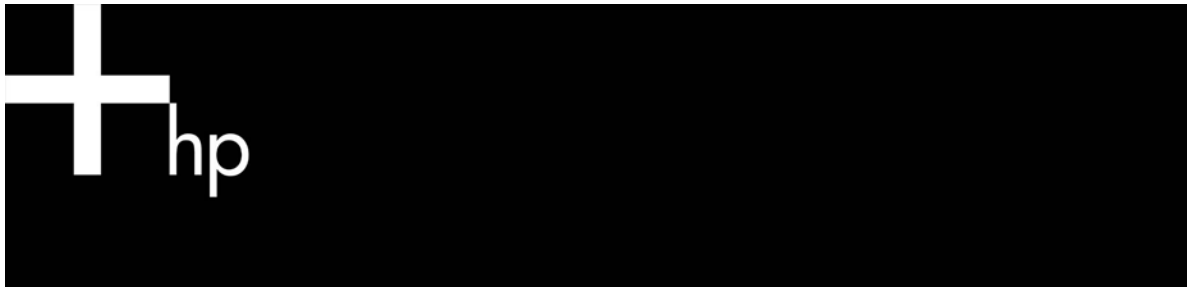
IPv6 – The evolution of the Internet



IPv6 – The evolution of the Internet

The unprecedented growth of the Internet is forcing an evolution of one of its most significant technology enablers, the TCP/IP protocol suite.

The current version of the Internet protocol (IPv4) has become inadequate because the Internet's explosive growth has rapidly depleted the available address space, forcing many organizations to resort to complex addressing schemes simply to connect to the Internet. Internet growth is also challenging current paradigms on ease of use and administration complexity. As expansion continues, the need for a new model that can scale with growth becomes more and more critical.

In addition, the Internet is evolving rapidly toward the use of wireless mobile devices that have to communicate with other mobile and stationary devices. The need for end-to-end security is more and more pressing as more content is communicated over the Internet. New technologies, like Wi-Fi, next-generation mobile terminals, network appliances, sensors, always-on devices, and so forth, require large numbers of IP addresses.

IPv4 has been both an agent of change and a barrier to growth. Although it has served the needs of many technologies, companies and individuals very well, IPv4 is not able to deliver the network technology necessary to support the next generation of the Internet.

Why can't IPv4 support the Internet's rapid expansion and the demand for enhanced services? There is an engineering limit to the amount of hacks and "band-aids" that can be applied just to keep TCP/IP running. These requirements are driving the development of the 'killer application' for the replacement of IPv4.

Internet protocol, version 6 (IPv6), standardized by the IETF (Internet Engineering Task Force) in 1998, is the next-generation Internet protocol. With its addressing capabilities, scalability, security features, ease-of-configuration, and network management capabilities, IPv6 is of vital importance to both consumers and businesses.

This new technology suite will be adopted by the market only if it can be integrated with the existing IPv4 infrastructure without significant disruption to services. Because there are millions of existing IPv4 network nodes, IPv4 and IPv6 protocols will continue to coexist for many years. IPv6 was carefully designed to ensure that hosts and routers can be upgraded incrementally, reducing interruptions of network service.

IPv6 advantages

IPv6 makes mobile Internet connections possible anywhere, any time, any way. It's not simply a new address format; it's a "smarter packet" as well. This allows IPv6 to provide increased functionality in such commercially important areas as security and network maintenance, as well as opening the door to new services such as Voice over IP (VoIP), audio and video conferencing, and gaming.

An IPv6 node can communicate with other nodes on the same IPv6 link without the use of servers or routers. IPv6 supports a stateless node discovery paradigm that provides the ability to discover the presence of nodes, routers, and the Link Configuration Parameters on the network. Node discovery is the first step in allowing a node to obtain an address using IPv6 Address Autoconfiguration.

An IPv6 host listens for Router Advertisements that indicate whether to use a stateless or stateful method for address assignment. If the host is instructed to use stateless address configuration, it uses the router prefixes announced in the form of IPv6 addresses. On the other hand, if the host is instructed to use stateful address configuration, then Dynamic Host Configuration Protocol (DHCPv6) is used to configure IPv6 addresses.

Of course, users are not aware of all the IPv6 advantages for network communications, but they will benefit from the new and improved set of mechanisms for Node Discovery and Address Autoconfiguration, which are far more robust and efficient than using the current IPv4 protocol.

Security, a crucial requirement for modern e-commerce, was not as great a priority when IPv4 was being developed. IPv4 servers often cannot determine whether packets are being received from a legitimate end node. Source address masquerading, or "spoofing," can be used to acquire confidential data or to gain control of a server. Solutions like firewalls combat these challenges but hinder connectivity at the same time.

Authentication, security encryption, and data integrity safeguards are an integral part of the IPv6 protocol, accomplished by using the IP Security Protocol (IPSEC) architecture. The IPv6 authentication header extension assures that a packet is truly from its source address. End-to-end encryption at the network layer is provided by another standard header extension; the packet itself is never touched.

IPv6 also advances the art of multicasting. This is important because of the increasing demand for streaming audio, video, and animated content. The improved address defines a large multicast address space, thereby limiting the degree to which multicast routing information must be carried throughout an enterprise. And IPv6 also introduces the concept of "anycast" services, whereby a group of nodes can be designated as an anycast group. A packet addressed to an anycast group's address is delivered to only one of the nodes.

IPv6 does not require Network Address Translation (NAT) for communications or deployment. This means that end-to-end solutions, including security, can be deployed today without NAT.

Going new places with IPv6

The distinctive hallmark of 21st century communications is mobility. Mobile voice services have already transformed business and personal interactions. But the full potential of mobile communications will not be realized until this capability is extended to data. Seamless mobility is being taken to the Internet, representing the true mobile communications revolution. Exciting waves of mobile communications products and services have been made possible by the revolutionary new network-layer protocol IPv6.

The problems with mobile Internet access today

When the Internet was first developed, it was intended to be a data-sharing network for the military and for research facilities. No one foresaw its growth as a communications powerhouse, and mobility was merely a concept. There was no need to distinguish between who you were and where you were connected to; it was assumed that they were one and the same. There is no information in the IPv4 address that indicates a new geographic point of attachment.

Although today's users have portable networking capability, it is far from ideal. The correct delivery of packets requires a new IP address for each new point of attachment. To establish a new connection, whether one moves 100 feet or 1,000 miles, requires a new point of attachment. As you probably know, connecting to the Internet from different locations can be a frustrating and costly exercise.

Mobility using IPv4 requires informing any agent in the routing process about a new location, necessitating additional infrastructure that is not always deployed in IPv4 nodes. The system has to be configured with a new address, a correct network mask, and a new default router every time the user establishes a connection from a new location. Consequently, the benefits you might realize from having mobile Internet access can be dissipated by the hardships required to attain that very access. Today's time-pressed consumers expect and demand a better solution.

The advantages of Mobile IPv6: Reaching the Net anywhere, any time, any way

With Mobile IPv6, location is no longer an issue when connecting to the Internet. The mobile node sends information about its point of attachment to a home agent, a node on the home network that allows the mobile node to be reachable at its home address regardless of its actual geographic location. Packets addressed to the mobile node are intercepted by the home agent and tunneled directly to the mobile node's current location.

Each IPv6 mobile node has two addresses: a home address and a care-of address. The care-of address is created whenever the mobile node changes its point of attachment to the Internet. Security between the mobile node and home agent can be accomplished using the IP Security Protocol (IPSEC).

Route optimization, provided by the Return Routability (RR) procedure within the Mobile IPv6 protocol, allows data to be sent directly from a correspondent node to the mobile node. The correspondent node communicates with the mobile node using common applications like e-mail, instant messaging, and streaming audio or video.

When the mobile node sends packets to another node, its care-of address is set as the source address, and a destination home address is included. This preserves the end-to-end model of TCP/IP, allowing mobility without interrupting the open connection.

Mobile IPv6 takes advantage of the extensibility of the IPv6 protocol by defining new Neighbor Discovery Messages and Types, the Routing Header, and the use of the Destination Option process specified in an IPv6 packet.

For mobile users, location need no longer be an obstacle when connecting to the Internet. The reduced costs in time and infrastructure will certainly spur greater use of these types of Mobile IPv6 connections.

The advantages of IPv6 and Mobile IPv6: pervasive deployment

Imagine that you are a doctor. You are making your rounds at different hospitals, which are in different towns. You need to update patient records and solicit input from specialists rapidly. You need access to centralized patient information and research databases from any place in the hospital or medical campus. You don't know it, but you need IPv6 and Mobile IPv6.

Mobile IPv6 permits users to remain connected across wireline (Ethernet, xDSL) and wireless (802.11, Cellular, Satellite) networks while roaming from one network to the next. With IPv6, mobile nodes can discover each other and form IPv6 addresses to communicate on a Wi-Fi (802.11) network using IPv6 Neighbor Discovery and Stateless Autoconfiguration.

These advantages permit a doctor to stay connected in route to the hospital from home, rather than shutting down his PDA/laptop at home, and reconnecting at the Wi-Fi location at the hospital. There is no doubt that mobility has become a way of life.

There are two components to security for Wi-Fi: one assures the privacy of the data transmitted over the network; the other protects the network itself against intrusion. Standards for securing the data link access include IEEE 802.11i and Wi-Fi protected access (WPA). The Authentication Authorization (AAA) protocol permits user authentication in an 802.11 network. Once authenticated, the node can then use IPSEC to further authenticate or encrypt their packets, providing two levels of security.

Using Mobile IPv6, the mobile node remains connected to a Provider Regional or local 802.11 network. In a manner similar to the way cellular networks maintain information about clients today with Home and Visitor Location Registers, AAA supports a distributed network of AAA servers and clients that maintain AAA information about clients. The integration of Mobile IPv6 and AAA for IPv6 provides a robust solution that can be deployed today. The Provider Regional or Local Mobility Manager act as an exchange point as mobile nodes roam within the provider region (such as the metropolis, campus, or global Information grid), or the locally connected network (the mall, a building, or an ad hoc network).

For the communications industry, Mobile IPv6 indeed means "going new places."

IPv6 timetable

HP believes, and the historical development of the Internet confirms, that consumers will not just want more and better products and services, but that they'll want to access these benefits as conveniently as possible. Until now in the computing world, that has required us to tailor information and devices. Important as those steps have been, the next advance is even more impressive: making the instant information of the Internet available in a way that addresses today's mobile work and lifestyle demands.

The time to prepare for this new world is now.

Some day, IPv6 will be as commonplace as is mobile telephony today, but the transition won't happen over night. Many upgraded hosts and routers will require backward compatibility with IPv4 devices for many years. You can expect to live in a world where IPv4 and IPv6 coexist for at least another decade. IPv6 was designed with such a transition in mind.

However, the global benefits of IPv6 will only be realized when IPv6 is the dominant protocol. In essence, the Internet is like a chain; its strength is determined by its weakest link.

Many factors are working in favor of IPv6's ascendance, the lack of IP addresses in developing and emerging economies, the increasing popularity of wireless communications, the increased dependence on the Internet as a source of information, the need for anywhere, any time, any way access and the natural progression toward convergence. All of these forces predict a bright future for IPv6.

HP and IPv6

HP has been a key designer and implementer of IPv6 since 1995, and was a member of the IETF Internet Protocol Next Generation Directorate that selected IPv6 as the next-generation Internet protocol. One of the original founders of the IPv6 Forum, HP chairs the IPv6 Forum Technical Directorate and the North American IPv6 Task Force. HP knows that IPv6 will help the Internet to evolve to support the connectivity of more devices and people at a scale far beyond the dreams of creators of the Internet, even beyond the way it exists now, where devices are pervasive and ubiquitous, and people are mobile. (See www.hp.com/network/ipv6.)

IPv6 products are delivered on all HP business-critical server platforms (HP-UX, Tru64 UNIX®, OpenVMS, NSK, Linux and Microsoft®) and the HP OpenView network management platform. Additional functionality for IPv6 will continue to be delivered across its product line, from access devices to printers to managed services.

To enable the adoption of dual IPv4 and IPv6 solutions, HP has implemented the core IPv6 IETF standards specifications and a set of transition mechanisms. HP has successfully participated in North America's largest IPv6 network pilot deployed called Moonv6.

HP Services is evaluating the services portfolio plans for 2004 and beyond. Initial plans are to focus on customer training, pilot testing and interoperability support, application audits, porting and migration strategies, and IPv6 transition and migration consulting services.

Plans for 2005 and beyond are to expand the services portfolio to offer application development, porting and migration, network architecture and design, network integration, configuration and deployment, network management and network support, and expanded customer training.

IPv6 transition and migration consulting services are targeted to help customers understand and analyze the requirements of IPv6, to assess how IPv6 will impact customer's current environment and services offered, and to provide recommendations for the transition to IPv6 and co-existence of IPv4/IPv6.

HP is committed to supporting the development of IPv6 and Mobile IPv6. The HP product portfolio continues to expand, covering today and tomorrow's needs, from the development of consumer devices and networking infrastructure to the support of back-end billing and customer care. HP is partnering with leading-edge solutions providers to create an exciting new world of communications where infrastructure solutions are integrated with end-user devices, and packaged IPv6 solutions are provided to the market.

For HP and its customers, anywhere, any time, any way IPv6 is no longer a vision; it's today's mandate.

For more information

www.hp.com/network/ipv6

XXXX-XXXXEN, 12/2004