



NEW NETWORKING PROTOCOL REDEFINES COMMUNICATION AND COLLABORATION POSSIBILITIES

BY BEN GOLDMAN, DIRECTOR, PRODUCT MARKETING, INTERNET TECHNOLOGY DIVISION

Federal managers or executives who are not already familiar with IPv6, a new network protocol, will soon need to add it to their vocabularies. This summer, the Office of Management and Budget (OMB) issued a mandate that all federal agencies must run IPv6 on their network backbones by June 30, 2008. Therefore, the question facing agencies is not whether to adopt IPv6, but rather when to begin the deployment and how to manage the transition with as little disruption as possible.

WHY THE PUSH TO IPV6?

What is commonly referred to as simply "IP" is actually Internet Protocol version 4 (IPv4), which the global Internet is rapidly outgrowing. Its fatal flaw is a limited number of IP addresses, with the remaining pool expected to be depleted within this decade. The need to conserve IP addresses so that they don't run out creates another problem, which is the inability to give every IP device a unique IP address that it retains, regardless of where the device is carried. Without this capability, called universal addressing, it is extremely complex, often prohibitively so, to deploy applications in which devices communicate directly rather than through a server. This capability, known as peer-to-peer networking, enables new, powerful applications for communication, collaboration, and operations.

The newest version of IP, IPv6, provides a practically unlimited number of IP addresses: billions and billions for every square meter on the planet. This makes it possible to assign a unique IP address to any device and carry it anywhere in the world, creating new possibilities for increasing agency effectiveness. Military branches, for example, can improve tracking and diagnostics by providing soldiers with multiple sensors to, say, provide their location, report the state of on-board equipment, monitor vital signs, and capture real-time video. Civilian agencies can directly interact with state and local agencies during emergency events without concern for overlapping address spaces, which can prevent communication at a crucial time. While these capabilities are possible with IPv4, they require complex workarounds such as translation, tunneling, and proxies that make the network far more difficult to administer.

THE REWARDS OF A GRADUAL TRANSITION

The good news is that agencies can transition to IPv6 gradually, without disrupting their current network operations. 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.

In most cases, making the transition requires simple software reconfiguration or updates. If older hardware needs to be replaced, agencies can follow their normal lifecycle replacement strategy to minimize the explicit cost to deploy IPv6.

For most federal agencies, the least disruptive path to integration is:

1. Educate network architects and engineers on the difference between the versions.
2. Forecast the budget required for necessary upgrades to networking devices and hosts, keeping in mind that devices requiring hardware upgrades can be replaced as previously planned because IPv4 and IPv6 can co-exist.
3. Establish IPv6 security and connectivity policies, which might or might not differ from the existing policies.

4. Begin enabling IPv6 on network devices. Start at the network backbone and work toward the desktop.
5. Prepare the domain name system (DNS), which translates host names into IP addresses.
6. Upgrade operating systems and applications on user devices such as PCs.

When IPv6 has been enabled on the entire network, agencies can begin using universal addressing and new IPv6-enabled applications.

How long the migration takes varies by agency. Agencies have considerable flexibility in how they plan the transition, because devices that support IPv6 can also run IPv4 for as long as appropriate. By preferring IPv6 wherever it is available, agencies can gracefully transition their devices and applications and avoid the need to explicitly force them over at a later date.

WHY NOT TO DELAY

Beginning the integration of IPv6 now rather than waiting till the 2008 deadline allows time for careful planning for a project that is no less in magnitude than planning the existing IP environment. Although the infrastructure is the cornerstone of the transition, the upgrade of all hosts and their applications to be fully IPv6-capable may continue for years. An advantage of acting now is to gain the operational benefits of IPv6 applications and operating systems for communication, collaboration, and operations as they become available. One application is Microsoft Vista, the next-generation Windows operating system.

Cisco expects that IPv6 and IPv4 will co-exist on networks for a very long time, and therefore has developed expertise and tools to help ensure concurrent operation and a smooth migration. For agencies that want assistance with the transition, Cisco provides services including product compliance, address provisioning and management, routing policies, security, infrastructure design, risks, and opportunities for simplifying the environment.

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



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems
International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. The Cisco Square Bridge logo is a trademark of Cisco Systems, Inc.; and Cisco, Cisco Systems, the Cisco Systems logo, are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Printed in the USA