop detailed design and equipment configurations, including:
  — IP addressing
  — DNS
- Identify and assign transition sequencing and engineering tasks

Testing and Piloting

- Create IPv6 test labs
- Develop test plans and production piloting
- Conduct dual stack testing
- Tunneling

The Diminishing Role of Network Address Translation (NAT)

In the short term, your private WAN could see fewer effects of the transition to IPv6 if you currently use Network Address Translation (NAT) to conserve internal IPv4 addresses. But in general, NAT's days are numbered, both at the enterprise edge and particularly in service provider networks.

Enterprise NAT

IP identifies a network or client device by an address – either a globally unique one or a reusable one assigned temporarily from a pool of addresses from a Dynamic Host Control Protocol (DHCP) server. NAT is a longtime practice in IP networking to conserve IPv4 addresses and add a measure of security to private enterprise networks.

NAT aggregates multiple, non-exclusive IP addresses behind the corporate WAN router, but shows just one unique address on the router interface to the public Internet. In other words, multiple enterprises' private IP networks could be using the same IPv4 address ranges internally, but the NAT router facing the public Internet displays a unique IP address that is globally routable.

Typically, the local enterprise WAN edge IP router uses NAT to keep track of who's who behind the WAN edge and maps end points to one another accordingly. Once a "hidden" device behind the NAT-enabled router establishes a session, the NAT device keeps stateful information about the session and thus "remembers" who at the back end is connected to whom or what in the public Internet.

In this way, NAT has been the conservator of IP addresses that bought the industry many years of time before having to migrate to IPv6's longer addressing scheme. However, the hidden aspect of individual resource IP addresses will not survive long in the more peer-to-peer oriented architectures of private and public networks (see below) going forward.

Cloud-based NAT: A Temporary Fix

NAT can also be used in the service provider network in the form of Large Scale NAT, or LSN. LSN moves today's NAT mapping and translation functions from the edge of enterprise and home networks into the service provider's network, creating a "centralized NAT."

This effort involves the service provider doing what enterprises have been doing with NAT in their private networks but on a much larger scale: masking thousands of customers behind a single IPv4 address. The temporary benefit of this is that it stretches a service provider's public IPv4 address space and buys time before wholesale IPv6 upgrades must occur.

There are serious drawbacks to this approach, however. For example, identifying individual devices and users behind the NAT becomes quite difficult. That's because when using LSN, each address no longer represents a single machine, residence or office. That IPv4 address now represents thousands of machines and users belonging to multiple service provider customers behind the NAT-enabled routers. So it becomes quite challenging to continue to map sessions and track who's who, and some connections are likely to break.

For example, applications with "push" sessions – those that are initiated by another party and intended to reach a given user – aren't possible, because the subscriber is hidden behind an IPv4 address that makes his or her specific address unidentifiable. While on an enterprise scale a router can retain stateful information about the two ends of a session and map flows to the proper end points accordingly. This becomes quite complex – in fact, nearly impossible – when the service

Fast Fact

The main driver to the new IPv6 protocol is that the IPv4 address space is virtually depleted. But IPv6 also offers new services and characteristics:

- **Built-in support for IPsec encryption**
- **Autoconfiguration, enabling systems to gain a network address without administrator intervention**
- **More classes of service, so potentially higher quality of service (QoS) and improved service-level agreements (SLAs)**

provider has no routing knowledge of each customer's private, internal IP network.

In addition, some Web site owners and Internet service providers (ISPs) block access based on IP address because of bad behavior of a single machine, user or network. But if thousands of customers and devices are behind one IP address, blocking access from it could unjustifiably deny service to many other customers of that provider.

These are some of the reasons that LSN should be considered a transitional and temporary approach to implementing IPv6, rather than a substitute for it.

Ultimately, pushing IPv6 as close to end users as possible – within individual enterprises and residences – avoids the additional layers of mapping and conversion that take place going through at least one large-scale layer of NAT and possibly another at the enterprise edge. Those conversions slow down performance and can break connections.

Benefits, Cautions with IPv6 Internet Connections

Direct IPv6 connections to the Internet bring both benefits and new challenges. For example, direct connections could actually improve peer-to-peer communications, such as voice over IP (VoIP). On the other hand, they introduce some new security risks.

VoIP Could Get Easier

An inherent benefit of IPv6 is that it delivers on the true intent of an IP network, namely bi-directional communication where end-point addresses are known by both parties. The arrival of IPv6 should eventually enhance VoIP when NAT functions disappear from the picture. Today, NAT makes it impossible to set up Session Initiation Protocol (SIP)-based calls to devices with private IP addresses unless the initiating VoIP device finds a way to bypass a firewall to get inside and find an intended recipient's IP address in the company's server.

Because VoIP sessions are inherently peer-to-peer in nature, this could be a reason to prioritize opening up the internal SIP service with a globally unique IPv6 address first, particularly if you are planning to eventually move away from NAT. Getting rid of NAT, inevitable though it may be, has implications for your security infrastructure.

Security/VPN Impact

When NAT ultimately disappears from the edge of the enterprise network, individual IPv6 addresses will be exposed directly to the public Internet. IPv6 does require support for IPsec as a fundamental interoperability requirement, indicating that it will be inherently more secure than IPv4. In other words, an IPsec VPN is built directly into the IPv6 network.

If you are an enterprise using a Multi-Protocol Label Switching (MPLS VPN) service, there should be no effect of IPv6 joining the network given that MPLS is a different protocol altogether. Whether you are running IPv4 or IPv6, the protocol will be encapsulated in an MPLS "wrapper."

Service providers, on the other hand, need to support IPv6 in the routers at the edge of their networks (the provider edge, or PE, routers) in the form of dual-stack IPv4/IPv6.

Note, though, that because IPv6 isn't backward compatible with IPv4, you'll need to upgrade some existing security tools to speak IPv6, basically recreating the security infrastructure you have in place for your IPv4 networks for the newer version of the protocol.

According to the National Institute of Standards and Technology (NIST):

> Prevention of unauthorized access to IPv6 networks will likely be more difficult in the early years of IPv6 deployments. IPv6 adds more components to be filtered than IPv4, such as extension headers, multicast addressing, and increased use of ICMP. These extended capabilities of IPv6, as well as the possibility of an IPv6 host having a number of global IPv6 addresses, potentially provides an environment that will make network-level access easier for attackers due to improper deployment of IPv6 access controls. Moreover, security related tools and accepted best practices have been slow to accommodate IPv6. Either these items do not exist or have not been stress tested in an IPv6 environment. Nevertheless, global aggregation of IPv6 addresses by ISPs should allow enhanced anti-spoofing filtering across the Internet where implemented[1].

Transition to IPv6 Summary: 5 Steps

When you move away from NAT, you'll need to support IPv6 on your internal network. For that to happen, you'll need a comprehensive strategy and detailed planning process that enables you to migrate using the following steps:

1. Establish an IPv6 Internet presence.
This involves adding IPv6 to your public servers. First, enable your public-facing Web and email servers with an IPv6 address in addition to their IPv4 addresses. This makes more resources available via IPv6 for everyone.

2. Enable internal users to access IPv6-enabled sites on the Internet.
This involves upgrading their operating systems to dual-stack addresses, if it hasn't already happened automatically by your OS system provider.

3. Migrate your WAN to dual stack (supporting both IPv4 and IPv6 protocols) by upgrading your WAN access routers.
This allows your private enterprise network to interoperate with newer networks and resources that support only IPv6 due to lack of IPv4 addresses.

4. Determine select priority migration candidates from there.
Consider whether you want to migrate any piece of your internal network out to the public IPv6 network – in other words, are there devices or subnetworks that could interface directly to the Internet? As mentioned, your VoIP and unified communications environment might be an early candidate, because of the peer-to-peer nature of it. As you introduce IPv6, remember that your DHCP servers will need an upgrade so they can assign IPv6 addresses.

5. Plan ahead for the long term

Over the long haul, you should plan to migrate your entire network to IPv6 and phase out NAT entirely. The main reason is simply that everything will need to be IPv6 sooner or later. Also, the mix of devices and connections likely to join your network, such as Wi-Fi-enabled smart phones and consumer-grade devices phones and tablets tend to change frequently, making it difficult for NAT to keep track of them and the state of their sessions.

Consider, too, that other machines that might one day connect to your IP network: soda machines, thermostats, surveillance cameras and other facilities aspects of the building, for example. Again, if you have NAT in place, getting to these individual devices becomes complex if NAT has to have some way to identify all of them and map application flows accordingly.

Notes

1. Guidelines for the Secure Deployment of IPv6 (Draft): Recommendations of the National Institute of Standards and Technology, February 2010.

Share this with your peers.

05/04/12 AB-2234

at&t