

IPv6: The Future of Networking and Communication for Embedded Devices

The next-generation Internet Protocol, IPv6, will dramatically increase the available number of IP addresses and enable efficient and secure peer-to-peer communication.

by Roger Boden
Interpeak

The kind of communication that will be enabled by the advent of IPv6 will be particularly useful in the embedded systems arena, as millions of new devices take advantage of Internet connectivity. Although IPv6 has been in the works for several years, there continues to be debate about its value. Many people and companies must answer the question: "IPv4 is working, and if it ain't broke, why fix it?" But there are many ways in which IPv4 is *not* working, and there are good reasons why the migration of IPv6 is not only desirable, but necessary.

Traditionally, only desktop computers and servers have been connected to the Internet. Individuals have relied upon their computers as gateways to the Internet, and only recently have people begun to rely on mobile computers and hand-held devices for online services and capabilities. Today's consumers are seeing a proliferation of devices with Internet connectivity, such as PDAs, mobile phones and even automobiles. The world is on the cusp of a time when many other devices will be connected: household appliances, burglar alarms, toys, watches and more. Internet usage will

leap from one or two devices per household to possibly several dozen.

The current Internet Protocol, IPv4, was designed in the 1970s and had one major objective: to offer ample IP addresses for computers to connect to the Internet. With 32-bit addressing, IPv4

allows a maximum of roughly four billion addresses. Such a number of addresses seemed like plenty in the 1970s, when bandwidth was limited and many people did not even know about the Internet. However, the 32-bit address length ended up allowing fewer addresses than planned.

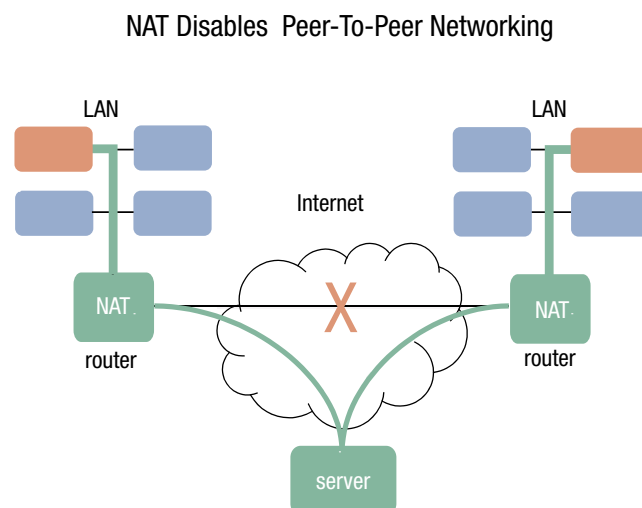


Figure 1 Peer-to-peer connections are often too complicated to set up in systems using NAT gateways. As devices proliferate, the difficulty only increases. This limitation is eliminated with IPv6, which does not require the NAT protocol to overcome the limits of available IP addresses.

More importantly for today's world, the uneven distribution of IPv4 addresses (with the U.S. using about 75% of the available IPv4 address space) has resulted in a dearth of addresses for Asia and other regions. Finally, the extraordinary leap in the number of devices that can now be connected to the Internet means that IPv4's limited address space will not allow every device a unique IP address.

Enter Network Address Translation

So far, network address translation (NAT) has taken care of the problem of limited address space by enabling the use of thousands of computers and devices to share a single unique IP address for access to the global Internet. Today, many gateways and firewalls are using NAT to establish an internal private network and enable the nodes on that network to communicate with the Internet. In fact, an enormous problem has been solved, and millions of networks are able to communicate over the Internet within the limitations of IPv4.

However, the evolution of the Internet and the proliferation of devices create several problems for an infrastructure that depends on NAT (Figure 1). Most notably, many devices will require peer-to-peer communication. For example, many mobile devices now include gaming, video and other applications that require an IP connection between two or more mobile devices. If such devices are hidden behind NAT gateways and do not have their own unique IP addresses, the following difficulties will arise:

- Applications will be complex to develop, as they will have to account for the numerous steps one device must take to communicate with another.
- IPsec, the Internet security protocol that will accompany IPv6 (and which we discuss below) does not work with NAT.
- The routing of IP packets will become increasingly complex as the number of devices proliferate and become more mobile.

Call for IPv6

By the early 1990s, it was clear that IPv4 was not a long-term protocol. Its design did not anticipate a number of requirements that turned out to be crucial. Such requirements not only pertained to the proliferation of devices, but also the need for additional security, simpler configuration and better prioritization of some services, such as real-time services (often referred to as Quality of Service issues).

IPv6 will remove any concern about the limitation of IP addresses. IPv6 uses 128-bit addresses, versus the 32-bit addresses used by IPv4. Compared to the total possible number of IPv4 addresses, 4.29 billion, IPv6 provides nearly 600 quadrillion addresses for every square millimeter on earth. That's 6×10^{23} addresses for every square meter of the earth's surface.

When each device has its own unique global IP address and NAT is no longer necessary, peer-to-peer communication will become much easier. Two devices will be able to establish direct communication without the need to translate between global and private addresses. Two-way applications such as IP telephony, video conferencing and gaming will be much simpler to develop. Routing tables will become far less complex, which will enable higher performance for Internet traffic and more bandwidth for additional communication.

Security – Greater or Fewer Risks?

The elimination of NAT, the enabling of peer-to-peer communication, the emergence of numerous new applications and the connection of billions of new devices are all advantages associated with IPv6. Yet such advantages raise serious questions about security: will tomorrow's Internet, with so many more individuals and devices communicating, be as safe as today's Internet? No. It will be safer!

IPv6 comes with its own security protocol, IPsec. Standardized by the Internet Engineering Task Force (IETF) for IPv6, IPsec is optional for IPv4 systems but mandatory for IPv6-specified systems. The security offered by IPsec comes into play

at the IP layer of the TCP/IP stack. Therefore, because IPsec is applied at such a deep or "low" level, there is inherent protection for all higher-level protocols, such as TCP, http, proprietary application protocols, etc.

IPsec provides several security services, including encryption, authentication, integrity and replay protection. In addition, IPsec allows the encryption of only particular application protocols while others are simply authenticated. Furthermore, one can also specify that communication toward specific IP addresses will be protected, whereas unprotected communication can be used for other destination IP addresses. The flexibility and transparency of the IPsec protocol makes it possible to tailor a security configuration for every need. Yet certain aspects of IPsec, such as using an Authentication Header and the Internet Key Exchange (IKE), are incompatible with NAT—another reason to move toward IPv6 and reduce (eventually eliminate) the use of NAT gateways.

In fact, one of the reasons many people are eager for the implementation of IPv6 is because of its security aspects. In his keynote speech at the 2003 North American IPv6 Global Summit last June, John Osterholz, Director of Architecture and Interoperability for the Department of Defense (DoD), noted the security advantage that IPv6 has compared to IPv4. "Our soldiers need better information in order to make better decisions. The lack of security and flexibility in the current IPv4 protocol is a drag on our wing. This isn't about do you trust the Internet for your kid's homework, it's do you trust your kid's life. If we fail, people die."

Quality of Service

Tomorrow's Internet will carry real-time traffic such as voice and video in addition to the multiple uses it serves today. IPv6 addresses the technical issues necessary to allow enough bandwidth for different applications and services, including voice and video. This capability, called quality of service (QoS), allows IPv6 routers to recognize certain types of traffic and give each type a specific

IPsec – Securing the Peer-To-Peer Connection

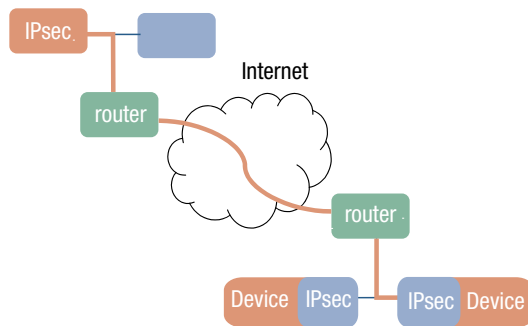


Figure 2 IPsec secures the entire peer-to-peer connection, protecting data in all parts of the transfer. This enables the use of non-secure networks like the Internet for the transfer of confidential data.

amount of the available bandwidth. In this model, real-time traffic will command a higher priority than all other traffic. This addresses the quality of service issue for voice and video, ensuring that these services are relegated to highest-bandwidth networks in a manner that isn't possible with IPv4. Unlike Y2K, IPv6 does not impose a specific deadline. Rather, IPv6 was designed to have a gradual, and therefore not disruptive, implementation.

As organizations upgrade equipment, they should do so with IPv6-capable products. The Department of Defense (DoD), for example, announced its transition strategy in June 2003. In order to minimize future transition costs, the DoD adopted a policy that requires all purchases made after October 2003 to be IPv4- and IPv6-capable. Director John Osterholz expects the department to be fully IPv6-compliant by 2008.

The North American IPv6 Task Force notes that a long transition is evidenced by the fact that vendors began to ship commercial IPv6 products in 2000, yet the DoD won't be fully IPv6-compliant until 2008.

For the public sector, we can expect that for the foreseeable future, most manufacturers will produce systems supporting both IPv4 and IPv6, so that if connections are not possible using IPv6 they can fall back and succeed using IPv4 (providing IPv4 connectivity existed prior to the introduction of IPv6).

Although this approach has advantages, it creates a bit of a chicken and egg dilemma. Which comes first, the user, the application or the product? A recent Reuters article cites Japanese operators

experiencing a number of challenges related to the lack of a "drop-dead" date:

- Operators are reluctant to offer IPv6 services until there is a stronger base of users and applications.
- Consumer product manufacturers are concerned that the network coverage and client base are not yet adequate enough to support IPv6-compatible products.
- Users will not demand IPv6-compatible products until the price is right and the market requires it.

Compaq Computer Corp., in its white paper "A Key Building Block for Next-Generation Networks," notes that "Compaq believes IPv6 deployment will occur in stages. The first stage will be deployment of regional IPv6 networks. Subsequent stages will see the development and deployment of additional products and services that build on the advanced features of the new infrastructure. The final stage will result in the migration of the national and global IPv4 infrastructure to IPv6."

The success of IPv6 requires a global effort. If suppliers in certain countries do not produce dually compatible products, the migration will be incomplete. Dr. Vinton Cerf, co-designer of the TCP/IP protocol, states "The value of IPv6 can be realized only if the deployment effort is broadly based on a global scale. Part of the IPv6 Task Force effort needs to be devoted to fostering IPv6 understanding wherever the Internet has gone, and beyond that to places where it can go with the help of the much-expanded IPv6 address space."

IPv6 task forces span the globe from the United States to China. A list of all the task forces includes groups in Japan, Europe, Korea, India, Taiwan, Iran, Brazil and Asia Pacific.

We have grown accustomed to connecting desktop computers to the Internet. Now we will see embedded systems taking advantage of the Internet in new ways. By removing the limitation of IP addresses, IPv6 will enable a large number of new types of devices and applications to benefit from the Internet. Many embedded systems will have their own IP addresses, thus eliminating the need for NAT. This will enable direct peer-to-peer communication, and it will also enable unprecedented security with IPsec. While many companies will focus on creating new devices for the IPv6 world, some are already focused on creating the software that will enable these devices to best operate—and interoperate—using both IPv6 and IPv4. Those of us working in this area are already seeing giant steps in security, ease-of-use and quality of service as real-time traffic such as voice and video are able to take advantage of the appropriate bandwidth. ▲

Interpeak
Stockholm, Sweden.
+46 8 545 275 80.
[www.interpeak.com].