WHITE PAPER

IPV6: WHY MOVE TO THE NEXT GENERATION OF THE INTERNET PROTOCOL?

Robert Winter, Technologist, Office of the CTO

May 2008

The vast majority of networks today, including the Internet, are based on the Internet Protocol, version 4 (IPv4) protocol. Developed over 25 years ago, IPv4 is showing its age. Its 32-bit addressing cannot accommodate the explosive growth worldwide of network-connected devices, particularly in Asia and China. It is estimated that the world may run out of IP addresses as early as 2010-2013. Moreover, IPv4 was not designed with security in mind and its security solutions have not kept pace with the expanding requirements of IP-based networks. These deficiencies are addressed by IPv6.

Two main forces are driving the transition from IPv4 to IPv6:

- The U.S. Department of Defense (DoD), as well as other U.S. government agencies, are mandating IPv6-compliant IT equipment, starting as early as June 2008.
- Internet use in countries outside the United States is steadily increasing and is driving commercial adoption.

Dell is quickly moving to meet DoD requirements, as well as those of our customers in Asia and the rest of the world. This white paper compares IPv4 and IPv6, reviews the two main IPv6 certification programs, and describes Dell's efforts to meet our customers' IPv6 needs.

Background

The IPv6, replaces the IPv4 protocol used in TCP/IP networks today. Introduced in 1981, IPv4 was not designed to scale to the magnitude of today's World Wide Web. Instead, it was originally designed as a mesh networking technology to support academic researchers in the U.S. It was funded by U.S. DoD Defense Advanced Research Projects Agency (DARPA). DARPA needed a networking technology that provided multiple and redundant routes to retrieve data and maintain communication, with no single point of failure.

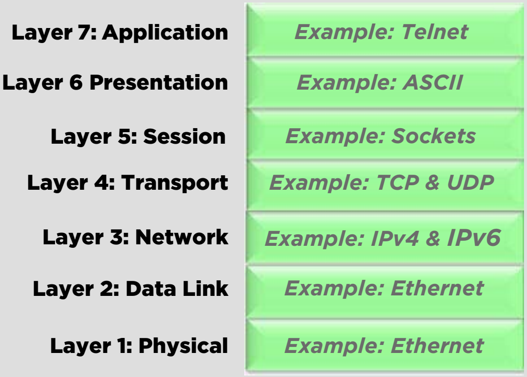
Since then, IPv4 has been extended to accommodate the explosive growth of the Internet. However, its deficiencies are becoming an issue in today's evolved Internet.

The main weakness of IPv4 is the limited number of addresses enabled by its 32-bit addressing scheme. IPv4 addresses are being depleted at an accelerating rate. Techniques have been developed to conserve addresses by reusing them, but these techniques tend to create an awkward and complex network infrastructure.

Other issues with IPv4 center on data packet inefficiencies, particularly in the "header," the portion of the packet that contains the addressing and

What is IPv6?

IPv6 is a layer 3 protocol in the Open Systems Interconnect (OSI) networking model shown in Figure 1. It is used by the Transmission Control Protocol (TCP) to transmit data across a packet-switched network.



Layer 7: Application	*Example: Telnet*
Layer 6 Presentation	*Example: ASCII*
Layer 5: Session	*Example: Sockets*
Layer 4: Transport	*Example: TCP & UDP*
Layer 3: Network	*Example: IPv4 & IPv6*
Layer 2: Data Link	*Example: Ethernet*
Layer 1: Physical	*Example: Ethernet*

Figure 1. OSI Protocol Reference Model

control information needed to transmit data over an IP network. These inefficiencies include:

- Unused fields and rarely used options.
- Variable header size, which is less efficient than a fixed-size packet.
- Unnecessary error-checking that is redundant to the error-checking mechanisms at the physical layer of most networks, including Ethernet.

In addition, IPv4 lacks robust quality of service (QoS) capability, which guarantees a specified level of service for network traffic such as audio and video that cannot tolerate latency. Finally, IPv4 does not provide the level of security required today.

While the issues with IPv4 are not yet critical, there is no doubt that they will be in the near future. The eventual need for a replacement IP technology is certain.

What is driving IPv6 deployment?

As mentioned earlier, there are currently two driving forces behind IPv6 deployment in the world. The first is the mandate from the U.S. DoD requiring that, starting in June 2008, all IT asset acquisitions by the DoD and associated agencies must support the migration to IPv6. The second driving force is the increase in Internet use around the world, especially in Asia. China, in particular, with its millions of Internet users is hindered by the antiquated IPv4 infrastructure.

U.S. DoD Deployment

In June 2003, the DoD issued a memo mandating IPv6 adoption.[1] In August 2005 the U.S. Office of Management and Budget (OMB) issued a similar memo,[2] soon followed by memos from other U.S. government agencies. In late 2006, the Defense Information Technology Standards Registry (DISR) produced its first "Product Profile Document" that classified all networked products into categories, each with specific IPv6 requirements. Companies that do business with the DoD must use this document to develop IPv6 product plans. A defined process governs IPv6 product certification and the Joint Interoperability Testing Command (JITC) agency performs certification testing.

Worldwide Deployment

International initiatives to foster IPv6 adoption and interoperability are emerging through organizations such as the IPv6 Forum.[3] The commercial drivers for IPv6 adoption will most likely occur outside of the U.S., which owns over 70% of the world's IPv4 addresses and thus has less imperative to move to another IP technology. As shown in Figure 2, the National Institute of Standards and Technologies (NIST) estimated timeframe of IPv6 dominance—defined as more than 50 percent IPv6 use worldwide—is around the year 2012.

IPv6 Technology Advantages

IPv6 is specified by the Internet Engineering Task Force (IETF) in a series of requests for comments (RFCs) that define its operation, structure, and usage scenarios. Work was begun in the early 1990s and the first informational RFC—"Comparison of Proposals for the Next Version of IP" (RFC 1454)—was released in May 1993. There are well over 300 RFCs that deal with IPv6, and more are being created all the time. The main specification, RFC 2460[4]—"The Internet Protocol Version 6 Specification"—is the foundation of most IPv6 requirements.

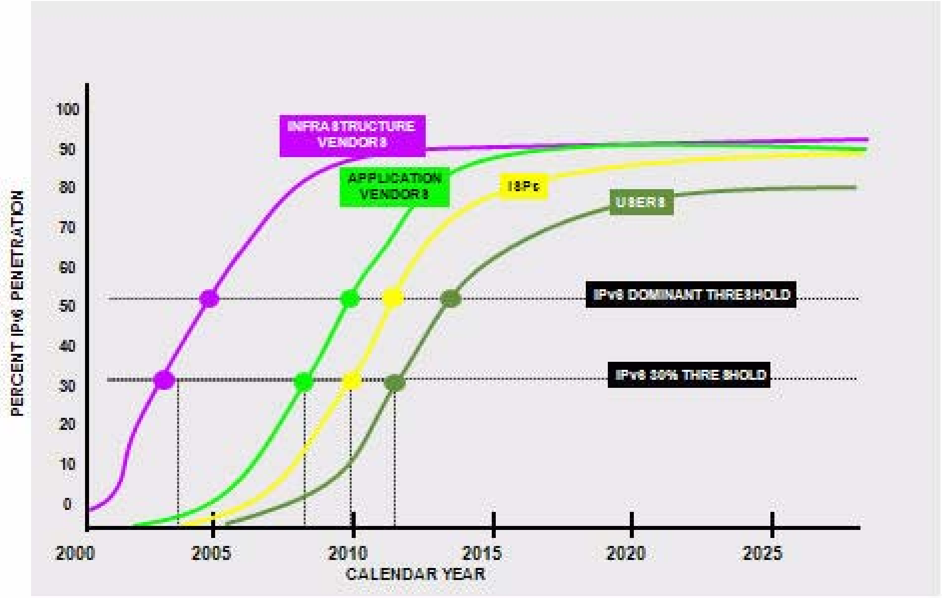
IPv6 offers improvements over IPv4 in its addressing scheme, packet efficiencies, error checking, quality of service (QoS) provisions, and security.

[1] See the DoD memo at https://acc.dau.mil/CommunityBrowser.aspx?id=31652.

[2] See the OMB memo at www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf.

[3] See www.ipv6forum.com.

[4] See RFCs at www.rfc-editor.org.



Source: "IPv6 Economic Impact Assessment," National Institute of Standards and Technologies, October 2005, www.nist.gov/director/prog-ofc/report05-2.pdf, Figure ES-1.

Figure 2. IPv6 Penetration Estimates in the U.S.

IPv6 Addressing

The IPv6 addressing scheme accommodates the growing need for IP addresses in the world. IPv6 expands the IPv4 32-bit addressing scheme to 128-bit (16-byte) source and destination IP addresses, providing over 3.4 x 10^{38} possible IP addresses. This large address space is allocated according to a defined IPv6 address subnetting structure so that it is more manageable than that provided under IPv4.

Even though only a small number of the possible addresses are currently allocated, there are plenty of addresses available for future use. This increased capacity will eventually render obsolete the address-conservation techniques such as network address translation (NAT) used in today's IPv4 networks.

How many IPv6 addresses are there?!?

- 340 trillion, trillion, trillion (or 340, 282, 366, 920, 938, 43, 374, 607, 431, 768, 211, 456) addresses. IPv4 has only 4 trillion addresses.
- More than all the grains of sand in the world.
- More than all the cells in all the organisms in the world.
- If IP addresses had volume and the IPv4 address space was a jelly bean, the IPv6 address space would be a sphere containing the entire solar system.
- Enough to assign each human being on earth many trillions of addresses.

IPv6 Packet Efficiencies

The format of the IPv6 packet header enables more efficient processing than IPv4. IPv6 has a fixed-length header that contains only essential fields. In contrast, the length of the IPv4 packet header varies to accommodate rarely used fields and options. This variable structure increases the complexity of processing IPv4 packets. Figure 3 compares the IPv6 and IPv4 headers. Although only twice the length of the IPv4 header, the IPv6 header accommodates much longer addresses than IPv4.

What happens during the transition to IPv6?

During the transition, both IPv4 and IPv6 network stacks will be supported by most network devices. IPv6 has been designed to tunnel inside an IPv4 network, as well as to deliver IPv4-originated packets.

IPv6 Error-Checking

When IPv4 was originally developed, it included error-checking because networks at that time were not as reliable at the physical layer as they are today. The IPv4 checksum mechanism helped ensure that data packets arrived intact. These days, networks are very reliable at the physical layer and include their own error-checking mechanisms. As a result, error-checking at the IP layer, which increases the packet-processing burden, is no longer needed. The IPv6 packet does not include a checksum, relying instead on robust error-checking at the physical layer.

IPv6 Quality of Service and Security

Unlike IPv4, there are new, larger fields in the IPv6 header that can be used to define how traffic is handled and identified, thus enabling better QoS capability for audio and video traffic.

One of these fields, the "Flow Label" field, identifies the series of packets exchanged between source and destination endpoints in a network. This field can be used to enforce prioritization or other policies on this flow. For example, IPTV and voice over IP (VoIP) applications that stream audio and video over the network require that the content be streamed at a predictable rate with low latency. With QoS capability, this traffic can be prioritized and streamed at a guaranteed rate.

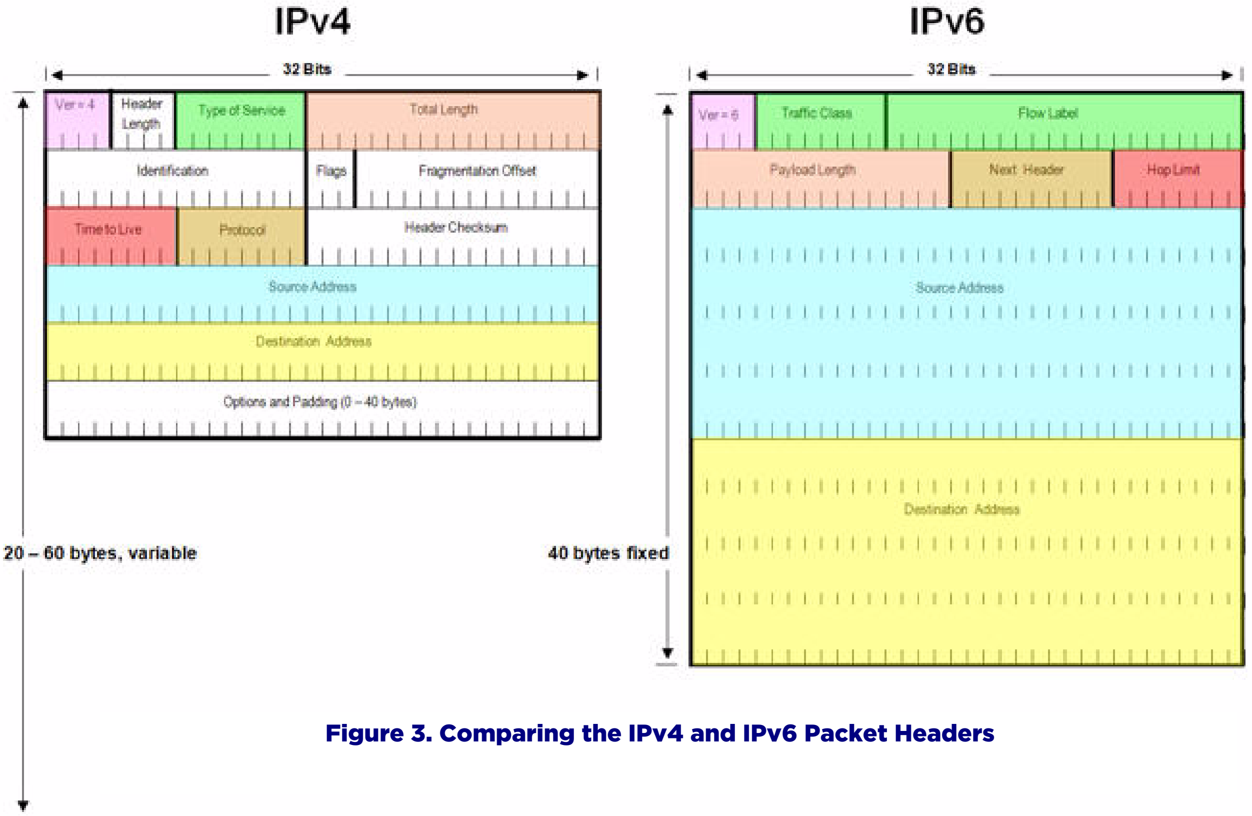


Figure 3. Comparing the IPv4 and IPv6 Packet Headers

Support for IP Security (IPsec) is an IPv6 protocol suite requirement as outlined in RFC 4224.[5] This requirement provides a standards-based solution for robust network security and promotes interoperability between different IPv6 security implementations.

IPv6 Compliance Programs

Two main IPv6 compliance certifications exist. The first is specific to the DoD and other U.S. government agencies. The second is the "IPv6 Ready" certification administered by the University of New Hampshire (UNH).

Inside the U.S.: DoD Certification

The DoD certification is administered by the Defense Information Technology Standards Registry (DISR) organization. The DISR document—"DoD IPv6 Standard Profiles for IPv6 Capable Products"—defines categories of IT equipment and IPv6 requirements for each category, in the form of RFC numbers. Product compliance is administered by the Joint Interoperability Test Command (JITC), a fee-based agency that certifies and maintains a list of IPv6-compliant products that are placed on the Approved Products List (APL). This list is used by the DoD when it issues requests for information and requests for quotes.

The DoD certification will only apply within the U.S. to IT equipment purchased by the DoD and other agencies of the U.S. government. Outside the U.S., the University of New Hampshire (UNH) "IPv6 Ready" program is expected to prevail.

Outside the U.S.: UNH "IPv6 Ready" Program

Outside the U.S., the UNH "IPv6 Ready Logo" program may be used. UNH is a well-known nonprofit organization that offers compliance testing for various aspects of networking, ranging from physical layer to protocol testing. The UNH "IPv6 Ready" program performs compliance testing that is not as stringent as the DoD certification, but ensures that "IPv6 Ready" network software stacks from different vendors are interoperable.

Dell IPv6 Plans

The consensus estimate of when IPv4 will run out of addresses is between 2010 and 2013. At that point, IPv6 will be required to meet the need for new IP addresses. Dell is working to meet the immediate requirements of the DoD and our customers in Asia, as well as longer-term worldwide requirements. In fact, a number of Dell products have already received both JITC and UNH certification.[6]

Dell is committed to delivering IPv6 technologies that enable customers to simplify and secure their IT environments, while optimizing current and future technology investments. Based on customer demand, Dell will strategically release IPv6 technology in specific products, software/firmware, and solutions.

For more information regarding IPv6 support for specific Dell products, contact your dedicated Dell account team.

For More Information

- IPv6 Forum: www.ipv6forum.com
- IPv6 Task Force: www.ipv6tf.org
- University of New Hampshire IPv6 Testing Consortium and IPv6-Ready list: www.iol.unh.edu/services/testing/ipv6
- JITC Approved Products List (APL): http://jitc.fhu.disa.mil/apl/ipv6.html
- IPv6 white paper: http://technet.microsoft.com/en-us/network/bb530961.aspx
- Microsoft FAQ: www.microsoft.com/technet/network/ipv6/ipv6faq.mspx
- U.S. Department of Defense Certification: http://jitc.fhu.disa.mil ✪

[5] See RFC 4224 at www.rfc-editor.org.

[6] See http://www.iol.unh.edu/services/testing/ipv6 and http://jitc.fhu.disa.mil.

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.