A POLYCOM WHITEPAPER

"How Will the Migration from IPv4 to IPv6 Impact Voice and Visual Communication?"

October 2011

BROADCONNECT Telecom
sales@broadconnect.ca
877-228-6616

Introduction

On World IPv6 Day[1] (June 8, 2011), major service providers—including Google, Yahoo!, and Facebook— will turn on Internet Protocol version 6 (IPv6) and for 24 hours they will offer their content over IPv6. While IPv6 implementations started in the 1990s, "World IPv6 Day" is the first global test that is intended to help service providers and vendors prepare for the inevitable migration to IPv6. Why is IPv6 so important to the Internet? And how will the migration to IPv6 affect voice and visual communication?

This paper discusses the shortcomings of the currently used IPv4 protocol and provides the rationale for migration to IPv6. The new protocol is not only a new way to package and transport information over the IP network, it also requires changes in the architecture of the Internet and enterprise intranets. Since real-time applications are very sensitive to changes in the transport mechanism, this paper will focus on the impact of IPv6 on voice and visual communications.

The Business Case for IPv6

IPv6 is a very small portion of the Internet traffic today and, while everyone agrees that more IP addressing space is needed, businesses and service providers have struggled to agree on the business case for IPv6. Businesses are trying to stall by buying address space from other users, and, when Microsoft purchased IPv4 addresses from Nortel[2], they set the price for IPv4 address at $11.25. Governments, including the U.S. Government, have been encouraging IPv6 by making it a mandatory requirement for all new products purchased by government agencies. Since vendors usually do not create separate product lines for government, IPv6 has been implemented in everything from telephones to video endpoints to soft clients. For example, Polycom's video solutions support IPv6, including Polycom® HDX® endpoints and the Polycom RealPresence™ Platform: Polycom RMX® platforms and Polycom CMA® and DMA™ solutions.

It is also extremely urgent for residential and mobile service providers since they are even bigger IP address space users than businesses. The consumer market drives content providers to enable IPv6 in their services (hence World IPv6 Day), which then will drive even more IPv6 adoption in the business community. IPv6 is gradually starting to make business sense.

Living in the IPv4 World

All information on the Internet and on private intranets is carried in IP packets. The packet format was defined in the 1980s and described in the Internet Protocol specification (also referred to as IPv4[3]). When IPv4 was designed, no one really expected that the Internet would become so pervasive and it seemed reasonable to use 32 bits (4 bytes) to address network elements; this resulted in approximately 4.3 billion addresses. Figure 1 depicts the structure of an IPv4 packet.

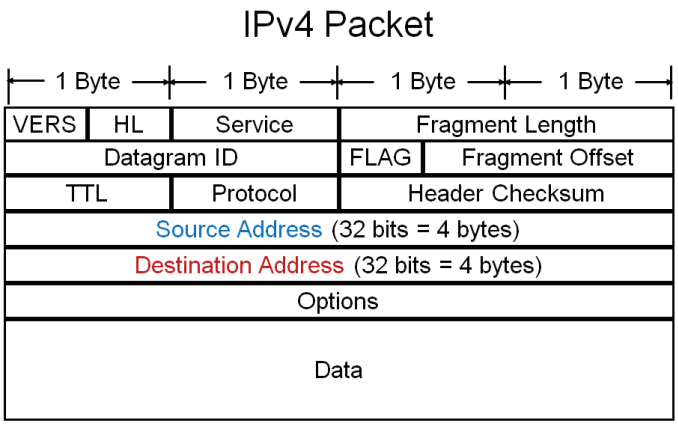

Figure 1: IPv4 Packet

The IP packet consists of a header and data. The header includes the addresses of the sender (source) and the receiver (destination) plus additional information necessary to route the packet over the IP network. The maximum size of the IP packet was set to 65535 bytes which was more than enough for any application at the time. Since the organizations initially using the Internet trusted each other, security was not an important requirement for IPv4, and the protocol itself did not provide any security mechanisms.

In the 1990s, the rapid growth of the Internet led to the first discussions about the design limitations of the IPv4 protocol. The industry was mostly concerned about the small address space and the discussion led to the definition of a new packet protocol (IPv6[4]) that used 128-bit addresses. However, changing the underlying networking protocol requires service providers to upgrade software and hardware, then to reconfigure their networks. No wonder service providers did not rush into implementing IPv6. Instead, service providers used Network Address Translation (NAT) and later double-NAT as work-arounds to overcome the address space shortage. NATs are usually implemented as part of firewalls, and directly impact voice and video communication because they hide the real IP address of the destination. This means that a voice/video device on the Internet cannot just call a device behind a corporate NAT. In addition, business-to-business calls must go through multiple NATs, and this frequently leads to call failures. Even if the call goes through the NAT, real-time application performance takes a hit because NATs makes computationally intensive manipulations on both incoming and outgoing packets, which leads to additional delay.

Another fundamental problem with NATs is that they change the IP address field in the IP packet and this leads to incorrect checksums and encryption failures. In other words, NATs break end-to-end security in IP networks.

Mapping private and public IP addresses (NAT) is one of the three main functions in IPv4 firewalls today. Another function

[1] *http://isoc.org/wp/worldipv6day/*
[2] *http://www.computerworld.com/s/article/9215055/Microsoft_offers_7.5M_for_666_624_IPv4_addresses*
[3] *IETF RFC 791, http://www.ietf.org/rfc/rfc0791.txt?number=791*
[4] *IETF RFC 1883 http://datatracker.ietf.org/doc/rfc1883/ and later RFC 2460, http://www.ietf.org/rfc/rfc2460.txt?number=2460*

is called "stateful firewall function." When packets arrive from the public network, the stateful firewall function determines if there is any outgoing traffic (that is, from the private network to the public network) belonging to the same connection. If there is, it lets inbound traffic into the private network. If not, inbound traffic is blocked and packets are dropped. The third main firewall function (Port Address Translation, or PAT) maps private to public port numbers. This is because IPv4 addresses are scarce and applications often use many different ports in association with a single IP address. The next section describes how the firewall functionality changes with the arrival of IPv6.

The Arrival of IPv6

The pool of available IPv4 addresses has been depleted, yet service providers need unique IP addresses for the home routers, laptops, and other mobile devices their customers are using. The address shortage is bad in Europe and even worse in Asia where China is adding something like 80 million Internet users a year.

IPv6 can immediately alleviate the address shortage. It allocates 128 bits for IPv6 addresses, which results in approximately 340 undecillion (a number with 36 zeros[5]) IP addresses. Figure 2 depicts the structure of an IPv6 packet header with the much larger address fields.

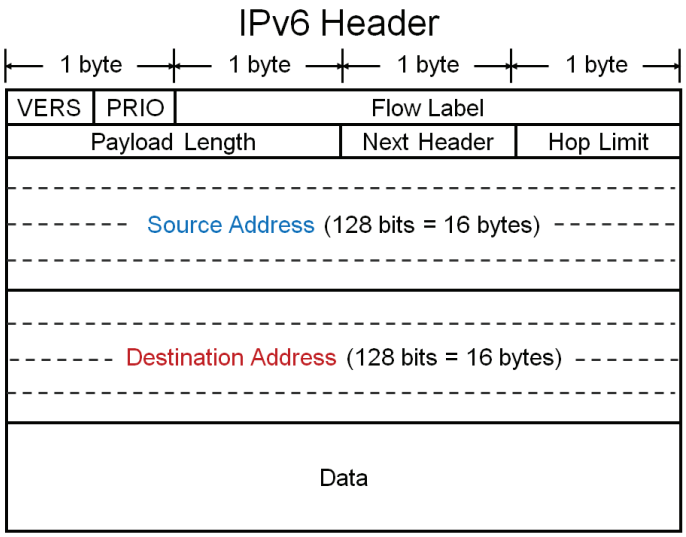

Figure2: IPv6 Packet

Breaking Barriers to Communication

Although the migration to IPv6 is driven by the address shortage, IPv6 brings many new functions that will have impact on real-time applications such as voice and video over IP. Since there will be enough IPv6 addresses for everyone and everything, NATs can be completely removed, and real-time applications would work much better on the Internet.

Some organizations believe that NATs' ability to hide IP addresses of internal IP servers and devices provide security, and these organizations push for retaining NATs in IPv6 networks. However, this argument is flawed since security experts have repeatedly stated that NATs today do not improve security because a hacker can scan the small IPv4 subnets—they usually have just 255 IP addresses each—within seconds, even if they are behind a NAT. Scanning IPv6 subnets in comparison is futile because these subnets are so large that it would take years to find something in the subnet.

Does IPv6 make firewalls obsolete? IPv6 firewalls will be required in the future to perform the stateful firewall function. However, IPv6 firewalls will not need to perform NAT and PAT. PAT is not necessary since the IPv6 address space is big enough to allow applications to keep the original port numbers. NAT is not defined for IPv6, in order to simplify end-to-end communication without interruptions. Note that if a firewall does not support IPv6, it will not recognize an incoming IPv6 Ethernet frame and will not let it through. Several newer firewalls such as Juniper NetScreen and SRX and the Cisco ASA support IPv6, but the vast installed base of firewalls is still lagging behind.

Security

Removing the NAT enhances security by allowing end-to-end security protocols such as IPSEC[6] to efficiently secure the communication in IP networks. IPSEC encrypts the data in the IP packet but allows routers to read and modify IP, TCP, and UDP headers. The IPSEC implementation requires scalable identity management infrastructure that must be deployed in parallel to IPv6/IPSEC, and as result the IPSEC specification will continue to be updated as better identity management infrastructure and encryption key mechanisms are developed.

Many security problems in IPv4 are related to packet fragmentation, which happens when a packet has to be sent through a slower link. The router splits the packet in multiple fragments and sends them as separate IP packets. The receiver must recognize the fragmentation, collect all pieces, and put the original packet together; this process can be susceptible to penetration. IPv6 does not allow packet fragmentation by intermediaries/routers because it requires that oversize packets must be dropped, and an ICMPv6 "Packet Too Big" message be sent to the sender. The sender then reduces the packet size so that it can go across the network in one piece.

Voice and Video Quality

Quality of Service (QoS) mechanisms developed for IPv4 can still be used with IPv6. Although it might seem that real-time applications could face potential increased latencies as a result of the larger address, the new header structure in IPv6 allows faster header parsing which leads to faster packet forwarding in routers. In particular, all optional information is taken out of the base header and transported via header extensions. The impact on real-time communication is positive: voice and video packets will move faster through the IPv6 network. It is only in mixed IPv4-IPv6 environments that latency increase can be expected, due to tunneling and translation delays.

[5] *http://en.wikipedia.org/wiki/Undecillion*
[6] *IETF RFC 4301, http://tools.ietf.org/html/rfc4301*

The new packet structure in IPv6 allows for larger packets with jumbo payload of up to 4 billion bytes[7]. This allows for sending more video information in a single packet, instead of splitting it in multiple packets, which should benefit visual communications, especially as video quality increases and video packets get larger.

However, larger packets lead to higher end-to-end latency, so these large packets are still not suited to live voice and video applications. Larger packets that exceed the so called Maximum Transmission Unit (MTU) on any of the links between sender and receiver must be fragmented, that is, split in smaller packets. As mentioned above, IPv6 does not allow routers to fragment large packets and instead requires them to drop the packet and send an error message back to the sender. Since there is no mechanism to assure the IPv6 packet will go through end-to-end, multiple routers on the path may drop packets and several retransmissions can follow before the IPv6 packet goes through. This, of course, leads to high latency that negatively impacts the user experience on voice and video calls.

On the positive side, IPv6 mandates that all links must handle a datagram size of at least 1280 bytes[8]; this is called the "minimum MTU". (In comparison, IPv4 has minimum MTU of only 576 bytes). If the sender keeps the IPv6 packets below 1280 Bytes, they will always go through the IP network.

Migration to IPv6 – Starting from the Backbone

There are fundamentally three ways to manage the transition from one version of a protocol to another, and this is no different with the migration from IPv4 to IPv6: dual-stack, tunneling, and proxy with translation.

In dual-stack implementations, devices/terminals/endpoints on one side and routers/switches on the other support both IPv4 and IPv6 simultaneously.

With tunneling, if the backbone network already supports IPv6 while attached regional/local networks only support IPv4, tunnels can be built either on the fly or statically (per configuration); these allow IPv4 packets to get encapsulated and transported over the IPv6 backbone, then converted back to IPv4 packets at the destination network.

The third approach of proxying with translation can be deployed when an IPv4-only network wants to communicate to an IPv6-only network. The translation mechanism manipulates the smaller IPv4 addresses to create a corresponding IPv6 address, and a border element performs the mapping between the two formats. In effect, this is a kind of IPv4-to-IPv6 NAT.

Note that just supporting the new IPv6 headers in networking equipment is only a part of supporting IPv6. Several other protocols have been enhanced to support IPv6: the Internet Control Message Protocol (ICMP) v6[9], the SEcure Neighbor Discovery (SEND)[10], the Dynamic Host Configuration Protocol (DHCP) for IPv6[11], the Domain Name System (DNS) for IPv6[12], Open Shortest Path First (OSPF) routing protocol for IPv6[13], and Mobility Support in IPv6[14].

The migration to IPv6 started with network backbones. Due to Polycom's involvement in Internet2, we know that this network already provides IPv6 services to the US Research and Education community through two IPv4-to-IPv6 relay routers. IPv6 support is easy to do for backbones that do not have any end users, and where issues are mostly around carrier-grade NATs and web filters that look into packets and cannot understand IPv6.

While some backbone networks such as CERNET2[15] in China are running only IPv6, many other backbone networks are running dual-stack. From a technology perspective, supporting IPv6 on the backbone is not a problem anymore but work continues on optimizing IPv4-IPv6 translation and tunneling techniques.

The Network Today

Commercial service providers are in different stages of deploying IPv6. Global Crossing, for example, has made a lot of progress, while Level 3 has so far been less aggressive in this area. It is expected that after the acquisition[16] is completed, Level 3's network will be up and running with IPv6.

National/regional/local networks are mostly not running IPv6 yet. However, National Research and Education Networks (NRENs)[17], for example, that connect to Internet2 backbone in the USA and to the GEANT backbone in Europe have time until 2012 to convert to IPv6.

IPv6 Support in the Polycom Solution

The Polycom visual communications solution already supports IPv6. HDX 6000, 7000, and 8000 endpoints have been supporting IPv6 since version 2.5. Since HDX technology is used in all of Polycom's telepresence systems, IPv6 is supported in OTX, RPX, and ATX telepresence solutions.

[7] *IETF RFC 2675, http://www.ietf.org/rfc/rfc2675.txt*
[8] *The value of 1280 was selected to be below the Ethernet max frame size of 1500 Bytes, so that the IPv6 packet can be efficiently transported in a single Ethernet frame. There are also some other considerations around the value of 1280 related to IPv4 -IPv6 tunneling.*
[9] *RFC 4443, http://www.ietf.org/rfc/rfc4443.txt?number=4443*
[10] *RFC 3971, http://www.ietf.org/rfc/rfc3971.txt?number=3971*
[11] *RFC 3315, http://www.ietf.org/rfc/rfc3315.txt?number=3315*
[12] *RFC 4472, http://www.ietf.org/rfc/rfc4472.txt*
[13] *RFC 5340, http://www.ietf.org/rfc/rfc5340.txt?number=5340*
[14] *RFC 3775, http://www.ietf.org/rfc/rfc3775.txt?number=3775*
[15] *http://www.cernet2.edu.cn/index_en.htm*
[16] *http://www.level3.com/en/About-Us/Newsroom/Press-Release-Archive/2011/2011-04-11-globalcrossing.aspx*
[17] *http://en.wikipedia.org/wiki/National_research_and_education_network*

In the Polycom RealPresence™ Platform, RMX1500, 2000, and 4000 media platforms support IPv6 and can be configured for IPv6-only, IPv4-only, or for dual stack IPv6-IPv4, which means that both IP protocol versions run simultaneously. IPv6 addresses can be used to address external entities such as H.323 gatekeepers, SIP proxies, DNS Servers, and Default Routers, as well as defined participants. Less visibly to the end user, IPv6 can be used to address internal RMX components within the RMX chassis, for example, the control unit, the signaling host, the shelf management, and the media cards[18].

The DMA 7000 solution supports IPv6 on all key interfaces—to the RMX solution, to the gatekeeper (the CMA solution), on the management interface, as well as for connections to DNS, Microsoft Active Directory, and other servers in the network. Finally, CMA 4000 and 5000 solutions supports IPv6 in "maximum security mode" that is required for JITC compliance.

Conclusion

The migration to IPv6 is inevitable but it will not happen fast. Network backbones will support IPv6 first, followed by mobile and residential service providers that are running out of IPv4 addresses. From the private networks, government and education will lead the way with businesses following them.

June 8, 2011 is the next in a series of practical steps to take the Internet and other IP networks to a future unbounded by space limitations, a future where everything can have its own unique IP address.

[18] *IPv6 is supported with MPM+ and MPMx media cards*

Acknowledgements

I would like to thank my colleagues Jeff Rodman, Alex McCarthy, Jeff Adams, Assaf Weissblat, and Andre Reid for their contributions to this work.

About the Author

Stefan Karapetkov is Emerging Technologies Director at Polycom, Inc. where he focuses on the visual communications market and technology. He has MBA from Santa Clara University (USA) and an MS degree in Engineering from the University of Chemnitz (Germany). He has spent more than 15 years in product management, new technology development, and product definition. His blog is http://videonetworker.blogspot.com/.

About Polycom

Polycom is the global leader in standards-based unified communications (UC) solutions for telepresence, video, and voice powered by the Polycom® RealPresence™ Platform. The RealPresence Platform interoperates with the broadest range of business, mobile, and social applications and devices. More than 400,000 organizations trust Polycom solutions to collaborate and meet face-to-face from any location for more productive and effective engagement with colleagues, partners, customers, and prospects. Polycom, together with its broad partner ecosystem, provides customers with the best TCO, scalability, and security—on-premises, hosted, or cloud delivered.

For more information, visit www.polycom.com, call 1-800-POLYCOM, or contact your Polycom sales representative.

Polycom Worldwide Headquarters
4750 Willow Road, Pleasanton, CA 94588
1.800.POLYCOM or +1.925.924.6000
www.polycom.com

POLYCOM®