The IPv6 Challenge – Part 1

A Service Provider’s Guide to the Basics, Transition Strategies, and Implementation Issues

A white paper by Incognito Software
January, 2011
The IPv6 Challenge – Part I

A Service Provider’s Guide to the Basics, Transition Strategies, and Implementation Issues

Contents
Introduction ............................................................................................................. 3
The Pace of IPv4 Address Exhaustion ........................................................................... 3
IPv6 Basics .............................................................................................................. 4
   Hexadecimal Notation ............................................................................................. 5
   Address Fields and Classifications ............................................................................. 5
   Multicast ............................................................................................................... 6
   Datagrams ............................................................................................................ 6
IPv6 Transition Options .............................................................................................. 7
   Cable.................................................................................................................... 7
   Dual Stack .......................................................................................................... 7
   NAT444 .............................................................................................................. 9
   Dual Stake Lite .................................................................................................... 9
   IPv6 Rapid Deployment (6RD) .............................................................................. 10
   Wireline Carriers ................................................................................................. 10
   The Universal IPv6 Gateway .................................................................................... 11
The SP Transition Challenge ....................................................................................... 11
   Planning and Training .......................................................................................... 11
   Provisioning .......................................................................................................... 12
   Implementation .................................................................................................... 13
      CPE .................................................................................................................. 13
      Security ............................................................................................................ 13
      Operations ...................................................................................................... 13
      Management Systems ....................................................................................... 13
   Conclusion .............................................................................................................. 13
**Introduction**

After a decade of talk, speculation, and not a little procrastination, broadband service providers are confronted with the stark reality that the accelerating depletion of IPv4 addresses erases all doubt about the urgency surrounding the transition to IPv6.

That this is no longer an arguable point is dramatically illustrated not only by the faster-than-anticipated shrinkage in the pool of unused IPv4 addresses, but also by the discovery among those who have begun the transition that the process is more complex and time-consuming than previously thought. Any broadband service provider that has not started an IPv6 initiative that includes planning for staff and resource requirements should do so immediately to avoid the risks and costs that further delay is sure to incur.

If there’s one fact that describes the magnitude of the transition challenges it’s this: IPv6, with its 128-bit address field that uses hexadecimal notation (base 16 vs. base 10), is not backward compatible with the 32-bit IPv4 addressing scheme. Every facet of the networking environment where IP addresses and processes are involved, from back-office, to routing and server infrastructure, to customer premises, will be affected by the switch to IPv6.

As a provider of Internet address management and broadband provisioning solutions, Incognito Software is deeply engaged with cable customers who have begun planning for the transition and who are already deploying IPv6 addresses. Incognito is also a key participant in CableLabs’ deliberations on the transition to IPv6. We are leveraging the knowledge we have gleaned from these engagements in our ongoing product development, and are ready to share our perspective on IPv6 and its impact on cable operators.

This document serves as an overview of the forces driving the industry’s transition to IPv6, the transition challenges and technologies, and the many other issues involved with implementing the new protocol. A second white paper addresses planning, provisioning, and the impact IPv6 will have on customer premises equipment and networking.

**The Acceleration of IPv4 Address Exhaustion**

The projected date when ISPs in North America will no longer be able to obtain new IPv4 addresses from the American Registry for Internet Numbers keeps moving forward as a result of a faster-than-expected rate of address depletion worldwide. At the beginning of 2009, the total number of addresses available for allocation through the Internet Assigned Number Authority pool represented about 12 percent of the 2.7 billion addresses originally allocated for public use. At the start of 2010, the percentage was down to ten percent, and by mid-year it had dropped to six percent.

According to statistics supplied by IANA, there were more new addresses issued in the first half of 2010 than in all of 2009. This acceleration is largely due to the fact that at the start of 2010, 90 percent of available addresses had been assigned to just 20 percent of the world’s population, leaving the remaining ten percent for the rest.
ARIN estimates that it will exhaust its share of IANA-supplied IPv4 addresses as of March 2012, at which point it will be impossible for ISPs in North America to obtain new ones. Then it becomes a matter of how many addresses each ISP has in reserve as to when their supplies will run out. However, efforts to stock up on reserves will not buy much time on the clock. Already ARIN has cut the per-request allocation of IPv4 addresses to ISPs from a year’s worth of anticipated requirements to just six months’ worth, with hints that it will soon cut the allocation window to three months’ worth.

Notwithstanding the pace of IPv4 address exhaustion, it’s still possible to hear technically savvy people question why service providers should feel any urgency, given their ability to use network address translation techniques to stretch the lifespan of the IPv4 addresses they hold in reserve. Today NAT is used to allow end-users to continually add to their collection of connected devices without requiring new public addresses.

A new version of NAT, known as NAT444, would overlay that traditional approach with a new one that employs Carrier-Grade NAT. CGN would allow one IPv4 address to be used for a large number of end-users, all of whom would be connected to that address by means of private address extensions. Thus, NAT444 would perform address translation on the customer side in a home gateway and in a CGN box on the service-provider network.

However, cable technology strategists have made clear their distaste for NAT444. While they concede many operators may have no choice but to use this technique, they say it is fraught with issues that could complicate operations and produce lapses in quality of service. Therefore, for reasons discussed below, they recommend limiting its use to the shortest time possible.

There is no elegant means to avoid the fact that in the near future every ISP is going to reach the point where it will be impossible to sign up a new customer without using IPv6. The issue then becomes a matter of gauging what’s entailed in preparing for IPv6 to make sure the transition begins in time to avoid a crisis. Because of the attendant complications of implementing the technology, the urgency becomes more acute with every passing month.

**IPv6 Basics**

The complications stem from the fact that IPv6 was designed to do away with any threat of address exhaustion for a long time. Because it is based on a 128-bit numbering scheme, the volume of possible combinations for individual addresses is astronomically greater than with the 32-bit IPv4 system; in fact, it equates to about 340 trillion trillion trillion addresses. ARIN describes this difference using the following analogy: If all IPv4 addresses were compacted to fit inside a golf ball, all IPv6 addresses at the same density would fill a sphere the size of the sun.

There are parallels between IPv6 and IPv4 with respect to network interface identification and routing, network layer addressing, and the number of IP addresses per device (where a PC, for example, has one address while routers have one for each physical network they connect to). However, there are many significant differences between the two protocols, most notably that the size of the IPv6 field is too large to continue using the familiar base-10 notation system. To reduce the number of characters required to represent an IPv6 address,
the IETF uses hexadecimal notation, which itself represents a learning curve for most network technicians.

Hexadecimal Notation

Hexadecimal notation is used in many number-intensive applications, including computer coding notation, HTML color coding, and IEEE 802 MAC addresses for technologies such as Ethernet. It is a base-16 system using the numbers 0 to 9 and the letters A to F to represent 10 to 15. Any given number represented by these numbers or letters is multiplied by a power of 16 depending on where the represented number is positioned in the string. Thus, just as 125 represents \((1 \times 10^2) + (2 \times 10^1) + (5 \times 10^0)\), so 3AF4 in hexadecimal notation is equal to \((3 \times 16^3) + (10 \times 16^2) + (15 \times 16^1) + (4 \times 16^0)\), or 15,092.

IPv6 fields are broken into 16 groups of 8-bit numbers, separated by colons. Here is an example of an IPv6 address in which all groupings are non-zero:

\[
\]

Double colons signify that the groupings in the intervening spaces are designated as zeroes, for example,

\[
2001:0618:71A3::8A2E:0370:7017
\]

Every device and software module that operates with IP addresses must use this notation when connected via IPv6.

Address Fields and Classifications

The long numbering sequence enables a hierarchical division that can support a large number of addresses in any given class of addresses, thereby allowing multiple levels of network and subnetwork hierarchies at both the ISP and organizational levels. As with IPv4, the unicast address format is by far the dominant mode to be used. It is divided into three primary spaces, with the first 48 bits allocated to the global routing prefix or network ID, the next 16 bits to the subnet identifier, and the final 64 bits to unique identifiers for each device.

The following are the four provisioning classifications for IPv6 addresses:

- **Stateful** – The address is provided by a DHCP server, typically along with other information such as the address of the DNS server and the default gateway.
- **Stateless** – Similar to IPv4 APIPA (Automatic Private IP Addressing), the host assigns itself an address that is automatically configured by router discovery.
- **Link-Local** – These addresses, beginning with FEC0, allow connections by users only on a given subnet.
- **Site-Local** – Confines routing to site-specific devices, preventing any use over the Internet.

Routing discovery uses the new neighbor discovery protocol, which replaces router discovery via address resolution protocol. By combining and augmenting aspects of ARP and internet control management protocol, NDP allows machines to discover information about their nearest router and to obtain information about other hosts. This prevents duplicating IP addresses when autoconfiguration is used.
Some of the differences between IPv6 and IPv4 are more nuanced than others. For example, both have unicast and multicast address types, but IPv6 eliminates broadcast and introduces what is known as “anycast.” By assigning the same IP address to more than one address, anycast creates an environment where communications are directed from a source to the easiest-to-reach member of the group. This would result in simplified load-sharing among routers in an organization.

**Multicast**

More significantly, the IPv6 version of multicast has more features and supports many more multicast addresses than is the case with IPv4. It should be noted that all IPv6-enabled devices must support multicasting.

In contrast to IPv4, which supports multicasting using the Class D address block in the classful addressing hierarchy, IPv6 has a specific block for allocating multicast addresses where any address starting with FF is an IPv6 multicast address. Multicast, like unicast, formats the bit field. This allows routers to be more efficiently aggregated, gives ISPs the flexibility to subdivide address blocks for customers, and provides end-user organizations the flexibility to subdivide their internal networks into multicasting subnets.

By allowing ISPs to set multicast scopes, IPv6 supports multicasting within a specific local network, a specific node, or specific site. This allows routers to determine how broadly to propagate multicast datagrams with much greater accuracy than was possible with IPv4 multicast.

**Datagrams**

A major point of departure with IPv6 is that it redefines the datagram format with a new approach to how headers are designed. This is partially in order to conserve space, given the greatly expanded size of the IP address that is carried in the header, but also to create more flexibility to support new features. Rather than employing just one header to contain all the fields, IPv6 datagrams have a main header that contains only the fields that all or most datagrams require and header extensions that apply to specific types of datagrams.

There are two types of header extensions: destination options intended for end-points, and hop-by-hop options that carry information for routers between the source and destinations. Header extensions defined so far include new support for quality-of-service features for multimedia and other applications, new security support (in authentication and encryption extension headers), and new support for autoconfiguration and renumbering and many other features, including header support for features in the aforementioned approach to multicasting datagrams.

Two other significant changes should be noted with regard to datagrams. First, IPv6 eliminates the traditional checksum calculation, which reduces space and the calculation time spent by every device that packages IP datagrams. Second, the minimum size of datagrams has been increased from 576 bytes to 1,280 bytes, greatly increasing the ratio of maximum payload to header length and cutting back on the amount of fragmentation that must be performed at the source.
Moreover, in IPv6 only the source node can perform fragmentation. Because fragmentation by routers en route is not permitted, a feedback progress has been defined using ICMPv6 (Internet Control Message Protocol for IPv6), which lets routers tell source devices they are using datagrams that are too large for the route.

**IPv6 Transition Options**

One of the key functionalities incorporated into the header extension options is support for mapping between IPv4 and IPv6 addresses to enable implementation of transition techniques for ISPs and other entities. Cable and wireline industries have been working both independently and cooperatively through the IETF to fashion their own variations on transition strategies, some of which are already well established as part of the IETF’s ongoing IPv6 initiative.

Any transition strategy entails finding ways to support using IPv6 addresses for adding new customers and/or new devices while continuing to support existing IPv4 addresses. Since IPv6 is not backward compatible with IPv4, routers running IPv6 must have different routing tables in order to serve IPv4-addressed devices, provisions for security must be altered, and many other steps must be taken to allow an IPv6-based ecosystem to emerge in an IPv4-saturated environment.

It’s well understood that IPv4-addressed end users and devices will be around for a long time, so that even if providers were to deliver a new IPv6 address to every user, they would still have to serve existing IPv4 devices. This also applies to new sign-ups (who are provided with IPv6 addresses), as they, too, will have IPv4-only devices such as iPads and IP-enabled TVs.

Whatever the transition approach, the changes must be invisible to users with no diminution in their quality of experience. This is a tall order, which is why so much effort is being expended by industry technology organizations to fine-tune the details of implementation and to define specifications for new devices that will satisfy these requirements. As service providers undertake preparations for the transition, it is important to bear in mind that these efforts are ongoing, with no cookie-cutter solutions in sight. It is essential for each service provider to stay in touch with these organizations and contribute to their efforts while they work on their own addressing and transition plans.

**Cable**

Where cable is concerned, Comcast has been a leading source of input to the rest of the industry. Their IPv6 program has moved through several phases, including implementation of IPv6 in its core network and various trials of different types of transition techniques. By leveraging the experiences of Comcast and other MSOs, CableLabs has identified four strategies, three transitional and one designed to prolong the rate of IPv4 address depletion, as being suited to cable’s needs. In all cases, CableLabs is helping to define best practices for optimizing the strategies while ensuring that they are compatible with IETF requirements.

**Dual Stack**

The baseline migration strategy is *Dual Stack*, where the service provider runs both IPv4 and IPv6 over the network, allowing end user devices to communicate in whichever protocol
they’re equipped for. If a dual-stack network device such as the CMTS queries the name of a destination and the domain name system gives it an IPv4 address (a DNS A record), the CMTS sends IPv4 packets. If the DNS responds with an IPv6 address (an AAAA record), it sends IPv6 packets. Any dual-stack network device can speak equally to IPv4 devices, IPv6 devices, and other dual-stack devices (where the devices agree on which IP version to use). Thus, under dual stack, the entire transition can be driven by the IPv6-enabled DNS.

Fortunately CableLabs stipulated that support for IPv6 be included in the DOCSIS 3.0 specifications. This allows cable companies operating in dual-stack mode to provide new customers 3.0 modems and assign them IPv6 addresses. Recently, CableLabs extended DOCSIS 2.0 specifications to accommodate upgrades of 2.0 CMTSs and modems to support IPv6 and dual stack as well.

When these IPv6-capable cable modems provision in IPv6 they use stateful DHCPv6 (Dynamic Host Configuration Protocol for IPv6) to acquire their IPv6 address, which is basically how modems provision with IPv4. The cable modem can provision itself for IPv4, IPv6, or dual-stack mode (where it gets both an IPv4 and IPv6 address for management purposes).

At the same time, existing customers equipped with DOCSIS 3.0 or IPv6-enhanced 2.0 cable modems on a dual-stack network can add and obtain addresses for new IPv6 devices that support stateful DHCPv6 provisioning. The modems will bridge IPv4 and IPv6 subscriber traffic no matter what mode the modem uses for management applications.

To extend address provisioning to devices that employ Stateless Address Autoconfiguration (a provisioning mode that is not used with DOCSIS), CableLabs has developed an eRouter specification that defines a lightweight dual-stack cable modem with an embedded router. The eRouter will do WAN-side configuration using stateful DHCPv6 while passing SLAAC or stateful provisioning commands through to devices in accord with whichever provisioning system they require.

CableLabs has also added IPv6 support for Packet Cable 2.0 so that embedded digital voice adaptors can provision in IPv4 or IPv6. However, unlike an IPv6-capable cable modem, whichever mode the eDVA is provisioned in will determine which mode it uses for all its signaling and media messages.

It should be noted that despite these preparations and the elegance of dual stack as a migration strategy, there’s one essential drawback: For every IPv4 device connected by an IPv6 subscriber, there has to be a new IPv4 address provisioned. This is because there is no IPv6 NAT to use for extending private addresses to IPv4 devices. In other words, that native dual stack will last only as long as the ISP has IPv4 addresses to hand out.

Given that most new subscribers will likely have at least one device that needs an IPv4 address, the absence of the private address option means the IPv4 exhaustion rate will be the same or even accelerated compared to what it would be using IPv4 with NAT for new sign-ups. Therefore, dual stack is not to be seen as a way to prolong address exhaustion, but rather as the best way to prepare for the eventual cutover to a predominantly IPv6 mode of operations while assuring support for legacy IPv4 devices.
The need to slow down IPv4 address exhaustion is where CGN-based solutions come into play, including NAT444 and Dual Stack Lite, both of which are endorsed by CableLabs. NAT444 is a dual-NAT approach that retains traditional NAT for extending private addresses to devices behind a customer's publicly addressed router while using the network-based CGN to extend private addresses to end users from a single IPv4 address.

Though it is still in IETF draft stage, NAT444 offers a way for service providers to extend their reserves of IPv4 addresses for a long time to come. Recognizing the usefulness of this technique, one leading router vendor has developed CGN modules for placement on installed core and edge routers, greatly simplifying the implementation of CGN by providers who are running services on those routers.

However, there are many unresolved concerns about how NAT444 might affect the quality of service. For example, with multiple subscribers sharing a single public IPv4 address, there is likely to be an impact on any systems that assume an IPv4 address uniquely identifies an Internet subscriber. Externally, these include e-mail spam monitoring and law enforcement systems. Internally, these include some provisioning systems to support automated subscriber activation, including self-service.

Moreover, the complications associated with connecting certain types of devices such as gaming consoles or Sling boxes to premises-based NAT routers could be magnified in the double-NAT environment where endpoints would be limited in their ability to negotiate port usage. Another CPE-related issue concerns the fact that filtering mechanisms in customer firewalls and routers frequently block packets from the outside network that have private source addresses. To overcome this problem, affected flows must be “hairpinned,” which entails sending them through the CGN to have private addresses of devices on the receive end translated to public addresses and then through the CGN again for the same translation process when those devices respond.

Perhaps most troublesome of all, the double NAT architecture fragments the network, which complicates troubleshooting and repairs. Notwithstanding efforts by the IETF and CableLabs to work through these issues, it’s easy to see why Suddenlink Communications engineer Eric Ballard in the June 24, 2010 webinar titled Cable’s Transition to IPv6 warned that NAT444 could become an operational nightmare for network service providers. To whatever extent service providers find themselves with no alternative but to use NAT444 to preserve their IPv4 address supplies, it’s clear the technique should not be relied on as an alternative to pushing ahead with implementation of IPv6.

Dual Stack Lite

As a way around the double NAT issue, which exploits the address-conserving capabilities of the CGN strategy while advancing the implementation of IPv6, Comcast has proposed what it calls “Dual Stack Lite.” DS-Lite provides a means by which all IPv4 traffic destined for IPv6-addressed customers is delivered over stateless IPv6 tunnels between the CGN and the customer’s IPv6 gateway. This solution, now in development as an IETF standard, would require that new customers who receive IPv6 addresses be equipped with gateways that perform this tunneling, avoiding the need to implement NAT for IPv4 devices at the CPE.

Comcast and the non-profit Internet Systems Consortium recently released open-source Address Family Transition Router software to facilitate service providers’ implementation of
DS-Lite. AFTR, the heart of the IPv4-to-IPv6 CGN translation process, operates in conjunction with another new element, the DS-Lite Basic Bridging BroadBand (B4) element, which resides in each IPv6 gateway device as the tunneling point for sending IPv4 traffic through the IPv6 network to the translation center.

Pending the outcome of trials, Comcast officials have indicated DS-Lite is likely to be the company’s preferred approach to accommodating new subscribers once the IPv4 address supply runs out. However, it expects to complete the transition to dual-stack operations prior to having to implement DS-Lite.

**IPv6 Rapid Deployment**

At the time of this writing, IPv6 Rapid Deployment (6RD) is in the final stages of approval as an IETF standard. It provides operators who have not equipped their networks to support IPv6 a way to deliver service to IPv6-addressed customers. It is viewed as an interim backup strategy, not as a way to avoid implementing IPv6 in the network.

6RD is a public tunneling solution that encapsulates IPv6 into IPv4. It uses a public IPv6 prefix to ensure that all IPv6 communications entering the operator’s local network pass through the operator’s tunneling points to reach designated users. The technology requires that CMTSs be upgraded to support encapsulation and de-encapsulation and that IPv6-addressed end users be equipped with modems or routers that do the same thing.

One drawback to this solution is that it requires operators to maintain control over customer premises equipment, since most off-the-shelf IPv6 home gateways do not support translation. Also, it remains to be seen in forthcoming field trials whether the technology has any adverse effects in real-world operations. So far, however, lab tests conducted by operators, CableLabs, and others have indicated that 6RD performs as intended.

**Wireline Carriers**

Wireline carriers have their own set of issues to deal with in accommodating the transition to IPv6. The IETF and the Broadband Forum (the carrier standards body) have made considerable progress toward establishing the transition technologies for implementing dual stack, but there’s still much work to be done.

The organizations have adopted a means of supporting dual stack that uses Point-to-Point Protocol, which carries the lion’s share of Internet communications over DSL access networks. The Broadband Access Server or Broadband Network Gateway, which acts as the CPE terminator in the network much as CMTS does in cable, performs the DHCPv6 relay and conveys the necessary radius attributes related to IPv6 within PPP sessions. However, all but the most recently deployed BRAS and BNG units will have to be upgraded to support dual stack over PPP.

As for CPE, new subscribers equipped with new TR-069 gateway modems can be readily supplied an IPv6 address over the PPP dual-stack implementation if their PC operating systems support installation of PPP over Ethernet software client adaptors. For example, recent versions of Microsoft OS support IPv6 and IPv4 over PPPoE. All the new customer needs to do to set up IPv6 provisioning is to initiate the PPPoE application on the OS CD by typing their username and password.
However, if the new subscriber doesn’t have such equipment, the implementation of IPv6 by means of dual stack over PPP becomes problematic. Customers with older routers will have to replace them, but even when they do, the new boxes are still not equipped to support legacy IPv4 devices on the customer network, and some may not adequately support public IPv6 addressing for IPv6-capable hosts on the home network.

Adding to the difficulties of IPv6 migration in wireline networks is the need to support dual stack where IP over Ethernet is used instead of PPP to deliver Internet services to customers. Here the Broadband Forum and IETF are still working to develop a standardized approach to enable IP DSLAMs, which act as DHCP relays, to implement DHCPv6 for stateful prefix delegation in customer gateways. Once the process is defined, conversion will require upgrades of deployed IP DSLAMs.

**The Universal IPv6 Gateway**

The CPE issues for wireline and cable will diminish over time as new options become available through retail outlets. The previously discussed CableLabs eRouter specification is one significant development in this area.

Going forward, in an effort to make off-the-shelf IPv6-capable routers as simple as possible, the IETF, CableLabs, and the Broadband Forum are working together to develop specifications for an IPv6 home gateway that would work in the dual-stack environment on both cable and DSL networks. The draft specifications, moving rapidly toward formal adoption at IETF, support both stateful provisioning as required by CableLabs and SLAAC as required in the DSL environment.

This new router specification leverages much of the work that’s already gone into the cable eRouter. Therefore, the new universal router will support connectivity of IPv4 as well as IPv6 devices to the home network. Both router specifications also support the IPv6 multicast proxy so that service providers and outside entities will be able to deliver multicast streaming services to IPv6 devices.

**Transition Challenges for Service Providers**

As standards bodies continue to refine and formalize the various transition and CPE standards it’s absolutely essential that service providers initiate internal IPv6 migration projects immediately. There is an immense amount of planning and training that must be undertaken before a company can begin the migration to IPv6 in its networks, and the implementation process itself is a massive undertaking that will take a considerable amount of time. These challenges are discussed in detail in the second white paper on IPv6. Here we provide a brief explanation of some of the key steps and challenges.

**Planning and Training**

It’s essential that preparations start with determining how various groups within the operations, engineering, and management layers will interact. This includes defining work flows, areas of individual and shared responsibility, and timelines. Frequently service providers underestimate how broad-based an effort the transition to IPv6 really is, and they are forced to bring people into the planning phase later than would be optimal.
Vendors, too, must be part of the planning process to ensure they are prepared to support whatever decisions are made that require support from network elements and operations components. Some vendors are more prepared than others to support IPv6. Knowing whether legacy equipment has that support is essential to near-term purchasing decisions as well as future migration.

As a new protocol, IPv6 requires that much thought be given to addressing plans, which first requires obtaining a prefix from ARIN and then determining how addresses will be assigned at the core, subnet, and end user levels. Planning also requires setting a strategy, including testing, for determining which migration path to take.

These steps lead to deeper, implementation-oriented planning around questions such as what the network feature topology looks like. Service providers need to determine the organization of the pure IPv4 network, the dual-stack IPv6 network component, the next-gen Routing Information Protocol for IPv6 (RIPng) for small business customers, and any pure IPv6 such as a multicasting network. Assessing core routing protocol choices – Intermediate System to Intermediate System (IS-IS) vs. Open Shortest Path First Version 3 for use with IPv6 (OSPFv3) – is part of the planning process as well.

Everyone directly involved in the planning initiative will face a learning curve, but it’s also important to assess who else in the organization should begin training on the essentials. This will ensure that all who have a role to play in implementation are adequately prepared by the time the launch phase begins. Beyond field and network operation center staff, there will also be a need for some degree of training for customer-facing techs and customer service representatives.

Provisioning

Advance preparations are essential in the provisioning arena, where IPv6 brings new concepts such as the Neighbors Summary Protocol that allows operators to provision at Layer 3. Stateful DHCPv6 prefix delegation parallels the stateful process used in IPv4 by cable operators, but, with no NAT to use, they’ll have to be able to work with SLAAC as well when it comes to addressing devices that rely on automated configuration. Service providers will also have to understand Alternative Provisioning Mode, a Layer 2 provisioning technique that provides a fallback to IPv4 or IPv6 if one or the other fails.

Any operators who are still using manual input to configure IPv4 addresses will have to move to an automated system, such as Address Commander from Incognito Software. Address Commander has supported IPv6 planning and management for several years and offers service providers an effective solution for planning, managing address assignment, and synchronizing their IPv6 assets with DNS systems.

Because the massive size of the IPv6 address space, reverse name mapping, an essential part of day-to-day operations over the public Internet, is impossible to administer manually. Equally critical are forward lookups for IPv6, where entering IPv6 addresses even in shorthand notation in a Web browser is problematic. Operators must be sure to have fully integrated IP address management and DNS management strategies in place before undertaking any transition to IPv6.
The IPv6 Challenge – Part 1

Implementation

Once in the IPv6 implementation stage, CPE, security, operations and management systems issues must be dealt with to ensure a smooth transition.

CPE

Service providers will need to fully understand the nuances of features, provisioning requirements, operations management, and emerging technologies of myriad devices to ensure they are prepared to continue delivering a convenient consumer experience. These devices include modems and router gateways and extend to PCs, connected TVs, and portable devices.

Security

IPv6 brings new security issues into play as well as better security through the inclusion of IPsec protocol as one of the header extensions. For example, the Neighbor Discovery Protocol introduces new security issues that might have to be addressed through secure FTP. Dynamic DNS adds convenience to operations but exposes new vulnerabilities that must be dealt with. (These are, in fact, currently a matter of intense discovery and testing among security experts with much left to be resolved.)

Operations

Operators will have to understand and prepare for many points of impact in operations. These include IP detail record collectors, configuring management information base data for dual stack and IPv6 anycast, and setting up SNMP for operations in dual-stack mode.

Management Systems

Every business and operations support system that uses an IP address field will have to be adjusted to accommodate IPv6. Many management components will be deeply affected, including Web systems, network management systems, deep-packet inspection, firewalls, and email systems.

Conclusion

Clearly, the acceleration of IPv4 address exhaustion leaves service providers no choice but to prepare for the transition to IPv6. It’s equally clear that the complexities of implementation will require wise use of time between now and when those addresses run out if service providers are to avoid serious problems in the years ahead.

In the second white paper on IPv6 we look closely at the address planning process, the details of provisioning, DNS operations, and the many factors to be considered regarding the fast-paced evolution of CPE. These are discussed in the context of various migration strategies in both the consumer and commercial services arenas.
Contact:

Incognito Software Inc.
Phone: 604.688.4332 or US/Canada toll free 800.877.1856
Fax: 604.688.4339
Email: sales@incognito.com
Web: http://www.incognito.com