Planning and Accomplishing the IPv6 Integration: Lessons Learned from a Global Construction and Project-Management Company

Abstract

After deciding to integrate Internet Protocol version 6 (IPv6), IT groups face a series of technical and planning decisions with long-lasting ramifications, including:

- Should we fully transition to IPv6 all at once, or integrate it gradually?
- Is it preferable to IPv6-enable the entire network infrastructure before transitioning applications?
- What is the best approach when applications need to co-exist 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 increase business efficiency with new IPv6-enabled functions such as mobility, sensor networking, and collaboration?
- How can we help ensure security for both IPv4 and IPv6 during the transition?

These and other decisions affect the ease of the IPv6 integration and how soon organizations can realize the business benefits.

This white paper examines issues involved in planning the IPv6 integration by describing the experience of a global construction and project-management company with offices in more than 100 countries. The company, referred to as Company6 in this white paper, embarked on the IPv6 integration project in 2005. Its goals were to support a new generation of IT applications and services, including peer-to-peer and mobility; enable rapid project mobilization in temporary job sites; and comply with its federal customers' requirements to implement IPv6-compliant networks by 2008. The IPv6 integration project entailed changes to the company's Cisco® network foundation, Microsoft operating systems and applications, other applications, servers, and desktops.

Company6 engaged two primary IT partners, Cisco and Command Information, to assist with transition planning, and received technical support from Microsoft. Its first decision was to make IPv6 an everyday part of all IT processes—from project management to network upgrades and application certification—rather than a separate effort.

Company6's success with IPv6 integration underscores the main principle of IPv6 integration planning, which is that upgrades to the infrastructure and applications can be performed in parallel. A completely IPv6-capable infrastructure by itself delivers no business value. Rather, organizations begin experiencing business benefits when they adapt their applications and operations to take advantage of new IPv6 capabilities that the infrastructure makes possible.

A completely IPv6 capable infrastructure by itself delivers no business value. Rather, organizations begin experiencing business benefits when they adapt their applications and operations to take advantage of new IPv6 capabilities that the infrastructure makes possible.

It is a myth that a company must adopt IPv6 all at once. Company6's experience demonstrates that by gradually integrating IPv6, IT staff members can learn what they need to know to help their organizations begin experiencing the benefits of IPv6 while the integration is under way.

This white paper begins with ten essential planning steps for organizations planning for IPv6 deployment and integration. The remainder of the paper describes each of Company6's carefully coordinated integration projects: the Cisco network foundation, applications, management, and security.

Ten Essential Planning Steps

Before embarking on the IPv6 integration project, Company6 followed Command Information's recommendations for planning:

Step 1. *View the operation in a network-centric world:* Company6 first determined how IPv6 would affect its operations, including new applications, opportunities, and threats. To maximize the return on investment (ROI) from IPv6, it is crucial to understand its effect on IT, operations, and the business model.

To maximize the return on investment (ROI) from IPv6 it is crucial to understand its effect on IT operations and the business model.

Step 2. *Establish goals, a critical path, and timelines:* For Company6, major milestones included developing a timeline for the project,

identifying partners (Cisco and Microsoft), obtaining approval from executive management, and acquiring an executive sponsor. Company6's project team included an IT project manager, network operations team, security team, software development, quality assurance, and people who defined purchasing policies.

Step 3. *Inventory IT equipment and build a deployment plan:* Company6 used the Cisco IPv6 Network Assessor Tool to scan its Cisco switches and routers to determine if they had the required memory and version of the Cisco IOS® Software. It also assessed its third-party devices. The inventory enabled Company6 to perform upgrades during its usual hardware lifecycle processes. This approach minimizes capital expense and also helps ensure that network equipment is already IPv6-capable when the company wants to begin using IPv6-capable applications and computers.

Step 4. *Identify software and services and develop an upgrade plan:* This requires establishing a lab and testing applications for IPv6 support. At Company6, any application that went into quality assurance (QA) came out IPv6 capable. Command Information maintains a database of applications, including the top 100 applications used in U.S. Department of Defense networks, indicating whether they are IPv6 capable. The earlier an organization enables IPv6 capabilities in its applications, the sooner it can begin experiencing the benefits of IPv6.

Step 5. *Create an IPv6 training strategy and plan:* Organizations should begin by training their security architects to understand the risks of IPv6 and how to mitigate them. Next, they should train their network architects to take full advantage of IPv6 capabilities. As an example, a video camera installed behind an IPv4 Network Address Translation (NAT) router in a remote location might require a complex configuration. But if the camera is only reachable via IPv6 from an external device, it requires a simpler configuration, reducing IT burden. IT employees should be trained to recognize this and other opportunities that IPv6 creates.

Step 6. *Develop an addressing plan and corresponding network architecture:* The first requirement is to understand all addressing requirements: intranet, extranet, and sites not managed by the company. Using IP Address Management (IPAM) automated tools saves time and eliminates numbering mistakes.

Step 7. *Obtain an IPv6 prefix:* Organizations can contact the Regional Internet Registry for their region to obtain either a Provider Independent (PI) or Provider Aggregatable (PA) prefix. In regions where PI space is not yet available, such as European regions within RIPE NCC control, organizations not elected for a PA prefix can only obtain a prefix from their Internet service provider or use Unique Local Addressing (RFC 4193). Global organizations not elected for a PA prefix might be eligible for PI space in other regions.

Step 8. *Develop an IPv6 threats and countermeasures security policy:* The same security threats exist with IPv6 as with IPv4. Organizations should develop a list of threats to be monitored. In particular, they need to protect against new threats that arise during the transition to IPv6, such as IPv6 exploits not detected by firewalls that are not IPv6-aware. Security considerations are discussed later in this white paper.

Step 9. *Develop an IPv6 procurement strategy and policy:* The global project-management company worked with its vendors to help ensure that all products would be IPv6 capable.

Step 10. *Draft an exception strategy:* Identify applications or systems that currently meet the business need and will likely not be modified in the foreseeable future. There is no cost justification for migrating these applications or systems to IPv6, so companies can plan for indefinite co-existence.

Integrating IPv6 into the Cisco Network

The network foundation for Company6's infrastructure comprises Cisco Catalyst® 6500, 4500, and 3500 XL Series Switches, Cisco integrated services routers, and Cisco 7200 Series Routers. It connects eight core data centers as well as 180 sites. The network serves as the platform for Cisco Unified Communications, the Microsoft Active Directory service, Microsoft Desktop operating systems, and wireless and mobility services.

Co-existence

IPv4 and IPv6 will need to co-exist for many years in most organizations, including Company6, for several reasons:

- Most companies adopt IPv6 on their infrastructure gradually rather than all at once.
- If an organization completely turned off support for IPv4 in the network, then its IPv4 applications, Web sites, and services would no longer work. By continuing to support IPv4, the organization can gradually upgrade applications to IPv6 and test them, which is less expensive than upgrading and testing all applications at once.
- It might not be possible to add IPv6 support to older applications for which a company does not own the source code.
- Upgrading or replacing old but stable operating systems, or platforms used for dedicated applications, might not provide ROI. In some cases, it makes better business sense to wait to replace those operating systems until their end of life.

To prepare for co-existence, Company6 identified the applications and locations to migrate to IPv6 and developed a migration schedule. The first locations selected had a large number of applications that can communicate over IPv6, such as Microsoft Internet Information Services (IIS) 6.0. Company6 developed scalable IPv6 enablement packages for its many Windows XP SP2 and Windows Server 2003 computers. Windows Vista computers are enabled for IPv6 by default.

Company6 engaged Command Information to help define and implement a phased integration plan. After evaluating the various methods for co-existence, the company selected the dual-stack approach. That is, in the places in the network that will support IPv6-capable applications, Company6 is setting up its applications and devices to support both IPv4 and IPv6. Table 1 summarizes the options for co-existence and their advantages and disadvantages.

Table 1. Comparing Network Approaches to IPv4 and IPv6 Co-existence

Deployment Strategy	Benefits	Limitations	Requirements
IPv6 Using Dual-Stack Backbones	• Supports gradual evolution to IPv6-dominant network. • Best design approach for campuses that have a mixture of IPv4 and IPv6 applications and simplifies transition from IPv4 to IPv6 applications. • All services, including QoS and multicast, are operational for both IPv4 and IPv6.	• Requires establishment of rules for dual-stack management and security.	• Deploy dual-stack routers and L3 switches with IPv4 and IPv6 addresses. • Provide enough memory for both IPv4 and IPv6 routing tables. • Establish switch environment that supports IPv6 router advertisements for stateless address autoconfiguration of clients. • Enable naming services for IPv6. • Validate device configuration to run both IPv4 and IPv6.

Deployment Strategy	Benefits	Limitations	Requirements
IPv6-over-IPv4 Tunnels	• Easy to implement over existing IPv4 infrastructures. • Low cost, low risk. • Workaround for carriers' lack of IPv6 services to the premises.	• As the IPv6 deployment grows, management and diagnostics become slightly more complex because of the independent tunnel and link topologies.	• Upgrade routers and L3 switches configured as tunnel end-points for dual-stack. • Enable naming services for IPv6.
Native IPv4 and IPv6 over Dedicated Data Links	• Strategic, long-term option. • A VLAN on campus or dedicated PVC, serial links, or optical lambda can be dedicated to IPv6. • Allows integration of IPv6 traffic without any impact on the IPv4 operations and business. • Eliminates need for IPv6-over-IPv4 tunnel.	• Might require additional hardware to split the traffic. • Increases complexity of network management and security.	• Configure routers dedicated to IPv6 traffic as dual-stack for specific services, such as network management. • Enable naming services for IPv6. • Carrier delivers native IPv6 services to the premises.
IPv6 over MPLS Backbones	• Integrates IPv6 over MPLS, avoiding the need for hardware or software upgrades to the network core.	• Implementation is required to run IPv6 over provider's IPv4 MPLS networks. • High management overhead. • Mostly applicable for organizations that have already deployed MPLS services	• Make nominal changes to the customer edge (CE) or provider edge (PE) routers, depending on the technique.

Company6's gradual approach to IPv6 integration minimizes the need to install and maintain transition technologies that will eventually be removed. Company6 did set up IPv6-over-IPv4 tunnels, but only in the few locations where the dual-stack upgrade will not be complete before a certain time. The tunnels allow the company to deploy and validate IPv6 applications independently from the infrastructure upgrade. They provide IPv6 WAN connectivity by directly encapsulating IPv6 packets within IPv4 packets using IPSec in transport mode (Protocol 41 Encapsulation). Company6 does not use any protocol-translation technologies.

Table 2 describes some IPv6-over-IPv4 tunnel mechanisms.

Table 2. Overlay Tunnel Mechanisms

Tunnel Mechanism	Primary Use	Benefits	Limitations	Company6 Requirements
IPv6 over IPv4 GRE Tunnel	• WAN connectivity. • Stable and secure links for regular communication.	• Well-known standard tunnel technique. • Currently supported in IPv6 for Cisco IOS Software. • Required for access to IPv6 points of presence of several U.S. carriers that are not yet providing IPv6 service to the customer premises.	• Tunnel between two points only. • Management overhead.	• ISP-registered IPv6 address. • Dual-stack router. • Required by Intermediate System-to-Intermediate System (IS-IS) protocol for IPv6.

Tunnel Mechanism	Primary Use	Benefits	Limitations	Company6 Requirements
IPv6 Manually Configured Tunnel (RFC 4213)	• WAN connectivity. • Stable and secure links for regular communication. • Can be protected by using IPv4 IPsec	• Tunnel standard dedicated to IPv6. • Currently supported on Cisco IOS Software.	• Tunnel between two points only. • Management overhead. • Must be removed when native IPv6 services are installed for WAN traffic.	• ISP-registered IPv6 address. Dual-stack router.
ISATAP Tunnels (IPv6 packets travel over IPv4 between dual-stack nodes)	• Campus connectivity. • Decreases deployment costs by enabling organization to turn on IPv6 in locations with older network devices that have not yet been upgraded to support IPv6. • Provides a simple and cost-efficient way to set up an IPv6 test lab	• Currently supported in IPv6 for Cisco IOS Software. • Supported in Microsoft Windows Server 2003, Windows XP, Windows Vista, and the forthcoming Windows Server 2008.	• No multicast support. • Management overhead.	• Dual-stack router

Phased Project

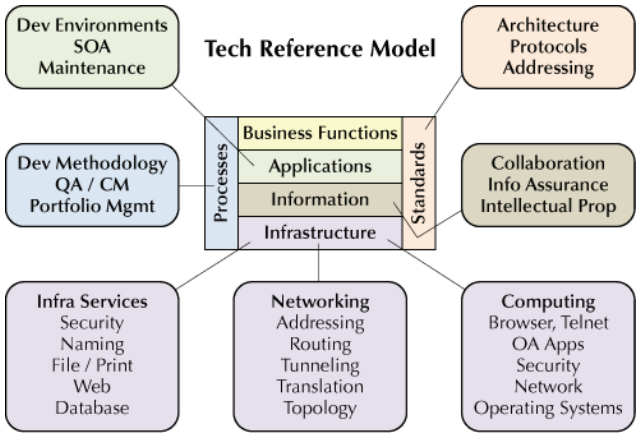
At the outset of the planning process, Company6 decided to integrate IPv6 in phases. The advantages of this approach are to enable:

- The IT group to gradually gain skills and confidence
- The IT group to develop best practices during the early phases, which would expedite the IPv6 integration in other sites
- Senior management to confirm that IPv6 is stable, manageable, and secure enough to be deployed.

During each phase, Company6 approached IPv6 integration from a systems perspective, considering people, processes and controls, and technology—not just technology. Figure 1 shows the scope of Company6's IPv6 integration project.

During each phase, Company6 approached IPv6 integration from a systems perspective, considering people, processes and controls, and technology—not just technology.

Figure 1. Tech Reference Model for IPv6 Integration at Company6

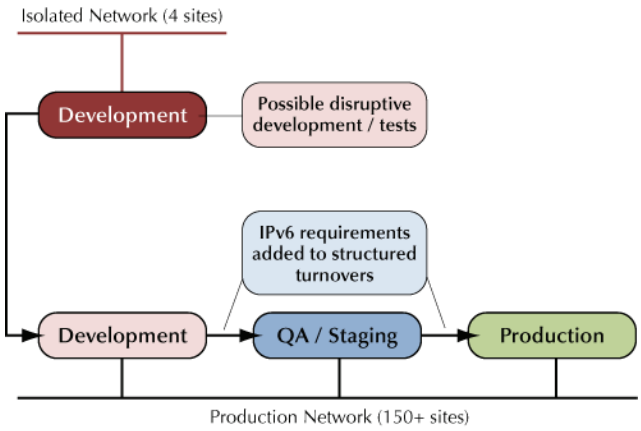


Following are the phases of the IPv6 integration project at Company6:

- *IPv6 in a local lab:* Company6 selected four test sites for the initial phase of the IPv6 integration, based on their security, management, and IT team expertise. The four isolated labs were set up to perform tests that could potentially be disruptive or create a security risk if deployed on the production network (Figure 2). The selected sites, which relatively large employee populations, include two primary sites that serve government customers, corporate IT, and Company6's largest data center. The sites were not connected to the production network or to each other. In the lab environment, Company6 determined that most unexpected results were 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. Other lessons learned include:
  - Stateless address auto-configuration works well for assigning IPv6 addresses to hosts. The lack of DHCPv6 scope options is not an impediment, and the scope options can be introduced when they become available.
  - It is helpful to run IPv6 in an environment with Microsoft Windows 2003 SP1 or Bind 9.3.2 or later DNS services.
  - While Windows Server 2008 fully supports DHCPv6 and DNS reverse lookup, Windows Server 2003 does not. However, Company6 determined that Microsoft Windows 2003 DNS services were adequate for production deployment while the company planned its migration to Windows Server 2008.
  - Microsoft Internet and Application Security (ISA) server does not currently support IPv6.

In the lab environment, Company6 determined that most unexpected results were 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.

Figure 2. Transition from IPv6 in Local Labs to Production Network



- *Intersite connectivity in a lab environment:* The four test sites, now using IPv6, were connected over IPv4 using IPSec in Transport Mode (Protocol 41 Encapsulation) tunnels. The use of well-understood technology, detailed in RFC4213, accelerated the trial. During this phase, the team revised the addressing plan, gained valuable experience with routing protocols, and started testing the end-to-end WAN performance of IPv4 compared to IPv6.
- *Pilot deployment in production LAN environment:* After IT staff in each lab had developed solid competence with IPv6, the company began its production LAN deployment at the four locations. The IT group set up Cisco routers to provide IPv6 prefix router advertisements and configured VLANs to transport Company6's IPv6 prefixes to production host computers, printers, and other devices. Microsoft Windows Server 2003 DNS services registered the IPv6 AAAA resource effectively, as they had in the isolated lab and QA environments. At the beginning of this phase, Company6 used name-based network tools that required name-address resolution. This was soon followed with IPv6 communications to local IPv6-enabled Web servers. The IT group developed Microsoft SMS scripts to handle IPv6 configuration and tasks on IPv6-enabled computers. Cisco wireless access points, which had been tested in the lab, were enabled selectively on the production networks and configured to provide user and computer certificate-based authentication. All VLANs in the pilot offices, including all data center segments, were IPv6-enabled. During this phase, Company6 developed scalable models that could be applied in other sites to quickly enable IPv6.
- *Pilot deployment in production WAN environment:* Company6 connected the four production LAN pilot

across the WAN using IPSec in Transport Mode (Protocol 41 Encapsulation) tunnels that had been tested in the isolated lab environment. The process was successful and uneventful.

- *Broad deployment in production LAN/WAN environments:* After testing and documenting the LAN, WAN, and host deployment models, Company6 began enterprisewide deployment, beginning with the remaining large offices and data centers. As of September 2007, more than 80 percent of the company's desktop and laptop computers were running IPv6. More than 50 percent of the company's employees are using IPv6-enabled LANs and WANs.
- *IPv6 and connectivity to the Internet:* Company6 has defined four discrete scenarios that it will test for security before allowing IPv6 connections with external sites:
  - 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

  Only one of the four lab sites is connected to the Internet, for security. However, during testing, all four sites will be reachable over IPv6. Company6 will implement IPv6 services to and from the Internet in phases as the IT group tests each scenario.
- *IPv6 and mobile access pilot:* IPv6-enabled wireless access testing began in the lab, using Cisco 1131 Wireless Access Points and Cisco 871W Integrated Services Router. The Company6 IT group defined standard configurations that include the company's certificate-based authentication, which is supported by Microsoft Active Directory and Microsoft Certificate Authorities. Basic IPv6 services, including forwarding IPv6 router advertisements to wireless hosts, are working well. WLAN devices using Windows Mobile 2003 and later are successfully acquiring globally routable IPv6 addresses.
- *Pilot deployment of IPv6 native Internet connectivity (planned):* Company6 will configure its Cisco routers in the test labs to transport external traffic over IPv6 when the company's carriers begin providing IPv6 connectivity. When this occurs, the company will no longer need the tunnelling technology used during the transition to IPv6.
- *IPv6 and mobile access to production network:* Several Cisco wireless access points and wireless routers are currently operating in a dual-stack mode. Cisco 4400 Series Wireless LAN Controllers are currently deployed in one location and will be placed into production in three other global locations in October 2007. The controllers enable centralized management of the company's Cisco 1131, 1242, and Cisco Aironet® 1250 Series access points in global sites. When the wireless LAN controller infrastructure is fully deployed, Company6 will enable IPv6 on all access points in the enterprise. The company plans to accelerate testing of mobile routers in early 2008.
- *Native IPv6 on internal network (planned)*

Network Device Assessment

Before changing any network devices, Company6 first conducted a detailed inventory that included hardware type, memory size, Cisco IOS Software release and licensing, and configuration parameters. Company6 used the Cisco IPv6 Network Assessor Tool to scan its Cisco switches and routers. To assess third-party devices, organizations can use a network management tool from that vendor.

IPv6 is a supported feature set on most Cisco IOS Software network devices deployed since 2001. Therefore, rather than replacing foundation devices, Company6 only needed to help ensure that they had adequate memory and were running a version of the Cisco IOS Software that supports the IPv6 capabilities that are important to Company6, such as security features. (A link to appropriate Cisco IOS Software releases for different Cisco switches and routers is provided at the end of this white paper.) If memory or Cisco IOS Software needed upgrading, then Company6 followed its ordinary process for upgrading equipment and then performed the IPv6 configuration.

Based on the results of the assessment, the company grouped the routers in the following categories:

- IPv6 compliant and running IPv6
- IPv6 compliant
- Requires Cisco IOS Software upgrade for IPv6 compliance
- Requires hardware upgrade to support Cisco IOS Software upgrade

- Legacy platform: cannot be upgraded to support IPv6 and must be replaced
- Will not be upgraded due to planned discontinuation

A network device assessment not only is mandatory for effective planning and scheduling, it also helps the IT group estimate capital expense (Table 3). By conducting the network assessment early in the planning stages, organizations can include their IPv6 requirements in their standard hardware refresh cycles.

By conducting the network assessment early in the planning stages organizations can include their IPv6 requirements in their standard hardware refresh cycles.

Table 3. Comparing the Capital Expense of Different IPv6 Integration Approaches for Company6

Relative Cost	Hardware	Software	Operation
Very High	Full replacement	Full upgrade	Local intervention
High to Medium	Hardware upgrade, such as increased memory, addition of line card or supervisor engine	Full upgrade	Local intervention
Medium to Nominal, depending on the need to purchase an upgraded license	No change	Full upgrade	Local or remote intervention
Nominal	No change	No change other than configuration	Local or remote intervention

Company6 expects that two-thirds of its Cisco routers will be running IPv6 for inbound traffic by the end of 2007.

Addressing Planning

The unlimited address space in IPv6 allows IT groups to design a network architecture that matches the organizational structure—for example, by embedding a building number, country, or device location into the address.

The nearly unlimited address space also enables organizations to consider using specific IPv6 address formats for privacy. One option is to use a globally routable prefix or Unique Local Addressing (RFC 4193) in the prefix portion, which has an effect similar to that of the private network address space on IPv4 (RFC 1918). Unique Local Addressing is not an option when Internet connectivity is needed, however, and might require numbering later. Another option for host privacy is to use randomly generated privacy addresses, which generate addresses from interface identifiers that change over time. This makes it more difficult for outside parties to view the addressing scheme. However, IT groups should be aware that randomly generated privacy addresses require appropriate management schemes for operational management and troubleshooting.

To develop its addressing plan, Company6 used IP Address Management (IPAM) tools. The cost-justification for the tools is clearer for IPv6 than for IPv4 because management is more complex when organizations use the unlimited address space creatively to meet business and network needs.

DNS and DHCP Considerations

The IT group must register IPv6 resources (AAAA records) on DNS servers. Windows XP clients perform DNS name resolution over IPv4, while Windows Vista clients use IPv6 if it is available.

The IT group also needs to define the auto-configuration method used for host addresses, either stateless auto-configuration or DHCPv6. Windows XP clients can only use stateless autoconfiguration, which does not rely on a DHCP server, and the DHCP server in Windows Server 2003 cannot offer IPv6 addresses. Windows Vista can use stateful addressing, which requires DHCPv6 services,

provided by Windows Server 2008. If an organization decides to use DHCPv6—even only in stateless mode to propagate information such as DNS servers addresses—the IT group must set the DHCPv6 Relay and Neighbor Discovery flags on routers and L3 switches.

Helping Ensure Application Compatibility and Taking Advantage of IPv6 Capabilities

Company6 coordinated its upgrade to Microsoft Vista and Windows Server 2008 with its IPv6 project.

Using the results of its inventory, Company6 is developing a schedule for upgrading its other client applications; commercial, off-the-shelf software (COTS); internally modified software; and custom applications.

Client Applications

Company6 has standardized on the Microsoft server product portfolio, including the Windows Server 2003 Enterprise Edition operating system. For testing purposes, the lab environment also includes Windows Server 2008.

Rather than establishing a separate project to certify that applications installed on employee computers are IPv6-compatible, the company's QA team tested for compatibility at the same time that it certified programs within the 2007 Microsoft Office system. With this approach, the incremental cost to transition client applications to IPv6 was only a couple of weeks of work for one person.

Applications that ship with Windows Vista and Windows Server 2008 are ready for IPv6-only or dual-stack environments. IPv6 has full parity with IPv4 throughout both operating systems. The growing importance of IPv6 factored into the design of the Peer-to-Peer (P2P) Framework, which is an open set of APIs that require IPv6 to operate. Windows Meeting Space is among the out-of-the-box applications that uses the P2P Framework and, therefore, will not work if IPv6 is disabled.

Following are lessons learned from Company6 as it tested applications for IPv6 compatibility:

- If the database is logging IPv6 addresses, make sure the address field is long enough.
- Multiple vendors are working on making their applications more stable when IPv6 is enabled end-to-end.
- In IPv6 mode, certain server-side applications, including Microsoft Internet Information Server 6.0 (when running on Windows Server 2003) support HTTP but not HTTPS. This becomes evident if a Web site switches between the two protocols.

Commercial and Internally Developed Applications

In late 2006, Company6 began testing its commercial and internally developed applications in an environment that has end-to-end IPv6 connectivity. The goal of testing was to help ensure that all applications could transport traffic over IPv6 before they were released into production. Microsoft provides the checkv4.exe tool to identify the code that must be changed. Any application submitted for QA is modified at that time to be dual-stack capable.

As new applications are developed, Company6 developers configure them to use IPv6 transport if it is available and IPv4 if it is not. The company has already configured IPv6 in its development environments, including the Microsoft .NET Framework.

New Applications Designed to Exploit IPv6 Capabilities

After IPv6-enabled its existing applications, Company6 began developing new applications that take advantage of new features in IPv6. One new application will use the discovery mechanisms in IPv6 to send e-mail messages directly from one person without two intermediary e-mail servers. The enablers are the discovery mechanisms in IPv6 and Microsoft's Peer Neighbor Resolution Protocol (PNRP). Another application under development will synchronize e-mails from a smartphone to a laptop over WiFi, without a DNS or collaboration server.

Company6 is also taking advantage of IPv6 to simplify application development, using the APIs that are part of the P2P Framework in Windows Vista. Using these APIs, Company6 developers do not have to specify the IPv6 clouds with which to register a particular name and IP addresses. Instead, the PNRP component of Windows Vista automatically determines the appropriate clouds to join and the addresses to publish within the clouds.

Examples of How Applications Work End to End over IPv6

One example is Windows Meeting Space, which enables groups of up to 10 users to quickly and securely form a shared, common networking session. Group members can make their desktops and applications available to other group members or transmit information to a Windows Vista–compliant video projector. Users can share and jointly edit files within a common work area. And they can

do all this through either a corporate network or a spontaneous connection.

Another example is the Advanced Incident Response System (AIRS) solution developed by Cisco and Command Information, with partners Arch Rock and pTerex. The AIRS solution enables continuous monitoring and tracking of emergency response personnel as they enter an incident area. IPv6 sensors track the vital health signs of response personnel and also report environmental statistics of the response area. As emergency response personnel enter the area, the solution capitalizes on the autoconfiguration and peer-to-peer networking capabilities of IPv6 to enable collaboration and interoperability among the sensors.

Management Considerations in a Dual-Stack Environment

The same operational team that managed Company6's IPv4-only environment now manages the dual-stack environment, using the same tools. During the initial phases of the project, it is not advantageous to manage each protocol separately. The reason is that although data collection and monitoring are important activities, the network-layer version used for these activities makes no difference. Therefore, Company6 is managing its IPv4 and IPv6 networks together rather than separately. Management tools in use at Company6 include:

- CiscoWorks LAN Management Solution 2.5 or later: Cisco Network Analyzer Module, available for the Cisco Integrated Services Router (ISR) and Cisco Catalyst 6500 Series Switches, monitor IPv6 as well as IPv4 traffic.
- Cisco NetFlow for IPv6, for router management: Cisco NetFlow Collector version 5.x or later can be used to analyze NetFlow IPv6 statistics.
- Microsoft Operations Management (MOM) Server for Microsoft Windows and DNS server management.
- Microsoft System Management Server (SMS) for patch deployment and software upgrades.
- An internal application that tracks servers and storage.
- An internal application to manage IP addressing: Cisco Network Registrar 6.2 or later can also be used for naming and addressing services for service provider and enterprise networks.

Security Considerations

Proper security precautions are mandatory for the successful integration of IPv6. Company6 engaged Command Information to provide IPv6 training to its security administrators. Among the security practices that Company6 adopted are:

- *Upgrading to IPv6-aware firewalls:* Many Internet access devices, firewalls, and intrusion prevention systems are not IPv6 aware. Therefore, hackers are already using IPv6 to deliver Trojans and other exploits that covertly send information from the network to the outside. To mitigate this risk, Company6 upgraded its firewalls to Cisco adaptive security appliances (ASAs), which are IPv6-aware.
- *Monitoring, and potentially controlling, all IPv6-over-IPv4 tunnel traffic:* This precaution blocks unwanted or uncontrolled IPv6 traffic over the Company6 network.
- Working around Internet proxies: Internet proxies are not IPv6 compatible. Instead, they either block IPv6 or else let it pass through.
- *Turning off dangerous 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. To mitigate this threat, Company6 uses Cisco Network Access Guardian, which identifies users and their roles and confirms that devices conform to security policy. Part of the company's security policy is to prohibit tunneling. When Cisco Network Access Guardian scans Windows devices and determines they are tunneling, it automatically turns off this feature.
- *Planning addresses for security:* The company uses Cisco ASAs to prevent address scanning, following guidelines in the Cisco SAFE architecture. Some organizations use the CiscoWorks LAN Management System for tracking.
- *Properly using IPv6 security mechanisms:* IPv6 simplifies the use of IPSec for encryption and authentication. IPSec provides end-to-end protection and also protects mobile devices, such as laptops, no matter where they are used.

Other security best practices for IPv6 include:

- Implementing privacy extensions carefully
- Filtering internal-use IPv6 addresses at the enterprise border routers
- Filtering unneeded services at the firewall

- Selectively filtering ICMP
- Maintaining host and application security
- Determining what extension headers will be allowed through the access control device
- Determining which ICMPv6 messages are required
- Denying IPv6 fragments destined to an internetworking device when possible
- Helping ensure adequate IPv6 fragmentation filtering capabilities
- Dropping all fragments with less than 1280 octets, except the last one
- Implementing RFC 2827-like filtering and encourage the service provider to do the same
- Documenting procedures for last-hop traceback
- Using cryptographic protections where critical
- Using static neighbor entries for critical systems
- Implementing ingress filtering of packets with IPv6 multicast source addresses
- Using traditional authentication mechanisms on BGP and IS-IS
- Using IPSec to secure protocols such as OSPFv3 and RIPng
- Using IPv6 hop limits to protect network devices
- Using static tunneling rather than dynamic tunneling
- Implementing outbound filtering on firewall devices to allow authorized tunneling endpoints only

Conclusion

Testing by Company6 and Cisco confirms that the IPv6 solution is working technically as expected, although much work remains. The transition process from IPv4 is not noticeable to the company's employees, customers, or partners. The company has already begun to experience the business benefits of new IPv6-capable applications, such as Windows Meeting Space.

For other organizations preparing to integrate IPv6 into their networks, it is crucial to remember that simply turning on IPv6 does not provide business value. Rather, organizations 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.

Organizations can prepare for IPv6 integration today by following the ten planning steps from Command Information at the beginning of this white paper and setting up a test lab. Most problems with IPv6 result from misconfiguration. By experimenting with application configuration in a lab, IT groups can develop their IPv6 skills and learn the optimum configuration for their business applications before deploying the applications into production.

For More Information

To read more about Cisco IPv6 technology, visit http://www.cisco.com/ipv6.

To read more about IPv6 planning and deployment services from Command Information, visit http://www.commandinformation.com.

To read more about on IPv6 capabilities in Microsoft products and how to modify application code for IPv6, visit http://www.microsoft.com/ipv6.

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

For the current status of IPv4 address depletion, visit http://www.potaroo.net/tools/ipv4.

For the appropriate version of the 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.

About the Companies

Headquartered in San Jose, California, Cisco is the worldwide leader in networking and communications for the Internet. Its IP-based solutions are the foundation of the networks that support business, education, government, and home communications. Cisco has been the primary networking hardware vendor for Company6 for many years.

Headquartered in Herndon, Virginia, Command Information is among the largest IPv6 companies in the United States, and offers strategy, application, network architecture, security services, and IPv6 transition planning to federal and commercial organizations. Company6 engaged Command Information to train its IT staff on IPv6 capabilities, business benefits, and transition options. After the training, the Company6 also engaged Command Information to assist with transition planning.

Headquartered in Redmond, WA, Microsoft is the worldwide leader in software, services, and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to empower people through great software—any time, any place, and on any device.

Printed in USA C11-439724-00 11/07