IPv6 Integration in Federal Government: Adopt a Phased Approach for Minimal Disruption and Earlier Benefits

Abstract

U.S. federal government agencies are required to integrate IPv6 into their network infrastructures, but the mandate does not define the required steps. The way an agency plans and executes the IPv6 integration will have long-lasting ramifications on agency operations, IT, and mission effectiveness. Important questions include:

- Should we attempt to fully transition to IPv6 all at once, or is it preferable to integrate it in phases?
- Given that not all applications will be ready for IPv6 at the same time, what is the best approach when applications need to coexist on IPv4 and IPv6?
- How can we take advantage of new IPv6 features, such as peer-to-peer communications and autoconfiguration, and reduce management requirements?
- How can we ensure security for both IPv4 and IPv6 during the transition?

The way that agencies answer these questions affects the speed and ease of the IPv6 integration and how soon they can realize its business benefits.

It is a myth that organizations must transition to IPv6 all at once. Rather, by integrating IPv6 in phases, IT staff members can learn what they need to know to help their agencies begin experiencing the benefits of IPv6 while the integration is underway. Following are the main phases required to validate and move IPv6 to full production:

- Test the IPv6 integration in network infrastructure and applications in a lab environment
- Conduct a pilot production deployment for one or more campus LAN segments, or the WAN, as appropriate for the business mission
- Expand the geographic reach of IPv6 by deploying it more broadly in the LAN/WAN environment and using it for Internet connectivity
- Adopt new applications, such as peer-to-peer communications and autodiscovery, that can enhance government applications and services. This phase is when agencies actually experience the benefits of IPv6. Integrating IPv6 into the network infrastructure is simply a prerequisite.

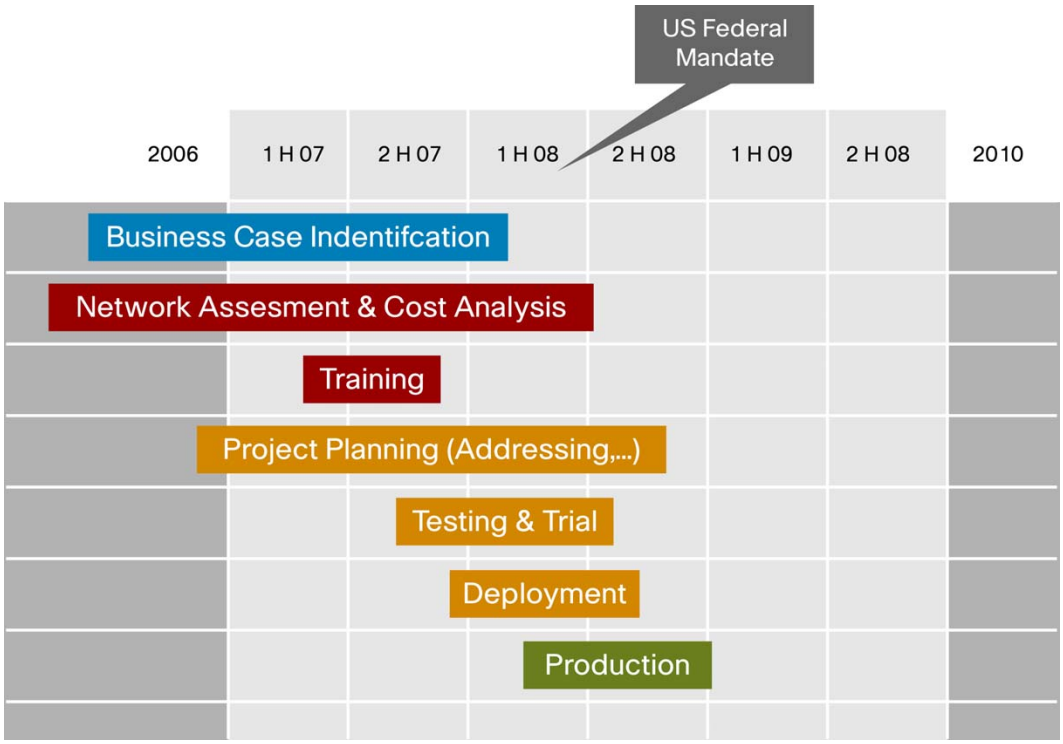
This paper provides guidelines for IPv6 integration in federal government. It outlines the actions that agency IT groups need to take during each phase of the integration. Sources for more detailed information on each phase are listed at the end of the paper.

Planning: Ten Essential Steps

To maximize the value of the IPv6 integration project, agencies can begin by developing a comprehensive plan. Following are planning recommendations that apply to all phases of the IPv6 integration: testing, pilot, broad deployment, and introduction of new IPv6-capable applications and services. Some of the steps can be performed in parallel:

- **Step 1 – View the agency's operation in a network-centric world:** Develop a positive business case for the IPv6 mandate by determining how its new capabilities can improve agency services. In the business case, analyze how IPv6 will affect IT, operations, and the overall business model. Consider new programs that the agency plans to launch within ten years that could take advantage of IPv6 peer-to-peer and autodiscovery capabilities. Possibilities include rapidly establishing command posts at disaster scenes; tying together currently incompatible communications systems with IPv6; and dynamically monitoring environmental sensors in data centers or specific racks.
- **Step 2 – Establish goals, a critical path, and general timelines:** The critical path includes provisioning the required hardware and software and implementing appropriate operational procedures. Figure 1 shows a sample timeline. When possible, coordinate the IPv6 integration with other IT projects, such as upgrading the infrastructure to support unified communications. This minimizes the incremental expense for the IPv6 integration.

Figure 1. Sample IPv6 Integration Timeline



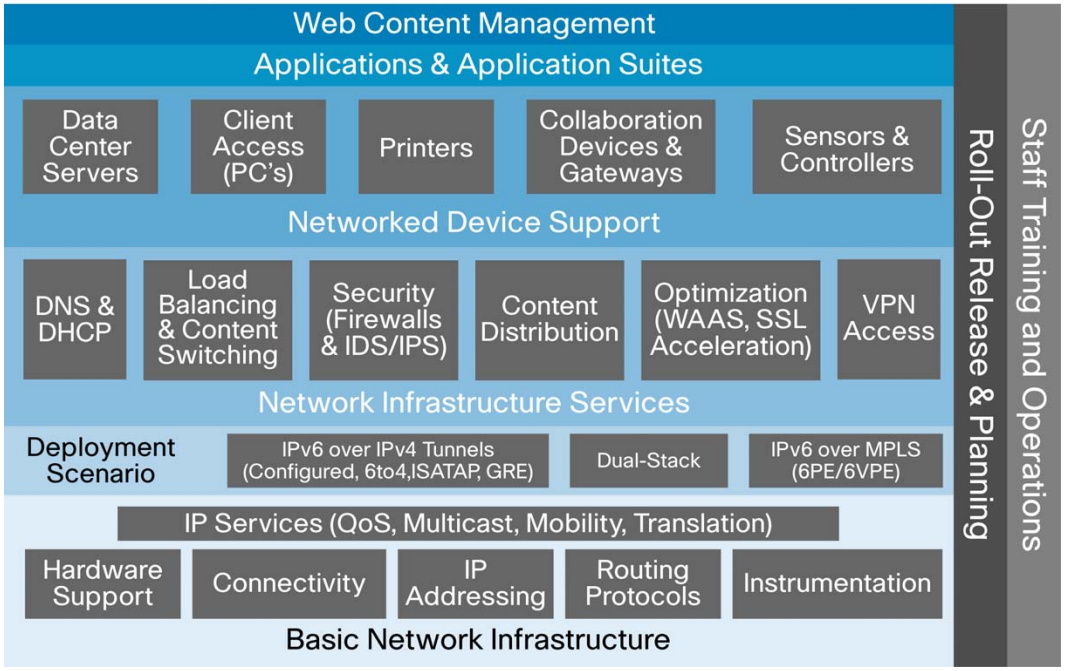
- **Step 3 – Create an IPv6 training strategy and plan:**
  - Train security architects to understand and mitigate the risks of IPv6.
  - Train executives and purchasing managers on how to specify IPv6 capabilities when they negotiate contracts with vendors and partners.
  - Train network architects to take full advantage of IPv6 capabilities.
  - Train application developers to take advantage of IPv6 features and capabilities to improve government services.
  - Train all IT employees who are involved with the network or desktop management, including employees on operations teams, to understand how IPv6 affects their area of responsibility.

- **Step 4 – Obtain an IPv6 prefix:** If needed, follow policies from the American Registry for Internet Numbers (ARIN) as well as guidelines from the federal organization. Before approaching ARIN, be sure to understand all addressing requirements: intranet, extranet, Internet, and sites not managed by the agency. Also know whether your agency needs unicast, multicast, or private addresses.
- **Step 5 – Develop an addressing plan and corresponding network architecture:** Establish policies for using the IPv6 prefix and decide which mechanisms to use to assign addresses: Dynamic Host Configuration Protocol v6 (DHCPv6), stateless autoconfiguration, or cryptographically generated addresses (CGA). Some agencies might use multiple mechanisms – for example, manually assigning addresses to critical servers and networking devices and using DHCPv6 to assign addresses to desktops. Network managers also need to review the impact of IPv6 Privacy addressing, if allowed, on network setup and operations. At the same time, recognize the role that the mechanisms will play for the increasingly mobile government workforce.
- **Step 6 – Assess IT equipment and identify the steps needed to integrate IPv6 into the network infrastructure:** The assessment includes hardware and software versions, memory size, configured features, and CPU usage. With this information, agency IT groups can perform any needed upgrades during their usual hardware lifecycle processes, reducing costs. They also learn what they need to develop the IPv6 integration test lab and test plan.
- **Step 7 – Develop an IPv6 procurement strategy and policy:** Define requirements for the IPv6 features and capabilities that the agency needs, and include them in all requests for proposal. Keep in mind that agencies can reduce capital costs by not asking for new capabilities several years ahead of time, but rather, with enough lead time for development. Be specific – that is, rather than specifying that equipment or software must be “IPv6-capable,” say that it must support a specific feature set defined in an IETF Request for Comment (RFC) or other well-known reference, and that the feature must either be already present or appear on the vendor’s roadmap. As an example, be sure to specify the appropriate IPv6 routing protocols for your design, as specified by the agency’s network architects. The links at the end of this paper include a list of products that have received IPv6 Special Interoperability Certification from the Defense Information System Agency (DISA) in accordance with the Department of Defense IPv6 Master Test Plan, as well as the latest guidance on what “IPv6-capable” means, from the National Institute of Standards and Technology (NIST) and Joint Interoperability Test Command (JITC).
- **Step 8 – Identify existing software and services and develop an upgrade plan:** For each host on the network, identify its operating system and applications. Use this information to determine if any hardware and software upgrades are required and schedule them to coincide with the usual hardware lifecycle process. Identify one or more applications to operate over IPv6, and then set up a lab to test those applications for the agency’s IPv6 environment. Several databases are available that indicate which applications used in federal government are IPv6-capable. The sooner an agency can take advantage of the new capabilities provided by IPv6 in its business applications, the sooner it will experience value from the investment.
- **Step 9 – Develop an IPv6 threats and countermeasures security policy:** Adapt the agency’s existing IPv4 security policies to include new considerations for IPv6. Consider security at every step in developing the overall network architecture. Major security considerations are discussed later in this paper.

- **Step 10 – Draft an exception strategy:** Identify applications or systems that will likely not be modified in the foreseeable future, either because they are too costly to integrate or are not part of the agency's future architecture. You will need to consider these applications and systems in the overall integration strategy if they will communicate over the new IPv6 network.

Throughout the planning and implementation process, keep in mind that IPv6 integration is a complex endeavor that happens gradually rather than all at once (Figure 2). It requires planning by network engineers and operators, security engineers, application developers, Web hosting and content developers, and business development managers. It also requires training for all agency personnel who will be involved in supporting the various network services that will take advantage of IPv6.

Figure 2. Elements of IPv6 Integration in Federal Agencies



Phased Approach

By taking a phased approach to IPv6 integration, the IT staff can selectively choose where to use IPv6 as the project progresses. This minimizes the need to install and maintain transition technologies that will eventually be removed. Other advantages of the phased approach are:

- The IT group can gradually gain skills and confidence.
- The IT group can develop best practices during the early phases, which helps to expedite the IPv6 integration in other sites.
- Agency managers and IT groups can confirm that IPv6 provides business value and is stable, manageable, and secure enough to be deployed.

  TIP: During each phase, approach IPv6 integration from a systems perspective, considering people, processes and controls, and technology – not just technology.

Table 1 shows the three major phases for IPv6 integration and the tasks to complete during each phase. More detail about how to complete these tasks appears in the remaining sections of this paper.

Table 1. Recommended Phases for IPv6 Integration

Phase 1: Integrate IPv6 into Infrastructure	Phase 2: Operate Selected Applications over IPv6	Phase 3: Move to Production
• Assess networking equipment, perform any needed upgrades, and then set up in selected locations • Register for an IPv6 prefix from a Regional Internet Registry (RIR) or ISP • Plan IP addressing and policies for autoconfiguration • Add minimum IPv6 support to critical networking services, including Domain Name Services (DNS) and Dynamic Host Configuration Protocol (DHCP) • Connect to the IPv6 Internet • Secure IPv6 access with access control lists (ACLs), firewall, and DMZ • Monitor IPv6 traffic on an ongoing basis	• Assess host and server operating systems and applications • Select operating systems and applications to update or configure them to operate over IPv6 • Configure naming services to make the selected applications available over IPv6 • Begin operating and monitoring the applications over IPv6 • Begin operating and monitoring applications, such as Internet Explorer and Mozilla Firefox, that use IPv6 when accessing IPv6 sites • Secure IPv6 on hosts • Deploy new applications and services that operate over IPv6; when selecting applications, look for applications that operate in a closed environment, which makes it easier to control variables	• Complete the deployment of IPv6 throughout the infrastructure • Finalize the upgrades to operating systems on hosts and servers • Ensure that management applications – internally developed as well as commercial – are fully operational over IPv6 • Ensure that the data center is fully operational for IPv6, including load balancer, Web server, and WAN optimization solutions • Upgrade specific solutions to IPv6, such as IP telephony

Integrating IPv6 into the Network

Following are the main steps to integrating IPv6 into the network. Throughout this phase and subsequent phases, try to regard the IPv6 integration project as an opportunity for the agency IT group to redesign its environment and explore new options to improve service delivery and simplify management.

Selecting an Option for Coexistence

Early in the project planning stages, agencies need to select an option for coexistence. IPv4 and IPv6 will need to coexist in government networks for many years, for the following reasons:

- Agencies cannot disrupt the delivery of mission-critical government services over the existing network. Agencies will adopt IPv6 on their infrastructure gradually rather than all at once.
- By continuing to support IPv4, the agency can migrate its applications and services to IPv6 over time, which is less expensive and less disruptive than upgrading and testing all applications at once.
- It might not be possible to add IPv6 support to older applications for which an agency does not own the source code.
- Upgrading or replacing old but stable operating systems, or platforms used for dedicated applications, might not provide value. It often makes better sense to wait to replace older operating systems or platforms until their end of life.
- Agency staff needs to receive training on IPv6, which takes time.

Agencies have several options to accomplish dual-stack networking – the coexistence of IPv4 and IPv6 – and the best approach for a given agency depends on its business goals, environment, and progress with IPv6 integration. Steps during the transition to dual-stack can include the use of IPv6-over-IPv4 tunnels, native IPv4 and IPv6 over dedicated data links, and IPv6 over Multiprotocol Label Switching (MPLS) backbones. An option for integrating older systems that will not be upgraded to IPv6 is to use translation mechanisms, including Network Address Translation –

Protocol Translation (NAT-PT). Figure 3 summarizes the mechanisms that can be used to integrate IPv6 into the existing infrastructure.

TIPS:

- Become familiar with the router and server resource requirements for the mechanism you select. For example, dual-stack and tunneling require additional processing power and memory in routers and servers, so you will need to take the requirements into account when you make equipment purchases.
- Be aware that it is generally unwise to front-end all systems with NAT-PT because this increases management complexity and operational costs.
- Realize that translation mechanisms such as NAT-PT can degrade performance and do not work well with all applications. The IETF has deprecated certain translation mechanisms.

Figure 3. Transition Mechanisms

	Environment	Comments
Core	Native IP – Core is IPv6-aware	Dual Stack
	MPLS – Core is IPv6-unaware	6PE*/6VPE**
WAN	IPv6 services on L3 managed services	Dual Stack
	IPv6 over L2 Services	Dual Stack
Campus	L3 infrastucture – IPv6-capable	Dual Stack
	L3 infrastucture – not IPv6-capable, or sparse IPv6 hosts population	ISATAP
Less optimum	IPv6 over IPv4 tunnels	Scalability and management issues
	Translation (NAT-PT)	Scalability and adapatability issues

* 6PE is IPv6 over MPLS
** 6VPE is IPv6 VPN over MPLS

Assess Network Devices

Before changing any network devices, conduct a detailed inventory that includes hardware type, memory size, software release and licensing, and configuration parameters. Many vendors provide tools to facilitate assessment. For example, the Cisco® IPv6 Network Assessor Tool scans Cisco routers and switches and then provides an easy-to-read report showing the results of the assessment and what needs to be done. Based on the results of the assessment, categorize all routers and switches as shown in Table 2. In addition to facilitating planning and scheduling, a network device assessment helps the IT group estimate capital expense.

Table 2. Categorize Routers and Switches to Estimate Capital Expense for Upgrades

Router Status	Costs
IPv6-compliant and currently running IPv6	None
IPv6-compliant but device needs to be configured for IPv6	IT staff time
Requires software upgrade for IPv6 compliance	Software and IT staff time
Requires hardware upgrade to support software upgrade	Hardware, software, and IT staff time
Legacy platform: cannot be upgraded to support IPv6 and must be replaced	Hardware, software, and IT staff time
Will not be upgraded due to planned discontinuation	None

TIP: By conducting the network assessment early in the planning stages, agency IT groups can include their IPv6 requirements in their standard hardware refresh cycles.

Take a Phased Approach to Infrastructure Integration

Following are recommended phases for IPv6 integration. They apply to testing basic connectivity during infrastructure integration as well as to testing applications in the IPv6 environment.

- **Testing IPv6 in a lab environment:** Testing in a lab enables the agency IT group to perform tests that could potentially be disruptive or introduce a security risk if deployed on the production network. Set up the test environment to resemble the production environment as closely as possible. Include the network hardware and software features targeted for IPv6 integration, as well as the first applications to operate over IPv6. At first, the test sites should not be connected to the production network or to each other. Later, after successful testing, connect them to each other. During the testing phase, the IT team gains valuable experience with integrating IPv6 into the network and can also determine if it needs to modify its technology plan or schedule.

  TIP: Many unexpected results during IPv6 testing are due to misconfiguration of LAN and VLAN segments and of services required to support IPv6, such as DNS. This underscores the importance of training and hands-on experience before IPv6 is deployed in an operational environment.

- **Pilot deployment:** After IT staff members in each lab have developed solid competence with IPv6, begin production LAN deployment in a few locations. During this phase, IPv6-enable the infrastructure in the pilot sites. Set up routers and switches to process IPv6 traffic. Configure the LAN to transport the agency's IPv6 prefixes to production host computers, printers, and other devices. Ensure that the security architecture is configured to handle both IPv4 and IPv6. Set up the DNS and DHCP servers to handle IPv6 queries. Configure the Network Management System (NMS) to monitor the IPv6 network. As part of the pilot, set up one ore more applications that can run over IPv6 so that the agency can begin experiencing the benefits of IPv6.

- **Broad deployment in production LAN/WAN environments:** When the pilot deployment in the production LAN environment is complete, connect the sites across the WAN, applying lessons learned from the pilot deployment. Make the tested IPv6-capable applications available throughout the agency.

- **IPv6 and connectivity to the Internet:** At this phase of the integration, the agency will be using dual-stack routers for Internet connectivity. Configure all existing network infrastructure (intranet, DMZ, extranet, and Internet) to block or allow IPv6 traffic as appropriate. Agencies that use IPv6 tunnels will probably want to limit this capability to a few

well-known routers. Test for security before allowing IPv6 connections with external sites. Recommended test scenarios include:

- IPv6 client behind the firewall connecting to IPv6 resource on the DMZ
- External IPv6 client connecting to IPv6 resource on the DMZ
- IPv6 client behind the firewall connecting to IPv6 resource on the Internet
- External IPv6 client connecting to IPv6 resource behind the firewall

Agencies can implement IPv6 services to and from the Internet in phases, as the IT group tests each scenario.

- **Advanced features:** In the final phase, investigate how to improve the design and delivery of the agency's existing and planned applications and services using IPv6 features such as mobility, security, quality of service (QoS), and multicast. On the surface, these features might not appear dramatically different from their IPv4 equivalents. However, notable improvements are possible from the combination of the IPv6 implementation of these features and the larger IPv6 addressing space. For example, an agency that upgrades its unified communications environment to IPv6 will set up QoS for the IPv6 traffic similar to the way that it is set up for IPv4 traffic. The difference is that the agency can take advantage of the larger address space to simplify its addressing scheme, which also simplifies deployment and the design of QoS policies. Agencies can also investigate the use of features that are improved in IPv6, such as Mobile IP, and incorporate them in new services that can be rolled out over IPv6 from day one.

Plan and Provision Addresses

The practically unlimited address space in IPv6 allows agency IT groups to design a network architecture that matches the organizational structure – for example, by identifying a building number or device location in the /64 prefix. (Taking this to the extreme, however, by identifying every type of device or structure, can very quickly use up address space.) Take the time to build a solid addressing scheme that will address the agency's growth and application plans. To ensure scalability, use address aggregation – that is, assign a block of addresses for exclusive use of each region in the network. Be sure to consider the ways that the Interior Gateway Protocol (IGP) will aggregate the addresses. Enhanced Interior Gateway Routing Protocol (EIGRP) is a good option for many agencies.

> **TIP:** Consider using IP Address Management (IPAM) tools for numbering, to save time and eliminate numbering mistakes.

Moving Applications to an IPv6 Environment

Assess all servers, desktops, laptops, and workstations to determine what they need to support IPv6. For example, a PC might need to be updated to Microsoft Vista to fully operate in an IPv6 environment with new applications. After the clients are IPv6-ready, begin upgrading existing applications to support IPv6 and installing new IPv6 applications. The Microsoft Peer-to-Peer (P2P) framework can be used for application development. A P2P application used in the private sector that also has relevance for government is ((Echo))MyPlace, which lets members of a community of interest instantly share location-based digital news and video content between distributed computers in a P2P network (http://www.thecarbonproject.com/social.php).

> **TIP:** Rather than establishing a separate project to certify that applications installed on employee computers are IPv6-compatible, test them at the same time you certify applications

for other requirements, such as compatibility within the 2007 Microsoft Office system. This approach minimizes the incremental cost to transition client applications to IPv6.

Test all applications in the lab to verify that they can operate over IPv6 before they are released into production. Configure them to use IPv6 transport if it is available and IPv4 if it is not.

After IPv6-enabling existing applications, consider developing new applications that take advantage of new features in IPv6 to help meet agency mission objectives. Examples include:

- New communications interoperability solutions that enable existing, incompatible communications systems based on IPv4 to tie into each other using the peer-to-peer capabilities in IPv6.
- A sensor-based data center solution that dynamically monitors the temperature in the data center, racks, and even specific devices.
- Continuously monitoring the vital health signs of response personnel as they enter the response area, as well as real-time environmental information.

Integrating IPv6 into Operations

The same IT team that currently manages the IPv4 network will be managing the dual-stack network. Dual-stack environments are easier to manage than tunneling environments because troubleshooting is simpler. Tools that can track and manage both IPv4 and IPv6 traffic avoid doubling the workload and simplify issue tracking. Table 3 shows the operational tools needed in a dual-stack environment. Operations and engineering staff will need ongoing training throughout the IPv6 integration to use these tools.

Table 3. Commonly Used Management Tools that Work in a Dual-Stack Environment

Type of Tool	Examples
Traffic Monitoring	Management Information Base (MIB) for IPv6, NetFlow IPv6 records, IPv6 service-level agreement (SLA)
Network Services	DHCPv6 Server and Relay, Domain Name Server (DNS), Network Time Protocol (NTP)
Network Management Systems	Network management applications specific to the IPv6 environment such as IPv6 topology mapping, IPv6 user tracking
Other Management Applications	Secure Shell (SSH) Protocol, Simple Network Management Protocol (SNMP), Syslog

Security Considerations

A fundamental premise of the IPv6 integration is to not disrupt the operations of the existing network, and a well-thought-out security plan helps to meet this goal. Security needs to be considered during all phases of the IPv6 integration.

IPv6 networks are subject to many of the same threats and attacks as IPv4 networks. They are also subject to new threats because of IPv6-specific characteristics and the specifics of various integration mechanisms. Vendors, including Cisco, are working to offer a full set of security features for IPv6. Until an agency's environment is IPv6-only, the IT group can use existing IPv4 security mechanisms that also secure hosts for IPv6. For example, existing 802.1X Network Access Control security solutions developed for IPv4 can continue to use the same mechanisms to secure the layers below the IPv6 protocol stack.

Following is a short list of recommended security practices:

- **Make reconnaissance more difficult through proper address planning for campus switches.** A common recommendation is to devise the addressing plan so that the 64-bit interface-ID of the switch is random and cannot easily be guessed.
- **Control management access to the campus switches.** Switches have loopback interfaces configured for management and routing. The IPv6 address for the loopback interfaces should not be easy to guess.
- **Implement IPv6 traffic policing, on a per-user microflow basis.**
- **Control ingress traffic from the access layer.** Filter the prefixes that are allowed to source traffic to help protect against basic spoofing.
- **Upgrade to IPv6-aware firewalls.** Adapt the agency's IPv4 security architecture to handle IPv6 transport. This requires redefining current firewall rules—for example, to specify which ICMPv6 messages can traverse the firewall and which transition mechanisms are allowed.
- **Monitor and control all transition mechanisms.** Turn off transitions that are built into certain applications. Applications that use automated tunneling, for example, can traverse firewalls, thereby exposing the network to the outside world. In agencies that have a mobile workforce, disable mechanisms on devices when they are used within the enterprise and enable them when they are used outside.

  TIP: If the agency's security policy prohibits tunneling, products such as Cisco Network Access Guardian can scan Windows devices and turn off this feature.

Conclusion

A phased integration minimizes the need for transition technologies and gives the IT group a chance to gradually gain skills and confidence and develop best practices. Agencies can prepare for IPv6 integration today by following the 10 planning steps at the beginning of this paper. Early on, set up a test lab to help analyze and verify the various hardware and software in the network. By experimenting with application configuration in a lab, federal government IT groups can develop their IPv6 skills and learn the optimum configuration for their mission-critical applications before deploying the applications into production.

It is crucial to remember that simply turning on IPv6 throughout the infrastructure does not provide business value in the federal government. Rather, agencies begin experiencing business value after they configure their applications to take advantage of new IPv6 capabilities, such as peer-to-peer communications and enhanced mobility.

For More Information

To read more about Cisco IPv6 technology, visit:
http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

To read about other organizations' experiences with integrating IPv6, visit:
http://blogs.technet.com/ipv6/

For the appropriate release of Cisco IOS® Software for different Cisco switches and routers, see the IPv6 Start Here manual at:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65ed.html

For a detailed guide to deploying IPv6 in campus networks, visit: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration_09186a00807753a6.pdf

For a list of products that have received IPv6 Special Interoperability Certification from the Defense Information System Agency (DISA) in accordance with the Department of Defense IPv6 Master Test Plan, visit: http://jitc.fhu.disa.mil/apl/ipv6.html.

For updates on certification activities, visit:

Joint Interoperability Test Command
http://jitc.fhu.disa.mil/apl/ipv6.html

National Institute of Standards and Technology IPv6 Profile Paper
http://www.antd.nist.gov/usgv6-v1-draft.pdf

IPv6 Ready Logo Program
http://www.ipv6ready.org/frames.html

For more general IPv6 information, visit:

http://www.6diss.org/

http://go6.net/

http://www.ipv6forum.com/

http://www.ietf.org/html.charters/v6ops-charter.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-462676-00 03/08