



Transitioning the Public Internet to Internet Protocol Version 6 (IPv6)

Before IPv6—IPv4

Today's Internet uses Internet Protocol version 4 (IPv4). For the average user, IPv4 does what it needs to. Yet, constant changes in many industries, along with rapid technology expansion, result in the need for greater capacity of some form or other.

IPv6 was first developed in 1994 with the intention of improving IPv4. While there are many changes between the two versions, the most notable is a longer IP address field. As a result of the explosive growth experienced by the Internet since its inception, many anticipated a rapid exhaustion of available IP addresses. IPv4 only supports a 32-bit IP address field, but IPv6 provides a full 128 bits for an IP address.

Ten years have passed since IPv6 was initially developed, so why hasn't IPv6 been adopted yet? For starters, the rapid deployment of NAT technology to preserve public IP addresses greatly reduced the demand for new IP addresses. The other features of IPv6 were less relevant, and the hurdles associated with deploying IPv6 were too enormous even to begin to contemplate. People often ask, "What ever happened to IPv5?" In general, protocols have fields that indicate their version. IPv4 uses the value "4." When the Stream Protocol (ST) was developed, it was assigned the value "5." ST wasn't really a replacement for IPv4, but rather, a totally separate protocol that was designed to coexist with IP. When IPv6 was proposed, "5" was already taken so the next IP protocol was assigned "6."

IPv6 Motivators

Still, IPv6 offers many benefits that IPv4 never will be able to provide. As mentioned previously, IPv6 supplies many more IP addresses than IPv4—340,282,366,920, 938,463,463,374,607,431,768,211,456 to be exact. Needless to say, it will be a while before IPv6 addresses run out. Beyond IP addressing, IPv6 introduces other enhancements:

- Native support for IPsec
- Anycast
- Native Quality of Service (QoS)
- Native Mobile IP
- Auto-configuration capabilities
- Optimized packet structure (i.e., less overhead)

These alone have not been sufficient to drive IPv6 adoption. For the most part, the benefits of these enhancements can be achieved through other means. For example, NAT greatly reduced the need for IP addresses. Dynamic Host Control Protocol (DHCP) helped with the configuration of end-user devices.

The two most powerful drivers of IPv6 actually may be new applications that are unique to IPv6 and competitive positioning among the service providers.

Applications

Applications may be the most important class of motivators for IPv6, simply because they have the potential to drive demand. Demand will drive ISPs, software providers, and equipment manufacturers to react.

With IPv6, new applications can be spawned that were not practical previously. These include:

- Remote telemetry applications. Monitoring of remote equipment (e.g., soda machines, utility meters, etc.)

Internet

IPv6 was developed to improve on its predecessor protocol, addressing many of the limitations that became apparent as the Internet grew. However, to generate improvements, a completely new protocol that was not backwards-compatible with the existing IPv4 specification was required. This created a technological hurdle that few have been willing to clear. Rather, the industry has found ways around the deficiencies of IPv4.

Of all of the benefits that IPv6 brings to protocol technology, the increase in IP addresses is the most notable. If the Internet is to continue to grow and support new applications, the world will need more IP addresses. Technologies such as Network Address Translation (NAT) are stop-gap measures to buy time. ***The point when IPv4 addresses will no longer be available for allocation from Regional Internet Registries (RIR) is unclear. Industry studies estimate the timeline anywhere from early 2011 to late 2012.***

A more likely motivation is the advent of new applications that require IPv6. ***An example is the Long Term Evolution (LTE) development occurring within Wireless Carriers. This technology was developed specifically for IPv6 to handle the expected increase in mobility users, a potential IPv4 exhaustion catalyst, due to the bandwidth benefits from LTE.***

- IP enabling the battlefield. Streamline communications for military applications, including access to real-time information from equipment and personnel
- Vehicle-based applications. Remote assistance and tracking capabilities, including on-board diagnostics, etc.
- Advanced interactive gaming. Especially when combined with QoS
- Inventory management and control. Including integration with radio frequency identification (RFID) systems
- Internet-enabled appliances. Existing appliances (e.g., refrigerators) and new ones
- An IP address for every person. This could enhance further work in the field of mobility and presence

Competitive Positioning

Competitive pressures and one-upmanship also will be powerful factors in the decision to make the leap to IPv6.

- Just as Wal-Mart transformed large parts of the retail supply chain, the possibility exists that certain large entities may deploy IPv6 and require others to support IPv6 in order to communicate. Perhaps the best example of this was the U.S. Department of Defense (DoD) mandate to provide support IPv6 by 2008.
- Certain parts of the Internet may emerge as “IPv6-only,” creating a separate Internet universe isolated from the current one. This may begin to appear first in developing regions, such as Asia, where the demand for IP addresses is growing quickly.
- IPv6 creates a “land-grab” opportunity for many second- and third-tier players. These players do not have extensive and expensive infrastructures to convert, so they may jump to IPv6 before the tier-one players. In turn, the large Internet backbone operators have extensive networks with numerous peers making the transition to IPv6 more difficult.

But the combined effect of these still may not be enough to rally an entire industry and market to react quickly. Unless demand is a factor, IPv6 advantages may not provide enough impetus to outweigh the difficulty and drive action by the parties that deliver IP.

Hurdles to Cross

The Internet is a complex system of routers, servers, protocols, and communications links. Think about all of the different Internet Service Providers (ISPs) that comprise the Internet, all of the different types of hardware employed, all of the different software versions used, all of the different customer devices, etc. It’s amazing they all work together. The reason they do is because they speak a common language—IPv4.

On the surface, it may appear that simply upgrading software or enabling a feature will solve the issue. However, the challenge is infinitely more complex. There are many legacy and home-grown devices in the Internet today that cannot be upgraded easily to support IPv6. Much of the IPv6 software code that has been released has not been tested extensively, particularly in a large-scale environment. Releasing unstable code into a large production environment could wreak havoc easily on the existing Internet ecosystem. There also are fears surrounding security in an IPv6 environment. What new vulnerabilities are waiting to be exploited? What old vulnerabilities are able to find a new lease on life? For these reasons, many large Internet-backbone operators are hesitant to jump headfirst into the IPv6 world.

Dual Stack

One of the biggest hurdles to cross with IPv6 is support for “two-of-something.” Today, the Internet supports one protocol, IPv4. Anyone ordering IP service does not need to think about what version(s) they require.

Given the incompatibility of IPv4 with IPv6, there likely will be an interim period when IPv6 is enabled and both versions are supported side-by-side. This essentially means that those who connect to the Internet will need to connect to both sides—the IPv4 side and the IPv6 side. Supporting two versions of the protocol instead of one becomes complex. Either every device, end-to-end, needs to support both protocols (also known as dual stack), or, at some point, address translation or tunneling will need to occur. And the issue of how applications and operating systems determine which one to use at anygiven time also must be sorted. All said and done, numerous moving parts are involved.

Backbone Networks

Most major suppliers of Internet backbone equipment already support IPv6 in their software and hardware. As noted previously, ISPs have been slow to deploy or enable IPv6 due to the uncertainty of its stability. The fact that most networks are hybrids, consisting of equipment from multiple vendors, as well as both old and new equipment, further complicates matters. Older equipment may not support IPv6, creating a need for a technology refresh—one that may not be justified financially. Perhaps just as frightening are all of the ancillary services that are provided by backbone operators. The most notorious and often overlooked is Domain Name Service (DNS). With the introduction of IPv6, the DNS infrastructure will need to evolve to operate on the IPv6 Internet, as well as be able to resolve IPv6 addresses.

Other services that need to be addressed are:

- Mail servers and gateways
- News servers
- Caching servers
- Various network monitoring and reporting systems.



Network Edge

Perhaps more difficult to convert to IPv6 than the core backbone is the network edge. This is where customers and peers terminate their connections. As the Internet evolved, an entire plethora of access types became available. Dedicated leased lines, dial-up and ISDN, DSL and cable, satellite, WiFi, 3G cellular, and so on. All of the edge systems that deliver these will need to embrace IPv6. This is difficult given all of the vendors that are involved. Likewise, the so-called edge has been commoditized greatly in recent years, raising the question about whether IPv6 is a good investment. Alternatively, gateway or NAT technologies may end up being deployed to allow the IPv4 end-user to interact with the IPv6 Internet. One example is Teredo. Also known as Shipworm, Teredo is an auto-configured tunneling mechanism that is supported in Microsoft® Windows XP and other systems. Other suitable tunneling technologies include 6to4 and Generic Route Encapsulation (GRE).

Customer Premises Equipment

Another area that has been commoditized highly is customer premises equipment (CPE)—particularly consumer-broadband equipment. In some instances, WiFi routers are offered at less than \$10 now. In order to extend IPv6 to the end-user, all of these devices will need to support it. That either implies extensive software upgrades or, more likely, some sort of technology refresh. In order to get the myriad of CPE manufacturers to support IPv6, there will need to be some strong motivators that create end user demand.

Operating Systems and Applications

One area that seems relatively promising is operating systems. Many of the top operating systems already support IPv6 today. They include Windows® XP, Apple Mac OS, Red Hat Enterprise ?? Linux, and UNIX. However, very little expertise to configure IPv6 on these systems exists, and, to the surprise of many, a substantial number of the applications that may reside on these systems are not IPv6-capable presently. Today, most applications are too aware of the networking layer below them—in some instances using IP addresses directly instead of DNS. Luckily, some of this is being addressed in future operating system and application releases.

Back-Office Support Systems

Since the Internet has found its way virtually into everything we do, it is only natural to find that IP addresses are being handled by a wide variety of systems. The systems that are used to maintain and manage IP networks are of particular concern. For service providers, this may include order-entry, provisioning, operations, and support systems. For enterprises, it may consist of network-management systems, databases, and other applications.

An initiative, similar to the Y2K-frenzy that occurred to ensure year 2000 compliance and/or remediation, may be required to identify and modify IP-address fields in countless systems. If this is the case, four questions will need to be answered.

1. Are IP addresses (i.e., not host names) being stored directly?
Generally, this is a bad practice, given that IP addresses may change from time-to-time for various reasons.
2. Are IP addresses stored as 32-bit numeric fields?
IPv6 uses 128 bits, requiring longer fields to be used.
3. Are IP addresses stored as strings?
IPv4 addresses have a maximum length of 15 characters versus IPv6 with a maximum of 39. Further complicating the situation, IPv6 uses eight numeric fields with colons as separators versus four fields with dots as separators in IPv4. IPv6 also has extensive rules for abbreviation, perhaps requiring changes in logic for processing addresses.
4. Will users need to support both an IPv4 and IPv6 address?
Since it may be necessary to operate in a dual-stack mode, tracking both addresses may be a requirement
Furthermore, logic will need to be developed to determine when to use each.

Rule and Policy Changes

Not only is IPv6 different in its structure from IPv4, but also it specifies rules and policies that do not easily fit well with how the Internet operates today. In order for IPv6 to be adopted readily by the Internet community at large, many issues will need to be addressed. Among the more notable rule and policy changes are:

National Address Block Allocations

With IPv6, IP address blocks are allocated on a national-level basis. This naturally will bring about the need for localized allocation policies and restrictions. For the most part, the Internet in its current form has remained non-political. IPv6 could potentially change that.

Perhaps of greater concern is the risk of changing borders. When this occurs, it is not clear how IP allocations might change or what new policies may arise. This is a particular concern for multi-national corporations that operate globally, as well as the ISPs that support them.

Multihoming

Multihoming, the somewhat common practice of connecting to the Internet with more than one connection in order to provide diversity and resiliency, is not well addressed in the IPv6 world. When an enterprise multihomes



today, it has the ability to route its IP traffic over any one of its Internet connections, regardless of network provider. The need for this is not likely to disappear when IPv6 becomes prevalent.

When IPv6 was developed, a great degree of aggregation was implemented, whereby ISPs were to be given large chunks of contiguous IP address space in an effort to streamline routing. In today's Internet, IP addressing is very fragmented. This ends up being very helpful for multihoming. Since IPv6 has longer and infinitely more IP addresses, the resources required for routing (mainly router memory and CPU) can be exhausted much more quickly. Therefore, aggregation is a sensible way to limit the number of routes. The bad news is that multihoming becomes impractical. To address this, several standards forums are discussing alternatives to de-aggregation in order to preserve multihoming and its benefits.

IP Security Key Distribution

Although IPv6 has the ability to support Internet Protocol Security (IPsec) encryption natively, it does not specify how key distribution will occur. Technologies such as Public Key Infrastructure (PKI) are promising, but, thus far, have not been proven to function well in a large-scale environment. More work is required in this area.

Walk Before You Run

Since ISPs are the ones that bring everything together—end-user devices and software, communicating via edge-services, over large IP backbones—perhaps they will shoulder the greatest burden in driving the adoption of IPv6. The technology is becoming available, and the fears are recognized. The applications haven't evolved yet, but, for many ISPs, there is great concern that they will not be able to react quickly enough when the applications do arrive.

Many ISPs may find themselves making early nominal investments in IPv6, not only to limit their financial risk, but also to provide them the opportunity to attain expertise.

Since the ISP has a base of customers that it must continue to serve with IPv4, it becomes necessary to maintain the integrity of that delicate environment while beginning to work with IPv6. For that reason, several ISPs have opted to deliver IPv6 initially using overlay networks, logically isolated from their larger core backbones. This approach brings many benefits to both the provider and its customers.

- Overlay services are able to use the capacity of the core backbone network.
- Not running IPv6 directly on the core backbone may allay fears of instability and security vulnerabilities.
- Use of tunneling technologies, such as GRE, provides a "secure" transport for the connection to customers and peers, while allowing IPv4 traffic to be processed normally.
- Isolation provided by tunneling also affords customers the ability to experiment with IPv6 on their production IP links without the need to deploy IPv6 directly onto their CPE routers. This is often accomplished using a dedicated router (behind their primary router) that is designated for IPv6 use.
- Ancillary services, such as DNS, can be operated independently in the IPv6 universe, thus providing further isolation from the production environment.

Summary

The evolution to IPv6 will not be an easy one. Even though some degree of progress has been made at the operating-system and backbone-router levels, much work is still required for application support and network edge. Perhaps the biggest burden will fall on the shoulders of the ISPs to embrace IPv6 and undertake the necessary integration to make it a reality. However, given the complexity of such an evolution and the time required to make the transition, IPv6 needs to be taken seriously today.

The catalyst that spurs adoption of IPv6 may be applications that have not evolved yet. These most likely will be applications that take advantage of key features of IPv6 or are perhaps only available on the IPv6 Internet. That will necessitate a move to the IPv6 platform and motivate end-users of those applications to the IPv6 world.

The biggest challenges to this transition theory come from the ubiquity of IPv4 in today's world, as well as the enhancements that have been made to IPv4 to overcome the issues that IPv6 is intended to solve. In the end, mandates from influential organizations such as the U.S. Department of Defense ultimately may be what drive the adoption of worldwide IPv6.

To learn more about Verizon's IPv6, contact your Verizon account manager or visit <http://www.verizonbusiness.com/us/data/>.

verizonbusiness.com

verizonbusiness.com/socialmedia verizonbusiness.com/thinkforward

© 2010 Verizon. All Rights Reserved. WP14656 8/10
The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

About Verizon Business

Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world's most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today's extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world's largest businesses and governments—including 96 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at www.verizonbusiness.com.

