IPv6 Migration Planning: Help for Getting There from Here

Anticipated and perhaps feared, IPv6 migration planning has begun. The November 2005 deadline for a core infrastructure assessment is long behind us, and now agencies face a February 2006 deadline for submitting a transition plan. By the end of June 2008, all federal agencies must run IPv6 on their network backbones.

But if compliance with the first deadline is any indication, it is clear that agencies need assistance in meeting future milestones. Of the 60 or so departments that Cisco® spoke to at the U.S. IPv6 Summit in Reston, Virginia, fully two-thirds had missed the November 2005 deadline for their infrastructure assessments. "Unquestionably, IPv6 migration is a daunting process and many agencies lack the needed in-house expertise," says Susan Shareshian, program manager for the Cisco Government Services and Support organization. "To avoid risk, many agencies want to work with a services organization that has experience with IPv6 migration in federal government."

Incentives: What Makes It Worthwhile

Even the worst procrastinators understand the eventual necessity of migration. A replacement for today's IPv4, whose pool of network addresses is nearly depleted, IPv6 provides more than enough unique IP addresses for every device on the planet – billions for every square meter on the planet's surface. This provides important new capabilities for federal government, such as equipping each soldier with multiple communications devices and environmental sensors, or ensuring that public safety agencies at all levels of government can communicate and collaborate without the problems caused by duplicate IP addresses.

Best Practices for IPv6 Migration

Therefore, the primary source of delays is not lack of motivation, but rather a desire for expert guidance in managing a task that is no less in magnitude than planning the existing IP environment. Budget concerns are also holding up action. "Most agencies don't know yet how much to budget for IPv6 migration," says Shareshian. "They can discover future budget requirements by starting now with assessment and planning, which cost very little."

For agencies still in the earliest planning stages, Cisco Government Services and Support organization suggests the following best practices:

- *Don't wait: develop a plan now*. Agencies that begin now can enjoy a well-planned evolution rather than an abrupt revolution. In fact, much of the existing equipment in federal agencies is already fully IPv6-capable. Cisco routers, for example, have been IPv6-compatible since early 2001.
- *Plan the migration thoroughly*. Consider activities, budget, time, manpower, and knowledge acquisition. After conducting their network assessments, agencies can take advantage of the Cisco Network Infrastructure Detailed Design Development service to discover the steps needed to comply with OMB mandates, and the optimum sequence. For example, during the transition, which is likely to take years, agencies need to ensure that IPv4 and IPv6 devices and networks can co-exist.
- *Consider network management*. Most existing network management systems support IPv4 only. Agencies will need to either supplement their existing systems with one that supports IPv6, or replace it with a system that supports both environments.

- *Take network security precautions.* "There is a widespread misconception that the new security features of IPv6 make it unnecessary to take any other security actions," says Sharesian. "While IPv6 does, in fact, protect the privacy of data as it travels over the network, it does not prevent unauthorized network access. Therefore, agencies need to plan for at least the same firewall and intrusion prevention systems that they currently have for their IPv4 networks."
- *Enable IPv6 from the network core to the desktop*. Start enabling IPv6 on the network backbone. After that, applications can be migrated one by one, beginning with the applications providing the most business benefit.

How to Get There from Here

Agencies that want help meeting the February 2006 deadline for a transition plan can obtain the following assistance from Cisco Advanced Services:

An *IPv6 Posture Assessment* provides a comprehensive view of the network's IPv6 readiness, developed by conducting a thorough assessment of the agency's Cisco network hardware devices and Cisco IOS® Software releases. Agencies discover areas of concern and the gaps that must be addressed early for a successful migration.

The *Network Infrastructure Detailed Design Development* is a hands-on, collaborative effort between the agency networking staff and Cisco Advanced Services engineers. It includes the IPv6 Posture Assessment as well as staff interviews and a detailed network design review. The deliverable is detailed design documentation that the agency can either execute itself or provide to the third-party implementer.

Federal agencies with complex projects use the *Network Infrastructure Implementation Engineering* service to gain access to the expertise of Cisco Advanced Services engineers for developing an implementation approach, a detailed implementation plan, and either remote or onsite support.

Cisco usually recommends the "dual-stack" approach, in which IPv4 and IPv6 are both supported. But some agencies will want to temporarily disguise IPv6 traffic as IPv4 traffic, or translate between IPv4 and IPv6. "Cisco engineers have hands-on experience with all three approaches and can recommend the best one for the agency's needs," Shareshian says.

Cisco IPv6 Migration Services are intended to transfer knowledge so that federal IT groups can become self-sustaining. "Knowledge transfer is critical because the transition to IPv6 will continue for years as applications are migrated one by one," says Shareshian. "As part of the services, Cisco engineers work with federal staff to teach them what they need to know about migration strategy, implementation, and network operations so that they can assume full control."

For more information, visit: http://www.cisco.com/go/ipv6.

CG/LW10072 01/06