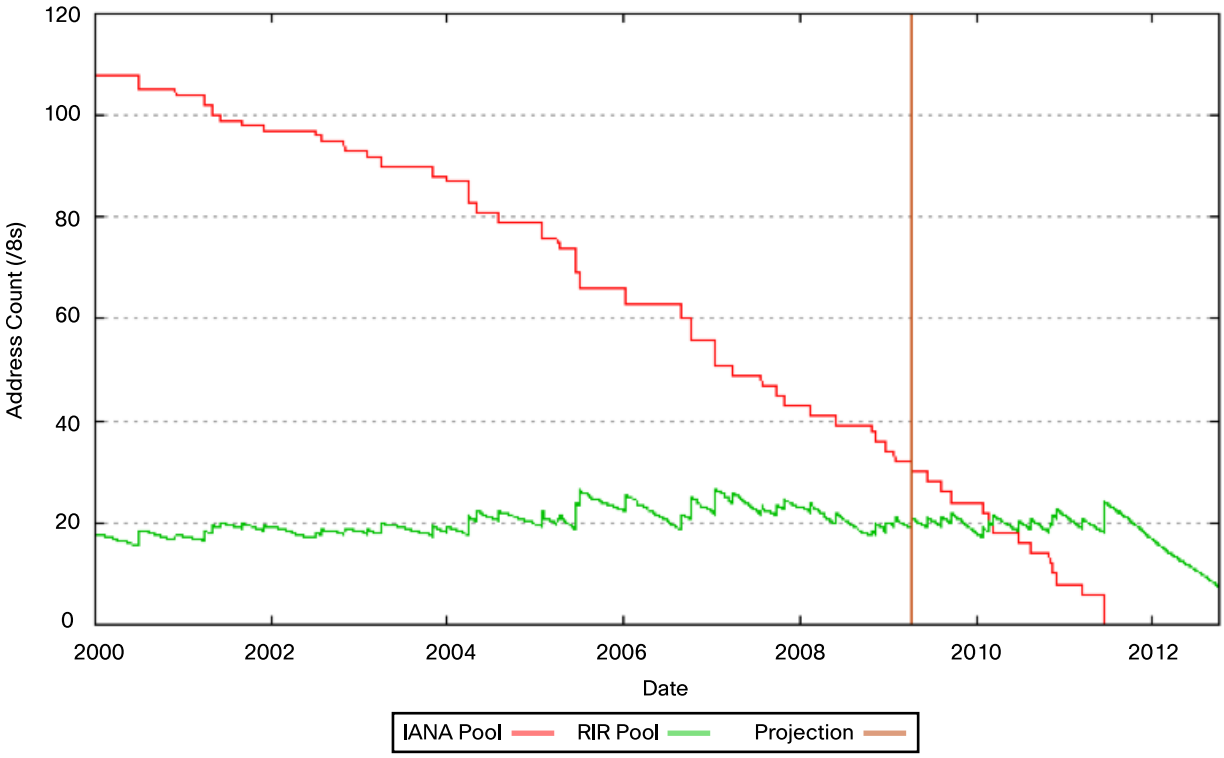
Cisco Catalyst 6500: Building IPv6-Ready Campus Networks

Why IPv6 Is Important

The Internet has grown so rapidly that the IPv4 standard can no longer support the number of users and functions. Figure 1 shows the prediction of IPv4 address-space exhaustion. Features such as Network Address Translation (NAT) can help overcome address-space limitations, but they also make bidirectional communication for primary triple-play (data, voice, and video) applications more challenging.

Figure 1. The prediction of IPv4 Address-Space Exhaustion (by Geoff Huston)



In the figure, the red line indicates the number of /8 address blocks remaining in the Internet Assigned Numbers Authority (IANA) free pool. The green line indicates the number of /8 address blocks available in Regional Internet Registry (RIR) free address pools. The vertical line indicates today.

IPv6, as the next generation of Internet Protocol, is tasked to fix numerous problems in IPv4. Of primary importance is the limited number of available IPv4 addresses. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, providing more than enough globally unique IP addresses for every networked device on the planet. In addition to its large address space, IPv6 offers other advantages over IPv4, including:

- Reduces operating expenses (OpEx) and configuration by facilitating autoconfiguration capabilities
- Enables better network bandwidth efficiency using multicast and anycast instead of broadcast
- Offers an easy way to enable new applications in mobility and in the data center with anycast support
- Offers more granular control of quality of service (QoS) with built-in flow-class capability

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- Provides unified framework for security
- Enables faster handover, route optimization, and hierarchical mobility

IPv6 Market Factors

The primary market factors for growing adoption of IPv6 follow:

- IPv4 address-space depletion, which is limiting the expansion of enterprises into emerging markets
- Growing support for IPv6 applications, including operating systems such as Microsoft Vista and Windows 7 server
- National IT strategy: The established goal for all federal government agency networks was to support IPv6 by June 30, 2008 (based on Memorandum M-05-22, “Transition Planning for Internet Protocol Version 6 (IPv6)”, issued in August 2005 by the Office of Management Budget).
- Infrastructure evolution where networks are being designed with IPv6 as baseline, including DOCSIS® 3.0, quadruple play (data, voice, video, and mobility), mobile service providers, Networks in Motion, networked sensors, etc.

IPv6 Network Deployment Requirements

With increased adoption of IPv6, enterprise customers are looking to build architecture that can provide (Figure 2):

- Optimized nonstop communication IPv6 delivery across the entire network
- Network infrastructure to support “transition technologies” to allow both IPv4 and IPv6 networks to run concurrently, because the transition of applications and enterprise networks from IPv4 to IPv6 will probably take several years
- Access security to IPv6 hosts and secure IPv6 transport through public networks
- Scalability and performance to support IPv6 growth

Figure 2. Smooth Migration to IPv6

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Building IPv6 Networks with Cisco Catalyst 6500

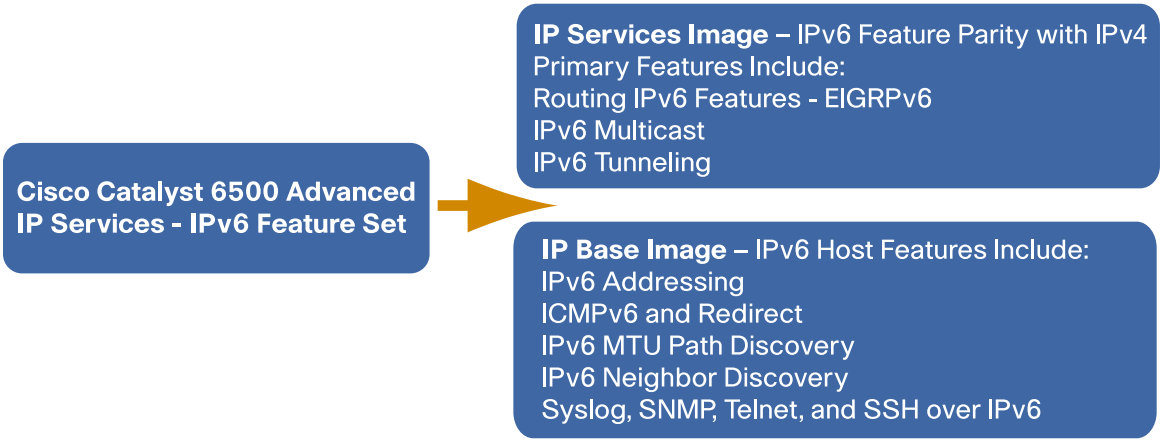
Cisco is a technology leader for enabling IPv6 functions (both hardware and software). The premier Cisco® Catalyst® switching platform, the Cisco Catalyst 6500, leads IPv6 innovations by extending support of dual-stack architecture starting with Cisco IOS® Software Release 12.2(33)SXI. This Cisco IOS Software release offers IPv6 customers the following benefits:

- Offers flexibility to deploy end-to-end dual-stack IPv4 and IPv6 campus networks
- Extends benefits of network virtualization to IPv6 running devices with IPv6 VPN over MPLS (6VPE) and IPv6 support on the Cisco Catalyst 6500 Virtual Switching System (VSS)
- Enables network infrastructure management across IPv6 networks
- Helps ensure secure IPv6 transport across public networks with hardware-accelerated IP Security (IPsec) encryption
- Increases adoption of IPv6 by making the same software functions available for IPv6 as for IPv4

IPv6 Repackaging

Cisco is committed to help IPv6 customers enable dual-stack campus architecture by making the same software feature licensing available for IPv6 as for IPv4, leading with Cisco IOS Software Release 12.2(33)SXI on the Cisco Catalyst 6500. Prior to Release 12.2(33)SXI customers had to pay a premium for basic IPv6 functions, but with the IPv6 feature repackaging changes in this release, this premium no longer applies. IPv6 feature licensing will follow the IPv4 model for Cisco IOS Software Release 12.2(33)SXI, as shown in Figure 3.

Figure 3. IPv6 Feature Licensing



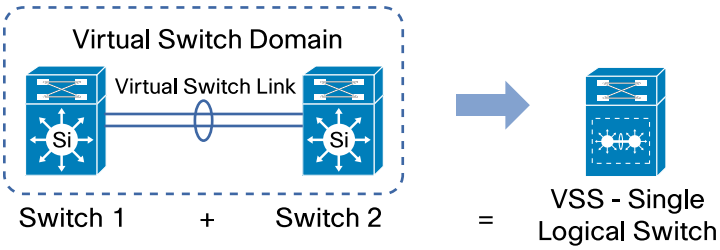
IPv6 Network Virtualization

Support for IPv6 with VSS

The Cisco Catalyst 6500 Virtual Switching System (VSS) is an exciting innovation on the Cisco Catalyst 6500 platform. It allows clustering of two Cisco Catalyst 6500 Switches together to form a single logical switching entity with 1.44-Tbps bandwidth capacity. It provides enhancements in different areas of enterprise campus and data center deployment, including high availability, network resiliency, scalability and performance, management, and maintenance. Figure 4 shows the physical and logical representation of VSS.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 4. Physical and Logical Representation of VSS



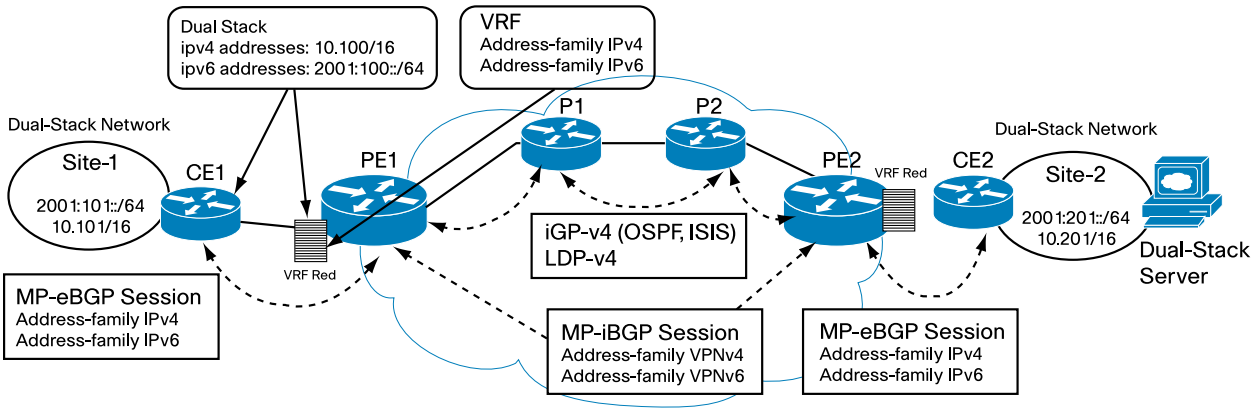
Widely adopted since its introduction in 2008, VSS is required to support scalable, reliable IPv6 networks. Cisco IOS Software Release 12.2(33)SXI2 on the Cisco Catalyst 6500 extends VSS support to IPv6 with the same feature set as non-VSS Cisco Catalyst 6500 systems. This enhancement allows for deployment of IPv4 and IPv6 dual-stack or IPv6 tunneling architectures on a Cisco Catalyst Virtual Switching System.

IPv6 VPN over MPLS

The Cisco 6VPE solution smoothly introduces scalable IPv6 VPN service, without affecting the existing well-controlled IPv4 backbone. For customers running IPv4, the IPv6 VPN service is exactly the same as running Multiprotocol Label Switching (MPLS) VPN for IPv4.

The IPv6 MPLS VPN operation model is similar to that of IPv4 MPLS VPNs. Enterprise customers who have already deployed MPLS IPv4 VPN services over an IPv4 backbone can deploy IPv6 MPLS VPN services over the same IPv4 backbone by upgrading the provider-edge (PE) router Cisco IOS Software and adding dual-stack configuration, without any change on the core routers. IPv4 services can be provided in parallel with IPv6 services. A provider edge-customer edge link can be an IPv4 link, an IPv6 link, or a combination of an IPv4 and IPv6 link, as shown in Figure 5.

Figure 5. IPv6 VPN over MPLS (6VPE) Operation



The IPv6 and IPv4 VPNs use the same components, including: Multiprotocol Border Gateway Protocol (MP-BGP) VPN address family, Route Distinguishers (RDs), Virtual Route Forwarding (VRF) instances, Site of Origin (SoO), and extended community.

The 6VPE router exchanges reachability information with the other 6VPE routers in the MPLS domain using MP-BGP, and shares a common IPv4 routing protocol (such as Open Shortest Path First [OSPF] or Intermediate System-to-Intermediate System [IS-IS]) with the other provider (P) routers and provider-edge routers in the domain. Separate routing tables are maintained for the IPv4 and IPv6 stacks. A hierarchy of MPLS labels is imposed on an incoming customer IPv6 packet at the provider-edge router:

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- Outer label (Interior Gateway Protocol [IGP] label) for internal BGP (iBGP) next hop, distributed by Label Distribution Protocol (LDP)
- Inner label (VPN label) for the IPv6 prefix, distributed by MP-BGP

Incoming customer IPv6 packets at the 6VPE VRF interface are transparently forwarded inside the service provider's IPv4 core, based on MPLS labels, eliminating the need to tunnel IPv6 packets. Provider routers inside the MPLS core are unaware that they are switching IPv6-labeled packets.

Encrypting IPv6 Traffic Across Public Domains with VSPA

IPsec has been widely deployed as a pervasive VPN solution to achieve data confidentiality, data integrity, and data authentication at the network layer (for example, Layer 3 of the OSI seven-layer networking model). The requirement on IPsec VPN performance in the network has been increasing as more and more enterprises become multinational and adopt the latest collaboration technology and tools such as video telephony, web collaboration, e-communities, information sharing, etc.

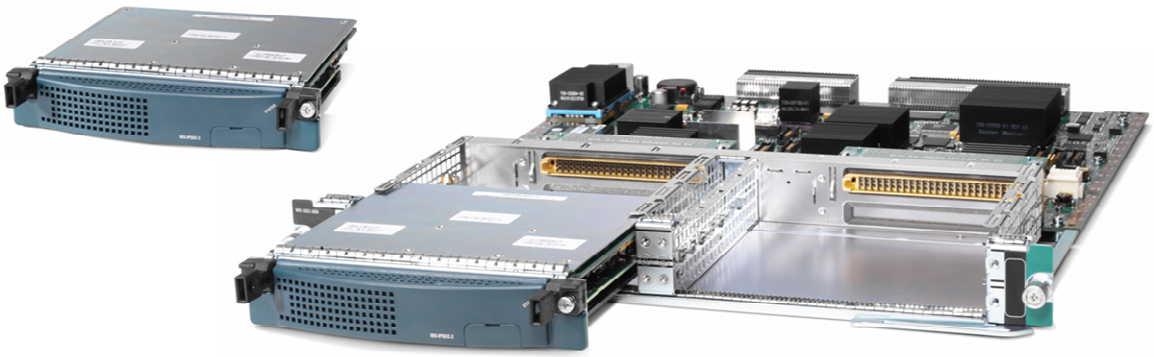
Designed from the beginning with security in mind, IPv6 has IPsec as a mandatory component; hence the IPsec security model must be supported for all IPv6 implementation. For a large production deployment, the IPsec encapsulation must be hardware-accelerated so that it can meet the performance requirement.

The Cisco Catalyst 6500 VPN Services Port Adapter (VSPA), shown in Figure 6, answers such demands by providing integrated high-performance IPsec VPN services for both IPv4 and IPv6 in a modular, flexible, and scalable form factor. A single VSPA supports multigigabit IPv6 IPsec traffic, and can scale up to 10 VPSAs on a single Cisco Catalyst 6500 chassis.

VSPA requires the Cisco Catalyst 6500 Series Services SPA Carrier-600 (SSC-600) to operate in the Cisco Catalyst 6500 Series Switches. Each SSC-600 module takes up one slot in a Cisco Catalyst 6500 Series Switch and can support up to two Cisco VPN Services Port Adapters.

Having VSPA support for both IP versions, the Cisco Catalyst 6500 Series Switches enable secure IPv4 and IPv6 dual-stack implementations with investment protection.

Figure 6. Cisco Catalyst 6500 VPN Services Port Adapters (VSPA) and Carrier-600 (SSC-600)



© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Enabling Dual-Stack Architectures with Cisco Catalyst 6500

EIGRP for IPv6

In addition to OSPF for IPv6 (OSPFv3) and Routing Information Protocol for IPv6 (RIPng), the Cisco IOS Software Release 12.2(33)SXI introduces Enhanced IGRP (EIGRP) support for IPv6. By upgrading their Cisco IOS Software to Release 12.2(33)SXI, customers can now enable dual-stack IPv4 and IPv6 EIGRP deployment in their campus networks.

Despite the commonality of EGRIP for IPv4 and IPv6, there are some differences when configuring EIGRP for IPv6:

- EIGRP for IPv6 is directly configured on the interfaces over which it runs. This feature allows EIGRP for IPv6 to be configured without the use of a global IPv6 address. There is no network statement in EIGRP for IPv6.
- EIGRP for IPv6 has a shutdown feature. The routing process should be in "no shutdown" mode in order to start running.
- When a passive-interface configuration is used, EIGRP for IPv6 does need not to be configured on the interface that is made passive.
- EIGRP for IPv6 provides route filtering using the **distribute-list prefix-list** command. The **route-map** command is not supported for route filtering with a distribute list.

First-Hop Redundancy Protocols for IPv6

The Cisco IOS Software Release 12.2(33)SXI introduces two First Hop Redundancy Protocols (FHRP) for IPv6 onto the Cisco Catalyst 6500 Switches, including:

- Hot Standby Router Protocol (HSRP) for IPv6
- Gateway Load Balancing Protocol (GLBP) for IPv6

HSRP and GLBP provide redundancy and high availability of the first-hop gateway to host devices, and GLBP extends this function to offer first-hop gateway load balancing as well.

HSRP for IPv6

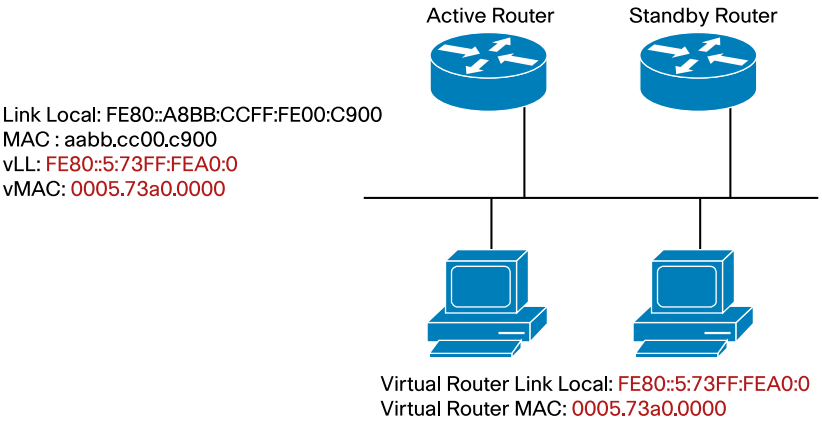
HSRP is designed to provide redundancy of the first-hop gateway to host devices. An active router and a standby router are elected within a HSRP group based on router priority. The active router assumes the active gateway role and is the only router in the group to forward traffic for the host devices. The standby router takes over when the active router fails or when preset conditions are met.

IPv6 hosts learn of available IPv6 routers through IPv6 neighbor discovery router-advertisement (RA) messages. These messages are multicast periodically, or may be solicited by hosts.

An HSRP IPv6 group has a virtual MAC address and a virtual IPv6 link-local address. The virtual MAC address is derived from the HSRP group number and is in the range of 0005.73A0.0000 through 0005.73A0.0FFF (4096 addresses). The virtual IPv6 link-local address is, by default, derived from the virtual MAC address. Periodic router-advertisement messages for the HSRP virtual IPv6 link-local address are sent to host devices when the HSRP group is active. Figure 7 depicts HSRP for IPv6.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 7. HSRP for IPv6



HSRP IPv6 uses a different virtual MAC address block than IPv4: 0005.73A0.0000 through 0005.73A0.0FFF (4096 addresses).

HSRP IPv6 uses User Datagram Protocol (UDP) port 2029.

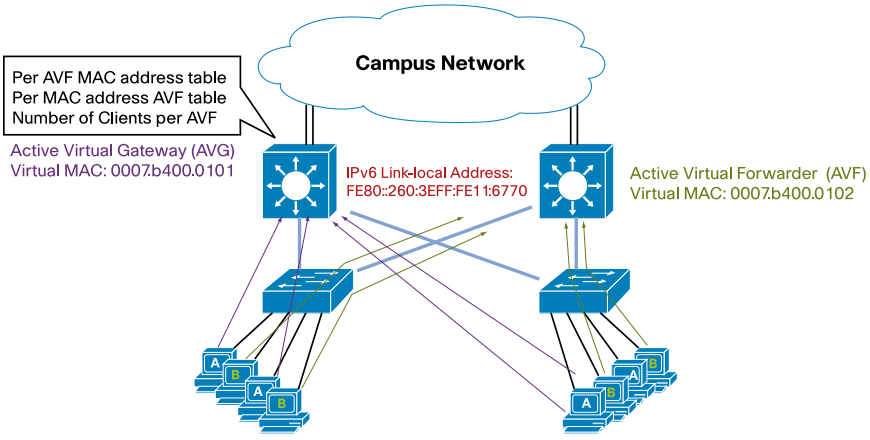
GLBP for IPv6

GLBP provides the first-hop gateway redundancy for IPv6 hosts - a function similar to HSRP. The difference between these two protocols exists in the way the protocols use the bandwidth of standby routers.

In HSRP, only the active router forwards packets for the hosts, while the other routers sit idle until the active router fails. Therefore, the bandwidth of the other routers is not used for forwarding traffic.

In GLBP, members of a GLBP group elect one router to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG if the AVG becomes unavailable. The AVG assigns a virtual MAC address to each member of the GLBP group. Each router assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These routers are known as active virtual forwarders (AVFs) for their virtual MAC address. For IPv6, AVG is responsible to send router-advertisement packets with the group virtual IPv6 link-local address to hosts. It alternates the source virtual MAC addresses while sending router-advertisement packets to different hosts. As a result, hosts use a different AVF as their gateway. Figure 8 depicts GLBP for IPv6.

Figure 8. GLBP for IPv6



	Hosts in A	Hosts in B
Default Gateway	FE80::260:3EFF:FE11:6770	FE80::260:3EFF:FE11:6770
Gateway MAC	0007.b400.0101	0007.b400.0102

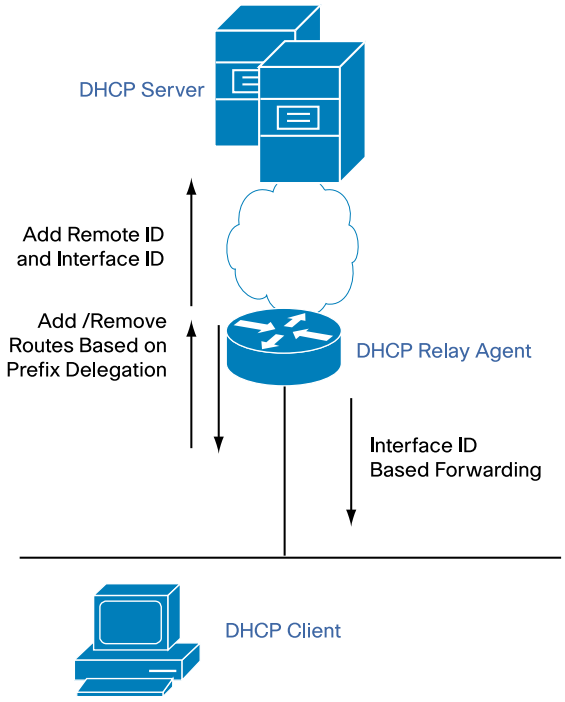
© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

DHCP for IPv6 Relay Agent Options

DHCP Relay Agent for IPv6 allows IPv6 routers to be relay agents to forward IPv6 DHCP packets between host devices and IPv6 DHCP servers. Cisco IOS Software Release 12.2(33)SXI introduces the following Relay Agent options to the Cisco Catalyst 6500 platform (Figure 9):

- Remote ID (RFC 4649) is inserted, allowing address selection at the server side.
- Interface ID (RFC 3315) is inserted, so DHCPv6 packets are forwarded back to the client.
- Prefix Delegation option (RFC 3633) is snooped and matching routes are inserted or removed.

Figure 9. DHCP for IPv6 Relay Agent Options



For more details about these options, please refer to the following URL:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp_ps6017_TSD_Products_Configuration_Guide_Chapter.html#wp1054045.

The DHCP for IPv6 Relay Agent function on the Cisco Catalyst 6500 is enhanced by these options.

IPv6-Ready Phase 2 Logo

The IPv6 Forum (http://www.ipv6forum.com) IPv6 Ready Logo program is a conformance and interoperability-testing program intended to increase user confidence by demonstrating that IPv6 is available now and is ready to be used. Figure 10 shows the IPv6-ready Phase 2 logo.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 10. IPv6-ready Phase 2 Logo

The Phase 2 logo expands the "core IPv6 protocols" test coverage to approximately 450 tests and adds new extended test categories. The Phase 2 Gold logo verifies optimum compliance after the complete series of tests, including the "MUST" and the recommended "SHOULD" parameters for the IETF specifications testing. The IPv6 Forum strongly encourages vendors to obtain the IPv6-Ready Phase 2 logo. The Phase 2 logo extended test categories include:

- IPsec
- Internet Key Exchange Version 2 (IKEv2)
- Mobile Internet Protocol Version 6 (MIPv6)
- Network Mobility (NEMO)
- DHCPv6
- Session Initiation Protocol (SIP)
- Management (Simple Network Management Protocol [SNMP] MIBs)
- MLD

The Cisco Catalyst 6500 is among the first Cisco Catalyst platforms to be IPv6 Phase 2 Logo certified.

For more information about the IPv6 Ready Logo program, please visit: http://www.ipv6ready.org/?page=home.

Conclusion

IPv6, as the next generation of Internet Protocol, is designed to solve the IPv4 address-space depletion problem and provide numerous other benefits. However, the transition between today's IPv4 Internet and a future IPv6-based one will be a long process during which both protocol versions will coexist.

The Cisco IOS Software Release 12.2(33)SXI release train enhances the IPv6 features on Cisco Catalyst 6500 Series Switches by providing:

- Investment protection with support for dual-stack IPv4 and IPv6 deployment
- Lower-cost ownership of IPv6-enabled networks with IPv4 and IPv6 feature packaging parity
- Network virtualization with 6VPE and IPv6 VSS support
- Secure IPv6 transport across public networks with hardware-accelerated IPsec encryption on VSPA

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx 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. (0903R)

Printed in USA C22-531339-00 04/09

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.