ITL BULLETIN FOR JANUARY 2011

INTERNET PROTOCOL VERSION 6 (IPv6): NIST GUIDELINES HELP ORGANIZATIONS MANAGE THE SECURE DEPLOYMENT OF THE NEW NETWORK PROTOCOL

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Internet Protocol version 6 (IPv6) is a new network protocol with updated capabilities and features that will support the expected future growth of the Internet. The Internet Protocol (IP) controls the transfer of information from one device to another over the Internet through the management of specific, unique network addresses. The information being sent is split into manageable packets; each packet has its own header that contains the sender's address, destination address, and other information to guide the packet through the Internet over many different paths. When the packets arrive at their destination, they are reassembled into their original form.

Because of the limitations on the address sizes that are available for the current network protocol (IPv4), the Internet will soon be running out of globally unique addresses. IPv6 significantly upgrades the services supported by IPv4, which has been in use since the 1980s. The enhanced capacity of IPv6 is expected to provide sufficient addresses to meet future world demand for IP addresses, and to provide improved, more efficient services, mobility, and security; these improvements will be necessary as the Internet expands to serve many new users.

Federal government organizations have started planning for the deployment of IPv6. The Office of Management and Budget (OMB), in its Memorandum for Chief Information Officers of Executive Departments and Agencies (September 2010), said that the federal government "is committed to the operational deployment and use of Internet Protocol version 6 (IPv6)." OMB described specific steps that agencies must take to expedite the deployment process. To assist federal organizations in this process, the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) developed a guide that explains the technical features, benefits, and potential security risks to be considered when organizations are planning for their deployment of IPv6.

NIST Special Publication (SP) 800-119, *Guidelines for the Secure Deployment of IPv6*

NIST's new guide, SP 800-119, *Guidelines for the Secure Deployment of IPv6,* describes and analyzes the new and expanded protocols, services, and capabilities that IPv6 provides, and advises organizations about the security issues and deployment strategies to be considered when planning the move to the implementation of IPv6.

Written by Sheila Frankel of NIST, Richard Graveman of RFG Security, John Pearce of Booz Allen Hamilton, and Mark Rooks of L-1 Identity Solutions (formerly of Booz Allen Hamilton), the guide examines the differences between IPv4 and IPv6, the security issues to be addressed, and other issues that might affect the future use of IPv6. The guidelines detail the IPv6 deployment process, including transition, integration, configuration, and testing. NIST SP 800-119 emphasizes that detailed planning will enable an organization to handle the deployment process smoothly and securely.

Figures and tables of information throughout the guide help the user to compare the significant features of IPv6 and IPv4. The major characteristics of IPv6 are described and summarized. The appendices to the publication include acronyms and abbreviations lists, and a list of references and other IPv6 resources. NIST SP 800-119 is available from the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html.

Why IPv6 is Needed for Networked Systems

IPv4 was developed in the 1970s and early 1980s for use in government and academic communities in the United States to facilitate communication and information sharing through information technology (IT) networks. Today the demand for networking services, including Web access, email, peer-to-peer services, and the use of mobile devices, has grown well beyond the expectations of the early network developers. IPv4 was designed to provide a 32-bit space for network addresses, which accommodated more than 4 billion addresses. As a result of the widespread deployment and growth of networking technologies and mobile communications, the IPv4 address space is no longer adequate to provide a sufficient number of globally unique addresses that will be needed in the future.

Technologies had been designed to overcome the limitations on address space. For example, network address translation (NAT) technology allows organizations to connect with the Internet but assign private addresses within the organization. However, these techniques have limitations since they may not be scalable; there can also be interoperability issues with other forms of NAT, as well as with other protocols and applications.

Another limitation of IPv4 is its design that favors interoperability over security and that does not contain features to protect the confidentiality, integrity, or availability of information. IPv4 did not originally support the use of cryptography to protect information from eavesdropping or unauthorized change, and did not provide for the authentication of network users. The open, multi-path character of IPv4 made networks vulnerable to threats and attacks.

Efforts to develop a successor to IPv4 started in the early 1990s within the Internet Engineering Task Force (IETF), a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF efforts focused

on solving the address space limitations of IPv4, as well as providing additional functionality and security for the Internet Protocol.

Major Features of IPv6

IPv6 is a protocol designed to handle the growth rate of the Internet and the demanding requirements of services, mobility, and end-to-end security for network communications. Major features include:

· IPv6 provides for **extended network address** sizes of 128 bits, a substantial increase over the 32-bits address sizes that are available with IPv4. This increased size allows for trillions of globally unique addresses that could be assigned to handle future needs for transmission of data, voice, and video services.

· IPv6 enables plug-and-play networking, or **autoconfiguration**, which allows devices to configure themselves independently using a stateless protocol and to configure their IP addresses and other parameters without the need for a server. Also, the time and effort required to renumber a network by replacing an old prefix with a new prefix are reduced.

· IPv6 provides a **simpler header structure** than the IPv4 header structure, allowing for improved and faster processing of packets and for protocol flexibility.

· IPv6 contains methods for **extension options,** including hop-by-hop option header, routing header, fragment header, destination options header, authentication header, and encapsulating security payload (ESP) header. These options promote improved processing and avoid some security problems.

· IPv6 supports **IP security (IPsec)**, a suite of protocols that can be used to secure IP communications by authenticating the sender, providing integrity protection, and providing for optional protection of the confidentiality of transmitted information.

· IPv6 includes **Mobile IPv6** (MIPv6), an enhanced protocol supporting roaming for a mobile node to enable the node to move from one network to another without losing IP-layer connectivity. This feature, however, introduces security concerns; operations such as route optimization will require that data transmitted between the home agent and the mobile node be appropriately protected.

· IPv6 provides **Quality of Service** options that can be used to implement policy-based networking choices to prioritize the delivery of information. This feature is still under development and could impact security considerations.

· IPv6 incorporates a hierarchal addressing structure and has a simplified header allowing for **improved routing of information** from a source to a destination. The large amount of address space enables organizations with many connections to obtain blocks of contiguous address space and to aggregate addresses under one prefix for identification on the Internet, reducing the amount of information routers must maintain and store.

· IPv6 packet fragmentation control occurs at the IPv6 source host, using the Path Maximum Transmission Unit (PMTU) Discovery procedure. This procedure eliminates the need for routers to perform fragmentation and provides for **efficient transmission** of information.

Security Issues to be Considered in the Deployment of IPv6

General risks to be considered in the deployment of IPv6 include:

· The **attacker community** is taking advantage of IPv6 and is developing techniques and tools for exploitation. If an organization's security controls are not already monitoring for IPv6 traffic, the traffic to and from client devices may not be detectable by existing security controls. This risk can be mitigated by reconfiguring or deploying security controls to be both IPv4- and IPv6-aware.

· The **unauthorized deployment** of IPv6 on existing IPv4 production networks exposes organizations to vulnerabilities that may be difficult to detect or mitigate. IPv6 support is available for most operating systems. The commands to enable IPv6 on these operating systems are easily accessible and user-friendly. As a result, IPv6 may be enabled by default.

· IPv6 includes the **vulnerabilities** that are inherent in any new or revised system. The inclusion of IPsec in IPv6 adds mechanisms for protecting the confidentiality and integrity of information. However, IPv6 does not address attacks that target other network layer communications, such as sniffing traffic, traffic flooding, man-in-the-middle attacks, rogue devices, or Address Resolution Protocol (ARP) table overflow attacks. Some of these attacks are dealt with partially in IPv6 while other attacks, similar in nature, exploit different features.

· Organizations may deploy IPv6, but continue to support IPv4 for legacy applications, services, and clients. This will result in a **dual protocol environment and increased complexity**. The use of two protocols can cause more problems and require more complex configurations to install new equipment or to change existing equipment. Attacks against upper-layer protocols could use either the IPv4 or IPv6 stack to reach the client.

· **Perceived risks** associated with IPv6 may cause an organization to delay deployment despite the fact that IPv6-enabled equipment is already available. General security concepts are the same for the deployment of both IPv4 and IPv6. Organizations will need time to acquire the level of operational experience and practical deployment solutions for IPv6, as they have developed for IPv4 over the years.

· Many vendors, including suppliers of security devices, are waiting for customer demand before implementing support for IPv6, while customers are **waiting for vendors to support IPv6** before purchasing software and systems. Some vendors fully support IPv6,

but many offer only limited support. The many elements that compose the networking environment may delay the development of IPv6 products.

NIST Recommendations for the Secure Deployment of IPv6

The migration to IPv6 services is necessary since the IPv4 address space is almost exhausted. This means that organizations that need new IP addresses will be assigned only IPv6 addresses. Thus, organizations that already have sufficient IPv4 addresses will still have to be able to communicate with organizations that have only IPv6 addresses. Organizations should begin now to understand the risks of deploying IPv6, as well as the strategies needed to mitigate the risks. Detailed planning will enable an organization to move smoothly and securely to the deployment of IPv6 and to maintain connectivity with Internet users throughout the world.

Federal agencies will most likely face security challenges throughout the deployment process, including:

· An attacker community that may have more experience and comfort with IPv6 than an organization in the early stages of deployment;

· Difficulty in detecting unknown or unauthorized IPv6 assets on existing IPv4 production networks;

· Added complexity while operating IPv4 and IPv6 in parallel;

· Lack of IPv6 maturity in security products when compared to IPv4 capabilities; and

· Proliferation of transition-driven IPv6 (or IPv4) tunnels, which complicate defenses at network boundaries even if properly authorized, and which can completely circumvent those defenses if unauthorized (e.g., host-based tunnels initiated by end users).

Organizations planning the deployment of IPv6 should consider the following during the planning process:

· IPv6 is a new protocol that is not backward-compatible with IPv4. This will require organizations to change their network infrastructure and systems to deploy IPv6;

· In most cases, IPv4 will still be a component of the information technology infrastructure. Even after the deployment of IPv6, organizations will require mechanisms for the coexistence of IPv6 and IPv4 implementations;

· IPv6 can be deployed as securely as IPv4; organizations should expect that vulnerabilities within the protocol, as well as implementation errors and lack of operational experience, will lead to an initial increase in IPv6-based vulnerabilities; and

· IPv6 has already been deployed and is currently in operation in large networks globally.

To overcome possible obstacles associated with deploying IPv6, organizations should consider the following recommendations:

· Encourage staff members to increase their knowledge of IPv6 to a level comparable with their current understanding of IPv4;

· Plan a phased IPv6 deployment utilizing appropriate transition mechanisms to support business needs; don’t deploy more transition mechanisms than necessary; and

· Plan for a long transition period with the coexistence of dual systems supporting both IPv4 and IPv6.

Organizations that are not yet deploying IPv6 globally should implement the following recommendations:

· Block all IPv6 traffic, native and tunneled, at the organization's firewall. Both incoming and outgoing traffic should be blocked;

· Disable all IPv6-compatible ports, protocols, and services on all software and hardware;

· Begin to acquire familiarity and expertise with IPv6, through laboratory experimentation and/or limited pilot deployments; and

· Make organization Web servers, located outside of the organizational firewall, accessible via IPv6 connections. This will enable IPv6-only users to access the servers and aid the organization in acquiring familiarity with some aspects of IPv6 deployment.

Organizations that are deploying IPv6 should implement the following recommendations to mitigate IPv6 threats:

· Apply an appropriate mix of different types of IPv6 addressing (privacy addressing, unique local addressing, sparse allocation, etc.) to limit access and knowledge of IPv6-addressed environments;

· Use automated address management tools to avoid manual entry of IPv6 addresses, a process that is prone to error because of the length of IPv6 addresses;

· Develop a granular ICMPv6 (Internet Control Message Protocol for IPv6) filtering policy for the enterprise. Ensure that ICMPv6 messages that are essential to IPv6 operation are allowed, but that others are blocked;

· Use IPsec to authenticate and provide confidentiality to assets that can be tied to a scalable trust model; for example, allowing access to Human Resources assets by internal employees who make use of the organization’s Public Key Infrastructure (PKI) to establish trust;

· Identify capabilities and weaknesses of network protection devices in an IPv6 environment;

· Enable controls that might not have been used in IPv4 due to a lower threat level during initial deployment; for example, implement default deny access control policies, implement routing protocol security, and other similar practices;

· Pay close attention to the security aspects of transition mechanisms such as tunneling protocols;

· Ensure that IPv6 routers, packet filters, firewalls, and tunnel endpoints enforce multicast scope boundaries and make sure that Multicast Listener Discovery (MLD) packets are not inappropriately routable; and

· Be aware that switching from an environment in which NAT provides IP addresses to unique global IPv6 addresses could cause a change in the definition of system boundaries as specified in the Federal Information Security Management Act (FISMA).

For More Information

Information about the Internet Engineering Task Force, activities, and specifications is available from http://www.ietf.org/.

NIST publications that provide information and guidance on planning and implementing network and information system security include:

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
NIST Special Publication (SP) 500-287, *A Profile for IPv6 in the U.S. Government – Version 1.9*
NIST SP 500-281, *USGv6 Testing Program User's Guide*
NIST SP 500-273, *USGv6 Test Methods: General Description and Validation*
NIST SP 800-54, *Border Gateway Protocol Security*
NIST SP 800-61, Rev. 1, *Computer Security Incident Handling Guide*
NIST SP 800-64, Rev. 2, *Security Considerations in the System Development Life Cycle*
NIST SP 800-77, *Guide to IPsec VPNs*
NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*
NIST SP 800-88, *Guidelines for Media Sanitization*

For information about these NIST standards and guidelines, as well as other security-related publications, see NIST's Web page http://csrc.nist.gov/publications/index.html.

Information about NIST's information security programs is available from the Computer Security Resource Center http://csrc.nist.gov/.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.