APRIL 2010

ePapers

NTCA

4121 Wilson Boulevard
10th Floor
Arlington, Virginia 22203
Phone/703-351-2000
Fax/703-351-2001
www.ntca.org

NATIONAL TELECOMMUNICATIONS COOPERATIVE ASSOCIATION

IPv6: WHERE ARE WE NOW?

by Jesse Ward, Telecommunications Industry Analyst, NTCA

In the mid-1990s, the architects at the Internet Engineering Task Force (IETF) foresaw a need for a next-generation standard and embarked on a journey to improve the Internet protocol, the Internet's foundation.

Nearly a decade after Internet protocol version 6 (IPv6) was finalized, the networking industry has yet to embrace the new standard. Instead, the industry has engaged in a debate concerning the benefits of our current standard, Internet protocol version 4 (IPv4), and the technological and business advantages for upgrading.

On January 19, 2010, the Number Resource Organization added fuel to the fire, announcing that more than 90% of IPv4 addresses have been allocated. Most experts agree that the crop of IPv4 address will run out by 2012, if not before.

Although the exact timing can be debated, the solution is clear; in order to ensure that the Internet continues to function and grow from a content and user perspective, the network must be upgraded to run on IPv6.

At this critical juncture, let's examine what IPv6 can offer, what transition methods are available, and how the next-gen standard will impact the rural Internet service provider (ISP) marketplace.

How IP Works

In 2001, Dave Lowe authored an introductory ePaper on IPv6, at the time a relatively new standard.

To recap, the Internet protocol suite is the set of communications rules which govern communication between computers across the Internet and other similar networks. Without these rules, the Internet could not function properly. The communications suite is commonly known as TCP/IP, named for two of the most important protocols in it: the transmission control protocol (TCP) and the Internet protocol (IP).

> “Most experts agree that the crop of IPv4 address will run out by 2012, if not before.”

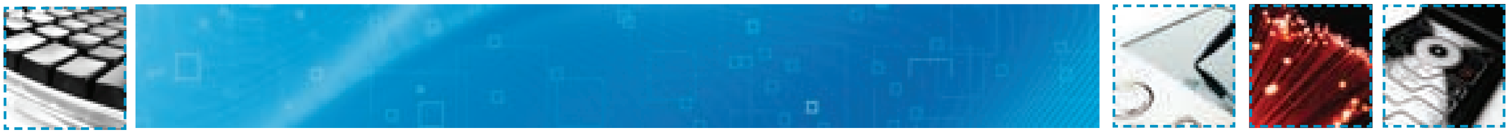
When information is sent over the Internet, the message is divided into small segments called packets. Each packet contains the sender's Internet or IP address, the receiver's IP address and the data to be sent. Routers along the Internet read the destination address contained in each packet and forward the packet to the next logical router, until the destination router recognizes the packet as belonging to the receiving computer/server found within its immediate network or domain.

Each packet carries only part of the message, traveling independently of all other packets, and can take different paths or routes along the Internet to reach the receiving computer. Consequently, packets may arrive in a different order than which they were sent.

The rules governing the delivery of packets are known as IP. TCP helps to reassemble packets at the receiving computer in the same order they were sent. TCP also provides important management functions, detecting problems with the transmission.

IPv4

IPv4 is forth generation of IP, and also the first version of the protocol to be widely deployed across the Internet and in use today. In order to accommodate a large number of hosts but not waste too much space in the packet overhead, the developers of IPv4 designed the protocol to use



32-bit addresses, and, as a result, it can support around 4 billion IP addresses.

Although this sounds like a large pool, it's quickly being exhausted. In order to transmit and receive data on the Internet, every device must have an IP address. As smartphones, gaming consoles, and WiFi-enabled devices such as a cameras, home alarm systems and even refrigerators become commonplace, the pool of unallocated IPv4 addresses is quickly dwindling.

IPv6

Designed as an upgrade, IPv6 uses a 128-bit addressing scheme and can support many, many billions of IP addresses—2 to the 128th power, or roughly 34 followed by 37 zeros.

When we talk about making the switch to IPv6, typically the discussion revolves around the available address space, often perceived as the one significant reason to upgrade. According to the Internet Society (ISOC)—the organizational home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB)—the main advantage of IPv6 is that it provides a much larger address space. ISOC also maintains that as a more recent protocol, IPv6 has a few design improvements over IPv4, particularly in the areas of auto configuration, extensibility, security, mobility and expanded routing. These features will be touched upon in the next few sections.

Auto Configuration

In an IPv4 world, every Internet-enabled device must be assigned a unique IP address, either by manual configuration, an error-prone and time-consuming task, or, more commonly, by using dynamic host configuration protocol (DHCP). In DHCP a client sends a broadcast request for configuration information. The DHCP server receives the request and responds with information from its database.

In an IPv6 world, DHCP is not necessary. Instead, a device can auto configure its own IP address. There is a mechanism whereby routers disseminate router advertisements that contain the upper 64 bits of an IPv6 address. The host combines this prefix information with either its physical, media access control (MAC) address (a unique identifier assigned to network interface cards by the manufacturer), or a private, random number, to generate the lower 64 bits itself and create a valid, unique IP address.

Looking toward the future, as more residential devices become Internet-enabled, auto configuration will save valuable time and expense.

Extensibility

IPv6 header has been designed in a way to speed up the routing process. In comparison with IPv4, the packet header is much simpler, with a fixed length of 40 bytes. Rarely used fields have been relocated to separate add-on or extension headers, which are only inserted into the packet header if they are needed.

There is a basic set of six extension headers, and the protocol allows for additional extensions without altering the basic header. Extensions may include quality of service (QoS), mobile IPv6 and security options such as IPsec. QoS is of course important for real-time applications such as video and voice.

The simplifications to the packet header enable routers to process and forward packets faster and more efficiently, improving overall network performance.

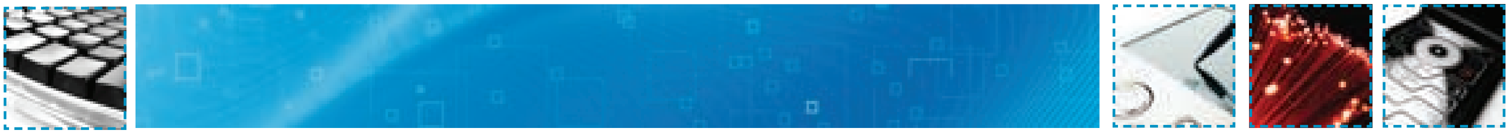
Security

IPsec is a protocol suite for securing end-to-end communications. It authenticates and encrypts each individual packet of a data stream, and can be used to protect all types of application traffic across the Internet.

IPsec support is mandatory in IPv6; this is unlike IPv4 where it is optional, but usually implemented. Most experts agree that including mandatory support for IPsec in the base specifications for IPv6 is an improvement, but the mere presence of IPsec does not mean that IPv6 is more secure than its predecessor.

Mobility

IPv6 was developed with mobile computing in mind. The auto configuration fea-



ture native to IPv6 assists with network and device mobility.

In an IPV4 world, relocating a subnet (a small division of the network) to a new router connection point is a significant undertaking. The network administrator must re-number the IP addresses of each displaced host. In an IPv6 world, subnets can be relocated with a minimal amount of administrative effort. The network admin simply changes a few router prefixes, and then each host configures its own IP address. The auto configuration feature of IPv6 also allows for easy connection of a handheld device when moving to or roaming on a foreign network.

The mobile IPv6 standard employed by mobile devices avoids the triangular routing trap. In triangular routing, packets that are sent to a mobile device (a.k.a. node) are first routed to the mobile node's home subnet and then forwarded to the device at its current location. However, packets that are sent from the mobile node are not handled in this way, but are instead sent straight to their final destination.

This may lead to problems as the source address of the packet will be the home address of the mobile node, not the care-of address assigned to the device on its guest network. Unlike mobile IPv4, mobile IPv6 avoids this triangular routing downfall, and is more efficient than its mobile IPv4 predecessor.

Expanded Routing

IPv6 has expanded routing capabilities which assist with the efficient delivery of packets and save valuable network resources in the process. IPv6 specifies several types of addresses assigned to a network device or host, including unicast, anycast and multicast.

> “IPv6 has expanded routing capabilities which assist with the efficient delivery of packets and save valuable network resources in the process.”

A unicast address identifies a single network interface, and is used when two hosts communicate directly with one another. Unicast addressing is common in all IP standards.

Anycast refers to addressing from one host to the nearest of multiple hosts. The advantage is that any of the recipients can forward the packets to other hosts, thus speeding the transmission. Anycast addressing is unique to IPv6.

Multicast is a group address. Oftentimes it's more efficient to send a message to a group, versus tying up network resources broadcasting the message. Multicast is part of the base specifications of IPv6; in IPv4 multicast is optional, although often implemented. Multicast addresses are useful when several hosts simultaneously need to receive the same information, such as live video broadcasts.

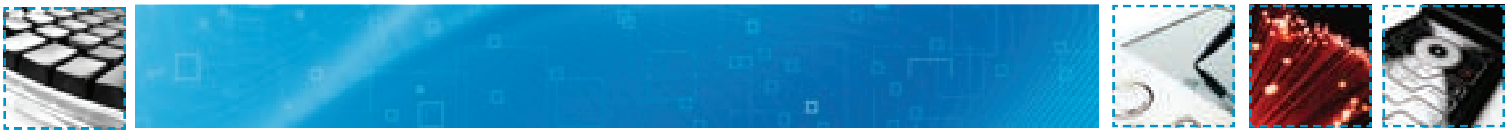
Each of these address types also has a scope, which specifies in what part of the network it is valid and unique. The scope can be limited to the node, link, site or global network.

Node-local addresses are valid only on the local node. An example is a loopback address contained in packet communiqués.

Link-local addresses are used to communicate over a single physical or logical network. Their function is for internal housekeeping reasons.

Site-local addresses are private addresses used only within the local network. Site-local addresses are the IPv6 equivalent of RFC 1918 private addresses in an IPv4 world, such as 192.168.0.0, 172.16.0.0 and 10.0.0.0. These are the primary addresses which have enabled network address translation (NAT) to function. (NAT is discussed in the next section.) Site local addresses cause pain for the developers of applications, the designers of routers and network administrators. As a result, the IETF has deprecated their use, although this does not prevent their continued use until a replacement has been standardized and implemented.

Finally, a global unicast address provides a globally unique, public IP address. These are only a few of the special address types contained in the IPv6 specifications, designed to enhance the efficiency and speed of communication.



What about NAT?

Despite these advantages many IT professionals question the need for IPv6, and maintain that the only real, concrete business driver for upgrading to IPv6 is the lack of IPv4 addresses. This problem, they maintain, can be resolved by relying on tools which conserve public IP address, such as DHCP and NAT. The central and failing tenant of this argument is that despite widespread use of said conservation techniques, the Internet is still quickly running out of version 4 addresses. NAT also violates the basic design principle of IP end-to-end connectivity across the Internet, creating an additional level of complexity within an operator's network.

Despite these drawbacks, NAT has value to the version 6 transition process. With NAT a single, public IP address is shared between many private IPv4 address. NAT is traditionally implemented at the edge of the network, within the customer's router or firewall, where it translates between private IPv4 addresses within the customer network, and one or a few public addresses assigned by the network provider which interface with the Internet.

NAT has since migrated further inside the network. Large-scale or carrier-grade NAT (CGN) is implemented within the service provider's network. It also translates between private and public IPv4 addresses; the private side of the CGN faces the end-user. CGN enables service providers to conserve IPv4 addresses by assigning customers private address rather than public, globally unique IPv4 addresses. Although NAT cannot overcome IPv4 address exhaustion, CGN is often used alongside a variety of transition techniques, discussed below, to assist with a smooth transition between the standards.

Interoperability

Upgrading to IPv6 is an expensive and time consuming endeavor. Despite the advantages numerated above, most carriers and enterprises do not see a driving business advantage for a forklift overhaul to IPv6. Instead the Internet community—network providers, application and content providers, and device manufacturers—is undertaking a gradual transition to IPv6. The end-user also can migrate to IPv6 independently, without coordinating with his ISP. This creates a complex transition period where IPv4 and IPv6 hosts must interoperate with one another.

The Internet engineering community had intended to make IPv6 backwards compatible with IPv4, but leaders of the IETF admitted to Network World in March 2009 that the transition process is less than seamless. IPv6 developers did not foresee that some legacy devices and applications would never be upgraded to IPv6, and some Internet websites may not have enabled public IPv6 access. The IETF is working to standardize additional techniques to assist with the transition.

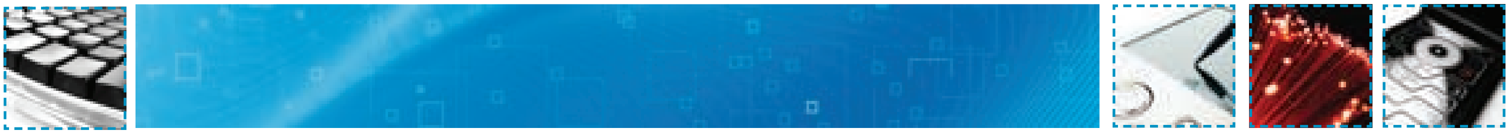
Currently, there are three main categories of transition techniques: dual-stack, tunneling and translation. Dual-stack techniques allow IPv4 and IPv6 to coexist in the same host. The system runs both IPv4 and IPv6 simultaneously, side-by-side, so it can access version 4 applications using its IPv4 stack, and version 6 applications using its IPv6 stack.

Dual-stacking is probably the easiest and most widely used transition technique, but it requires that the host have both a public IPv4 and a public IPv6 address. Further, in order for this method to single-handedly guide us through the transition, every host must be dual-stacked.

Tunneling was traditionally designed to support IPv6 traffic over legacy, IPv4 infrastructure. IPv6 packets are placed inside IPv4 packets, transmitted across the IPv4-only part of the network, and then the IPv4 portion is removed and the packets continue on their way over IPv6.

Comcast is championing a new transition technique called dual-stack lite, an extension of the tunneling concept. In dual-stack lite, IPv4 packets are encapsulated in IPv6 to traverse IPv6-only parts of the service provider network. At the consumer's premises, a home gateway must support the technique by encapsulating the packets. On the service provider end, a CGN decapsulates the packets, and enables many dual-stack lite clients to share a single IPv4 address. Tunneling techniques allows operators to incrementally deploy IPv6.

Translation, the third category of transition techniques, enables an IPv6-only host to communicate with an IPv4 host, or when a portion of the network can



IPv6 Presents New Security Issues

Unintended security wholes surface with any new standard. Here are two of the most important considerations for rural ISPs.

In an IPv4 network, NAT is almost always implemented to conserve public IP addresses. The device also acts as a simple (and perhaps unwanted) firewall, blocking incoming sessions. But in an IPv6 setting, where addresses are plentiful, NAT is not needed, and without its presence there is no automatic protection from outside applications initiating incoming sessions. It's important to educate your customers that a firewall is a necessary security practice; it will allow outgoing connections and return traffic, but bar incoming, unauthorized connections.

As noted in the Interoperability section, end-users can upgrade to IPv6 independently of one another, and without coordinating with their ISPs. Tunneling is a key transition method that may already be occurring over your network, allowing IPv6 packets to masquerade as IPv4. Tunneling also opens up key security vulnerabilities. If ISPs are not monitoring the pathway it may be used as an avenue of attack.

only carry one IP version. Some translators work at the NAT level, translating all packets of one version to packets of another version. Other translators are application level gateways (ALG) which only convert packets belonging to certain applications. The presence of translators creates bottlenecks, slowing down transmission. As such the other two types of transition technique often are preferred over translation methods.

Rural Telco Implications

The American Registry for Internet Numbers (ARIN) allocates blocks of IP addresses to Internet service providers within North America and parts of the Caribbean. In the case of small service providers, state-run fiber networks typically receive large blocks of IP addresses from ARIN, divide them up and distribute them to local telcos. In turn, the local network provider assigns IP addresses to end-users.

Iowa Network Services (INS) operates a statewide network which supports 147 independent telephone companies and cooperatives in Iowa, and acts as liaison between ARIN and its members. INS Planning Engineer Maury Malone has developed a plan to coordinate the version 6 transition effort with its member ISPs. INS is taking a phased approach which includes education, engineering and implementation.

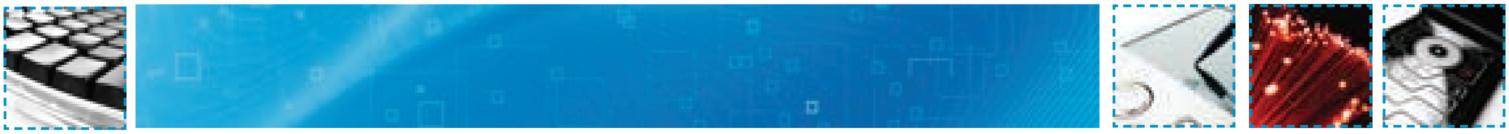
"Right now we making our members aware of the impending transition, and reviewing their current infrastructure to determine if its supports v6 connectivity," Malone said.

The availability of equipment is essential to the transition efforts. Malone acknowledged that not every device will need to be upgraded to support the new standard. For instance, Ethernet enables both v4 and v6. However, routers are a key component to the transition as they will need to support both standards.

INS is internally deploying IPv6 on its core network in order to gain vital knowledge and practice with the new standard. "In many ways it remains to be seen how this overlay of v6 traffic will affect our member's broadband subscriber access networks," Malone said. "This is where we need to acquire operational experience."

Wisconsin Independent Network LLC (WIN) Manager of Internet Operations Jon Kable is likewise engaged in the version 6 transition process for his state-run fiber network. Kable's year-end goal is to set-up a test network at each of its ISP member sites. One of the primary objectives is to test legacy consumer networking equipment, particularly modems and WiFi routers which often are not IPv6 compatible. Most modern computer operating systems are set up for dual-stack operation, but manufacturers of home networking equipment have not been as forward thinking. In order to access IPv6 content and services, the end-user must ensure that his home networking equipment and devices support the new standard.

Equally as important as coordinating downstream, state networks and rural ISPs need to orchestrate with upstream bandwidth providers. INS has approached its tier-one backbone providers. "Most of them have plans for a version 6 transition, and several have just begun to offer IPv6 end-to-end connectivity,"



Malone reported. “Unfortunately v6 is not deployed evenly across the tier-one networks; if the provider has native v6 support available, it’s in large metropolitan areas, as opposed to remote populations.” INS is looking to acquire a circuit to the next state in order to connect with a version 6 backbone.

One of the biggest issues with IPv6 is a chicken and an egg scenario, or, as Kable described it, “a dog chasing its tail.” It’s difficult to motivate consumers and network providers to transition to IPv6 without providers offering content in the new standard. According to Kable, there are greater than 300,000 entries in the IPv4 routing table, and, in comparison, less than 3,000 IPv6 entries. But this is quickly changing as a growing number of websites including eBay, Facebook, Google, NetFlix, Yahoo, YouTube, Microsoft and Wikipedia are adding IPv6 support. (Network World has more.)

WIN and INS both foresee a transition period where version 4 and version 6 content will be available. WIN is planning for a dual-stack transition, where customers will run both standards simultaneously. “IPv4 is not going away anytime soon,” Kable said. “End-users, particularly legacy version 4 users, will be able to access version 4 and version 6 content for many years to come. But until the content moves it’s not necessary to move our customers to dual-stack.”

Left unspoken is the notion that this is all a house of cards, predicated on the continued availability of version 4 addresses. Neither state-run network has encountered problems receiving IPv4 addresses, but both INS and WIN have observed ARIN tightening its policies, perhaps a nod to the finite version 4 resources.

Malone and Kable agree that the one compelling reason to transition to IPv6 lack is the lack of available address space in an IPv4 world. Once the transition has taken place, IPv6 will save valuable admin resources by streamlining address allocation. Kable explained that in an IPv6 world, an ISP can obtain more than 65,000 addresses at one time. This is in striking comparison to the current state of affairs where IPv4 addresses are in steep demand, and only assigned to ISPs and end-users sparingly. “Because of the lack of IPv4 addresses, WIN has set an internal policy, not to assign more than 510 addresses to any one segment at a time,” Kable said. “So if an ISP uses those up, we have to go back and re-assign more.” This is a time intensive task for all involved.

As additional hosts, network operators and content providers transition to IPv6, it’s important for network administrators to understand the next-generation standard, and embark on a transition plan. “It’s a matter of being prepared,” Kable said. “We didn’t want to wait until the thirteenth hour to make our transition plan. Version 6 is coming, perhaps sooner than later.”

Malone added that the best advice he can give to other ISPs and state networks is to gain operational experience with version 6 and begin a phased transition approach as soon as possible. “The goal is to make the v6 transition transparent to the end-user, and eliminate the pain on his end.”

Considerations for Rural ISPs

1. Educate yourself. Visit ARIN’s IPv6 Wiki.
2. Open a dialogue with your backbone provider.
3. Update outdated equipment in your central office with IPv6-ready devices, operating systems and applications
4. Ensure that the home networking equipment you are providing to end-users is IPv6 capable. Test your customer’s equipment, including modems and WiFi routers

Resources

American Registry for Internet Numbers (ARIN)
ARIN IPv6 Wiki
Ars Technica Guide to IPv6
Internet Engineering Task Force
Internet Society (ISOC)
Network World Guide to IPv6 Guide
Network World Review of Carrier-Grade/Large-Scale NATs