

Cisco IOS[®] IPv6

A stylized graphic of a globe with white grid lines on a blue background, positioned on the left side of the page.

Introduction

The continuous growth of the global Internet requires that the overall architecture evolve to accommodate new technologies that support increasing numbers of users, applications and services. Internet Protocol Version 6 (IPv6) is designed to enable ongoing Internet expansion.

Cisco Systems, leveraging its leadership in defining and delivering IP networks, believes in providing its customers and partners with comprehensive information regarding significant emerging technologies, so that they are fully informed and can work jointly with Cisco to implement the best solutions for their environments. Therefore this Statement-of-Direction addresses IPv6, articulating the Cisco position and detailing current and future support across Cisco's strategic product family via Cisco IOS[®] Software. It also discusses the IPv6 technologies, considers business drivers, migration scenarios, and standards status in order to provide sufficient information to enable customers to make the right planning decisions for their networks.

Market Drivers

Overall market adoption of IPv6 will be determined by the ability of the architecture to best accommodate Internet growth, new applications and compelling IP Services. These factors underscore the original rationale behind IPv6 definition and the market drivers for evolution that are evaluated below.

In terms of IP Services integrated into the architecture, IPv6 (formerly known as IP Next Generation, 'IPng') most notably offers expanded IP addresses, integrated auto-configuration, quality-of-service (QoS), enhanced mobility and end-to-end security.

The IETF IPng Working Group quadrupled the IP address length (to 128 bits) to meet anticipated future demand for IP addresses. The net result of this expansion provides thousands of addresses for each individual throughout the global population, using only a fraction of the IPv6 address space. At the same time, a hierarchical addressing structure has been proposed for IPv6 that is designed to reduce the size of Internet routing tables. In order to facilitate Intranet-wide address management, stateless address auto-configuration techniques were built in, enabling large numbers of IP hosts to easily discover the network and get an IPv6 address associated with their location. It is expected that future IETF work on the address structure will provide enhanced multi-homing capabilities. Support for class-of-service comes in the form of a 'Traffic Class' field compliant with the IETF Differentiated Services (DiffServ) model. To meet networking security requirements, the IP Security Architecture (IPSec) is mandatory.

In incorporating support for emerging services, IP version 6 effectively acted as a catalyst for the introduction of these key capabilities into IPv4 implementations such that we now have the functionality equivalence shown below:

IP Service	IPv4 Solution	IPv6 Solution
Addressing Range	32-bit, Network Address Translation	128-bit, Multiple Scopes
Autoconfiguration	DHCP	Serverless Configuration, Reconfiguration, DHCP
Security	IPSec	IPSec Mandated, works End-to-End
Mobility	Mobile IP	Mobile IP with Direct Routing
Quality-of-Service	Differentiated Service, Integrated Service	Differentiated Service, Integrated Service
IP Multicast	IGMP/PIM/Multicast BGP	MLD/PIM/Multicast BGP, Scope Identifier

Therefore, given these comparable services now currently offered by IPv4, the compelling IPv6 benefits center on its expanded and global addressing, serverless auto-configuration and direct-path mobile IP since these allow for continued growth in the number of IP devices and applications uniquely addressed and connected to the Internet.

The emerging applications fueling demand for addresses include Internet Appliances, Internet-enabled wireless devices such as personal digital assistants (PDAs), home area networks (HANs), Net-connected automobiles and integrated telephony services (as voice migrates to an IP transport). In particular, “always-on” environments for devices and applications that must be reachable by communication initiated externally, for example the shift in residential Internet access to use broadband technologies such as DSL, cable modem or Ethernet-to-the-Home, preclude address conservation techniques such as IP address pooling/leasing. Also the anticipated rollout of wireless data services has been identified as a key IPv6 driver, this reflected in the fact that the relevant industry standardization bodies, e.g. the 3rd Generation Partnership Project (www.3gpp.org), Universal Mobile Telecommunication System (www.umts-forum.org) and Mobile Wireless Internet Forum (www.mwif.org), consider IPv6 as the foundation for future IP services.

Aside from these applications that extend the Internet’s functionality for existing users, consideration must be given to the global population and the requirements that for example, highly populous nations will place on current Internet addressing.

Existing IPv4 Addressing Solutions

Current Internet growth, from the perspective of IPv4 addressed devices, has been sustained by the fact that, for today’s dominant applications (such as email and the web), access to the global Internet does not require globally unique addresses for most devices. Current Network Address Translation (NAT) techniques deployed at the boundaries of public Internet have enabled the widespread reuse of non-unique or unregistered IPv4 addresses while still providing the limited connectivity required by today’s applications. This involves translating the IP addresses of packets as they are switched between internal, privately addressed networks into a public network such as the Internet. It should be noted that translation techniques such as NAT-PT (Network Address Translation and Protocol Translation) will play a pivotal role in the integration of IPv6 into production networks since the ability to also translate between IPv4 and IPv6 address families ensures that connectivity between the two domains is preserved.

IPv4 address management techniques could prove too cumbersome in certain emerging markets, however recognizing that different networks and applications have different underlying needs, Cisco is committed to develop IPv4 addressing solutions as well as IPv6.



Integration and Coexistence

Fundamental to the successful market adoption of a new architecture or technology suite is the ability to integrate it with an existing infrastructure without significant disruption to services. Given the magnitude of the task involved in replacing today's IPv4 with the new IPv6, integration and coexistence need to be well defined and planned and this has been the focus of the IETF Next Generation Transition (NGtrans) Working Group for several years. There is however no reason to expect a full migration to the new IPv6 and for an indefinite period both IPv4 and IPv6 nodes will coexist. In tackling IPv6 integration into IPv4 networks, the approach taken has been to partition the tasks into the host/client portion and the network portion. Several techniques have been identified and are explained in the following sub-sections and it is reasonable to anticipate that significant deployments of IPv6 will employ a combination of these mechanisms. Further information is currently available at:

<http://www.ietf.org/internet-drafts/draft-ietf-ngtrans-introduction-to-ipv6-transition-06.txt>

The Cisco IOS implementation of IPv6 includes support for the main integration techniques and adheres to the following overall objectives:

- Deployment of IPv6 services when/where needed
- No disruption of IPv4 services
- IPv4/IPv6 services between Hosts/Applications
- Incremental upgrade and deployment, No 'Flag Day'
- Minimize operational cost, learning curve and support requirements

Selecting a Deployment Strategy

The key strategies used in deploying IPv6 at the edge of a network involve carrying IPv6 traffic over the IPv4 network, allowing isolated IPv6 domains to communicate with each other before the full transition to a native IPv6 backbone. It is also possible to run IPv4 and IPv6 throughout the network, from all edges through the core, or to translate between IPv4 and IPv6 to allow hosts communicating in one protocol to communicate transparently with hosts running the other protocol. All techniques allow networks to be upgraded and IPv6 deployed incrementally with little to no disruption of IPv4 services.

The four key strategies for deploying IPv6 are as follows:

- Deploying IPv6 over IPv4 tunnels: These tunnels encapsulate the IPv6 traffic within the IPv4 packets, and are primarily for communication between isolated IPv6 sites or connection to remote IPv6 networks over an IPv4 backbone. The techniques include using manually configured tunnels, generic routing encapsulation (GRE) tunnels, semiautomatic tunnel mechanisms such as tunnel broker services, and fully automatic tunnel mechanisms such as IPv4-compatible and 6to4.
- Deploying IPv6 over dedicated data links: This technique enables isolated IPv6 domains to communicate by using the same Layer 2 infrastructure as for IPv4, but with IPv6 using separate Frame Relay or ATM PVCs, separate optical links, or dense Wave Division Multiplexing (dWDM).
- Deploying IPv6 over MPLS backbones: This technique allows isolated IPv6 domains to communicate with each other, but over an MPLS IPv4 backbone. Multiple techniques are available at different points in the network, but each requires little change to the backbone infrastructure or reconfiguration of the core routers because forwarding is based on labels rather than the IP header itself.
- Deploying IPv6 using dual-stack backbones: This technique allows IPv4 and IPv6 applications to coexist in a dual IP layer routing backbone. All routers in the network need to be upgraded to be dual-stack with IPv4 communication using the IPv4 protocol stack and IPv6 communication using the IPv6 stack.

Table 1 summarizes the primary use and benefit for each strategy.

Table 1 Deployment Strategies: Primary Uses and Benefits

Deployment Strategy	Key User/Primary Use	Benefits
IPv6 over IPv4 Tunnels	Service provider wanting to offer initial IPv6 service. Enterprise wanting to interconnect IPv6 domains or link to remote IPv6 networks.	Can demonstrate demand for IPv6 for minimal investment. Easy to implement over existing IPv4 infrastructures. Low cost, low risk.
IPv6 over Dedicated Data Links	Service provider WANs or metropolitan area networks (MANs) deploying ATM, Frame Relay, or dWDM.	Can provide end-to-end IPv6 with no impact on the IPv4 traffic and revenue.
IPv6 over MPLS Backbones	Mobile or greenfield service providers, or current regional service providers deploying MPLS.	Integrates IPv6 over MPLS, thus no hardware or software upgrades required to the core.
IPv6 Using Dual-Stack Backbones	Small enterprise networks.	Easy to implement for small campus networks with a mixture of IPv4 and IPv6 applications.

In addition to the strategies for deploying IPv6 within your IPv4 environment, you also need protocol translation mechanisms (for example, a NAT-PT device to connect IPv6-only web browsers to IPv4-only web servers) or dual-stack servers (for example, an e-mail server that handles IPv4-only and IPv6-only mail clients) to allow communication between applications using IPv4 and applications using IPv6. These mechanisms become increasingly important as IPv6 deployment moves from the testing to the actual usage phase, and more relevant as application developers decide that continuing to support IPv4 is not cost-effective.

Eventually, as IPv6 becomes the protocol of choice, these mechanisms will allow legacy IPv4 systems to be part of the overall IPv6 network. The mechanisms translate between the IPv4 and IPv6 protocols on the end system, or on a dedicated server, or on a router within the IPv6 network, and, together with dual-stack hosts, provide a full set of tools for the incremental deployment of IPv6 with no disruption to the IPv4 traffic.

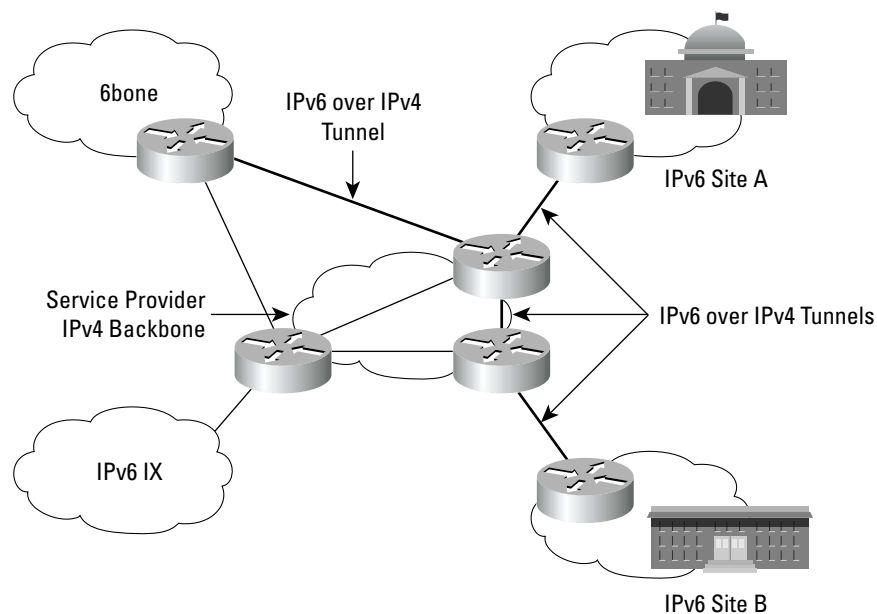


Deploying IPv6 over IPv4 Tunnels

Tunneling is the encapsulation of IPv6 traffic within IPv4 packets so they can be sent over an IPv4 backbone, allowing isolated IPv6 end systems and routers to communicate without the need to upgrade the IPv4 infrastructure that exists between them. Tunneling is one of the key deployment strategies for both service providers and enterprises during the period of IPv4 and IPv6 coexistence. Figure 1 shows the use of IPv6 over IPv4 tunnels.

Tunneling allows service providers to offer an end-to-end IPv6 service without major upgrades to the infrastructure and without impacting current IPv4 services. Tunneling allows enterprises to interconnect isolated IPv6 domains over their existing IPv4 infrastructures, or to connect to remote IPv6 networks such as the 6bone.

Figure 1 Deploying IPv6 over IPv4 Tunnels



A variety of tunnel mechanisms are available. These mechanisms include manually created tunnels such as IPv6 manually configured tunnels (RFC 2893) and IPv6 over IPv4 GRE tunnels, semiautomatic tunnel mechanisms such as that employed by tunnel broker services, and fully automatic tunnel mechanisms such as IPv4-compatible and 6to4. Manual and GRE tunnels are used between two points and require configuration of both the source and destination ends of the tunnel, whereas automatic tunnel mechanisms need only to be enabled and are more transient—they are set up and taken down as required, and last only as long as the communication.

IPv6 for Cisco IOS software supports IPv6 manually configured, IPv6 over IPv4 GRE, IPv4-compatible, and 6to4 tunnel mechanisms. Tunnel broker services are provided by service providers.

Other tunnel techniques, such as ISATAP and 6over4, are available for use over campus networks or for the transition of local nonrouter sites.

The ISATAP tunneling mechanism is very similar to 6to4 tunneling, with the IPv4 address embedded in the lower 32 bits rather than the upper 48 bits of the IPv6 address. Cisco plans to support ISATAP tunnels in the next phase of IPv6 for Cisco IOS software.

The 6over4 mechanism maps IPv6 multicast addresses into IPv4 multicast addresses, determining the endpoint of the tunnel using neighbor discovery. The mechanism emulates a virtual link layer or Ethernet within the site, but note that IPv4 multicast routing is a prerequisite. Cisco does not plan to support 6over4 within Cisco IOS software, and we recommend use of ISATAP tunneling when available, or use of native IPv6 routing within the campus.

Table 2 summarizes the primary use, benefits, and limitations for each tunneling mechanism.

Table 2 Overlay Tunnel Mechanisms: Primary Uses, Benefits, and Limitations

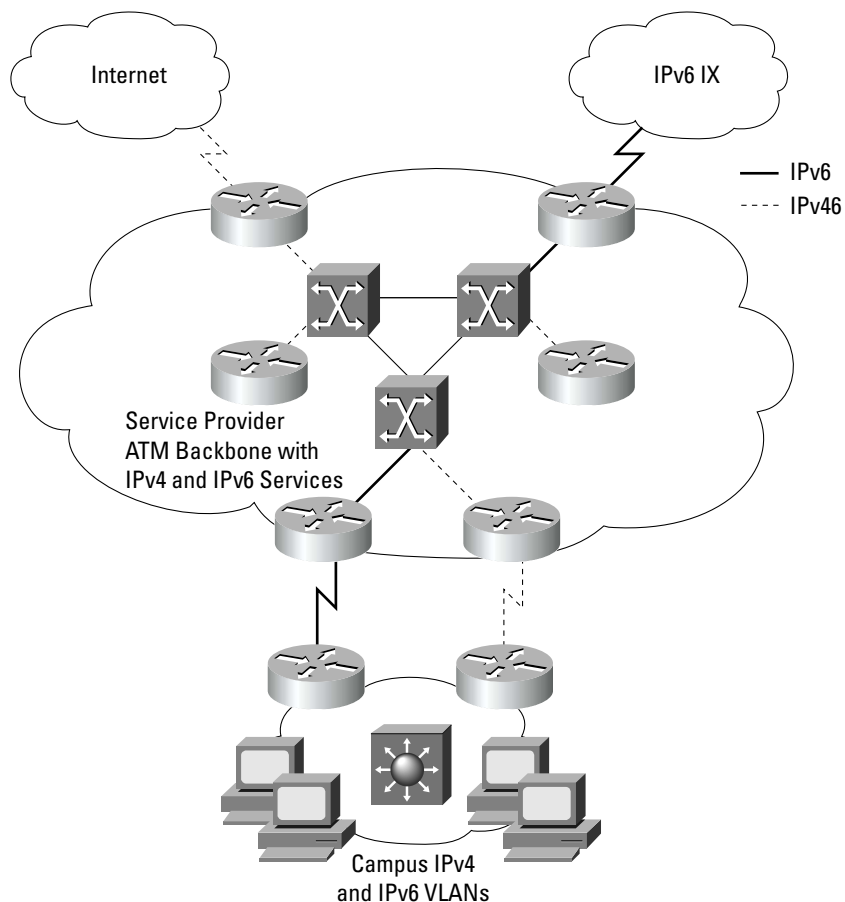
Tunnel Mechanism	Primary Use	Benefits
IPv6 Manually Configured Tunnel	Stable and secure links for regular communication. Connection to 6bone.	Supported in IPv6 for Cisco IOS software now. DNS with support for IPv6 not required.
IPv6 over IPv4 GRE Tunnel	Stable and secure links for regular communication.	Well-known standard tunnel technique. Supported in IPv6 for Cisco IOS software now.
Tunnel Broker	Standalone isolated IPv6 end systems.	Tunnel set up and managed by ISP.
Automatic IPv4-Compatible Tunnel	Single hosts or small sites. Infrequent communication.	Supported in IPv6 for Cisco IOS software now.
Automatic 6to4 Tunnel	Connection of multiple remote IPv6 domains. Frequent communication.	Easy to set up with no management overhead. Supported in IPv6 for Cisco IOS software now.
ISATAP Tunnels	Campus sites. Transition of nonrouted sites.	To be supported in the next phase of Cisco IOS software.
6over4 Tunnels	Campus sites. Transition of nonrouted sites.	—



Deploying IPv6 over Dedicated Data Links

Many WANs and MANs have been implemented by deploying Layer 2 technologies such as Frame Relay, ATM, or optical, and are beginning to use dWDM. Figure 2 shows a sample configuration for IPv6 over dedicated data links.

Figure 2 IPv6 over Dedicated Data Links



Routers attached to the ISP WANs or MANs can be configured to use the same Layer 2 infrastructure as for IPv4, but to run IPv6, for example, over separate ATM or Frame Relay PVCs or separate optical lambda. This configuration has the added benefit for the service provider of no loss in service or revenue for the IPv4 traffic.

IPv6 for Cisco IOS software supports IPv6 over dedicated data links.

Deploying IPv6 over MPLS Backbones

IPv6 over MPLS backbones enables isolated IPv6 domains to communicate with each other over an MPLS IPv4 core network. This implementation requires far fewer backbone infrastructure upgrades and lesser reconfiguration of core routers because forwarding is based on labels rather than the IP header itself, providing a very cost-effective strategy for the deployment of IPv6.

Additionally, the inherent Virtual Private Network (VPN) and traffic engineering services available within an MPLS environment allow IPv6 networks to be combined into VPNs or extranets over an infrastructure supporting IPv4 VPNs and MPLS-TE.

A variety of deployment strategies are available or under development, as follows:

- IPv6 using tunnels on the customer edge (CE) routers
- IPv6 over a circuit transport over MPLS
- IPv6 on the provider edge (PE) routers (known as 6PE)

The first of these strategies has no impact on and requires no changes to the MPLS provider (P) or PE routers because the strategy uses IPv4 tunnels to encapsulate the IPv6 traffic, thus appearing as IPv4 traffic within the network. The second of these strategies, only available on specific Cisco routers such as the Cisco 12000 and 7600 Internet routers, also requires no change to the core routing mechanisms. The last strategy requires changes to the PE routers to support a dual-stack implementation, but all the core functions remain IPv4.

Table 3 summarizes the primary use, benefits, and limitations for each MPLS mechanism.

Table 3 MPLS Mechanisms: Primary Uses and Benefits

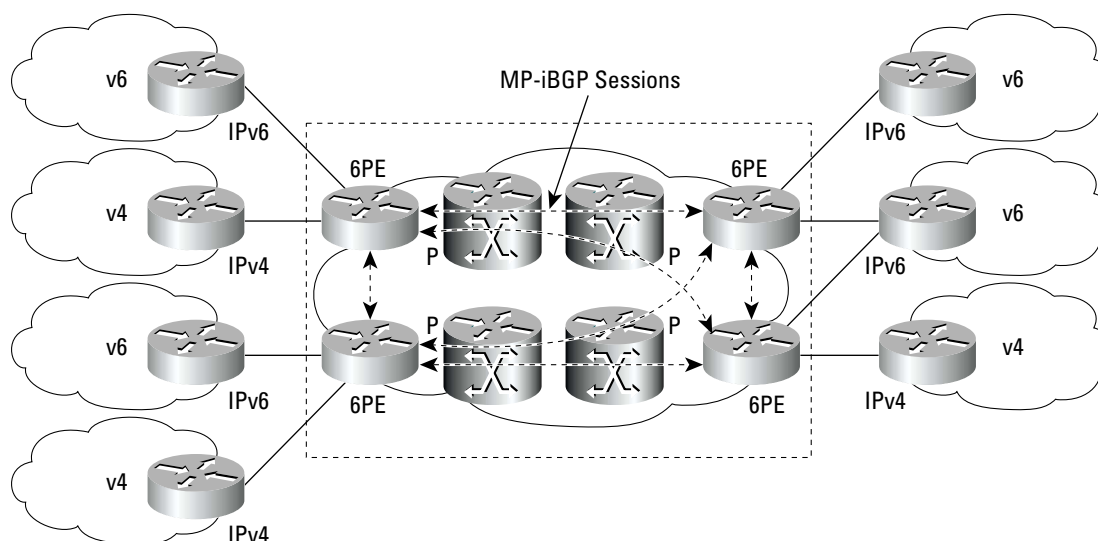
MPLS Mechanism	Primary Use	Benefits
IPv6 Using Tunnels on CE Routers	Enterprise customers wanting to use IPv6 over existing MPLS services.	No impact on MPLS infrastructure.
IPv6 over a Circuit Transport over MPLS	Service providers with ATM or Ethernet links to CE routers.	Fully transparent IPv6 communication.
IPv6 on PE Routers	Internet and mobile service providers wanting to offer an IPv6 service.	Low cost and low risk upgrade to the PE routers. No impact on MPLS core.

IPv6 on the Provider Edge Routers

A further deployment strategy is to configure IPv6 on the MPLS PE routers. This strategy has a major advantage for service providers in that there is no need to upgrade either the hardware or software of the core network, and it thus eliminates the impact on the operation of or the revenue generated from the existing IPv4 traffic. The strategy maintains the benefits of the current MPLS features (for example, MPLS or VPN services for IPv4) while appearing to provide a native IPv6 service for enterprise customers (using ISP-supplied IPv6 prefixes). Figure 3 shows the configuration for IPv6 on the PE routers.



Figure 3 IPv6 on the Provider Edge Routers



The IPv6 forwarding is done by label switching, eliminating the need for either IPv6 over IPv4 tunnels or for an additional Layer 2 encapsulation, allowing the appearance of a native IPv6 service to be offered across the network. The core network continues to run MPLS and any of the Cisco IOS software-supported IPv4 interior routing protocols, eliminating the requirement for upgrades to the hardware for native IPv6 forwarding and allowing the network to continue with current proven releases of Cisco IOS software.

Each PE router that must support IPv6 connectivity needs to be upgraded to be dual-stack (becoming a 6PE router) and configured to run MPLS on the interfaces connected to the core. Depending on the site requirements, each router can be configured to forward IPv6 or IPv6 and IPv4 traffic on the interfaces to the CE routers, thus providing the ability to offer only native IPv6 or both IPv6 and native IPv4 services. The 6PE router exchanges either IPv4 or IPv6 routing information through any of the supported routing protocols, depending on the connection, and switches IPv4 and IPv6 traffic using the respective fast switching path (either Cisco Express Forwarding [CEF] or distributed CEF [dCEF] for IPv4 or CEF or dCEF for IPv6) over the native IPv4 and IPv6 interfaces not running MPLS.

The 6PE router exchanges reachability information with the other 6PE routers in the MPLS domain using multiprotocol BGP, and shares a common IPv4 routing protocol (such as Open Shortest Path First [OSPF] or i/IS-IS) with the other P and PE devices in the domain.

The 6PE routers encapsulate IPv6 traffic using two levels of MPLS labels. The top label is distributed by the label distribution protocol (LDP) used by the devices in the core to carry the packet to the destination 6PE using IPv4 routing information. The second or bottom label is associated with the IPv6 prefix of the destination through multiprotocol BGP-4.

The 6PE architecture allows support for IPv6 VPNs; Cisco IOS software may add support for VPN or VRF as the market requires.

Cisco plans to support 6PE routers in Phase II of its IPv6 for Cisco IOS software release strategy. Refer to the Internet-Draft *draft-ietf-ngtrans-bgp-tunnel-02.txt* for further information on 6PE routers.

Deploying IPv6 Using Dual-Stack Backbones

Using dual-stack backbones is a basic strategy for routing both IPv4 and IPv6. All routers in the network need to be upgraded to be dual-stack. IPv4 communication uses the IPv4 protocol stack (with forwarding of IPv4 packets based on routes learned through running IPv4-specific routing protocols), and IPv6 communication uses the IPv6 stack with routes learned through the IPv6-specific routing protocols.

The key requirements are that each site has an IPv6 unicast global prefix and appropriate entries in a DNS that map between host names and IP addresses for both IPv4 and IPv6. Applications choose between using IPv4 or IPv6 based on the response from the DNS resolver library, with the application selecting the correct address based on the type of IP traffic and particular requirements of the communication.

Today, dual-stack routing is a valid deployment strategy for specific network infrastructures with a mixture of IPv4 and IPv6 applications (such as on a campus or an aggregation point of presence), requiring both protocols to be configured. However, apart from the obvious need to upgrade all routers in the network, limitations to this approach are that the routers require a dual addressing scheme to be defined, require dual management of the IPv4 and IPv6 routing protocols, and must be configured with enough memory for both the IPv4 and IPv6 routing tables.

For more information on the IPv6 Deployment Strategies, refer to

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6_sol/ipv6dswp.htm

IPv6 @ Cisco

Cisco has taken a leading role in the definition and implementation of the IPv6 architecture within the IETF and continues to lead the industry in standardization. Many of the IPv6 Standards are already published by the IETF; while at the same time enhancements are work-in-progress. Current status can be obtained from

<http://www.ietf.org/html.charters/ipngwg-charter.html>.

IPv6@Cisco Summary

- Cisco co-chairs the IETF IPng and NGtrans Working Group
- Cisco IOS IPv6 software has been extensively deployed in the prototype 6Bone network (www.6bone.net) for test purposes over several years
- Cisco 6Bone router is operational as a major 6Bone hub
- Cisco is a founding member of the IPv6 Forum (www.ipv6forum.com)
- Worldwide Cisco TAC support
- Information on Cisco IOS IPv6 may be found on www.cisco.com/ipv6



Cisco IOS Roadmap

Cisco IOS IPv6: 3 Phases Roadmap

Deploying a new set of protocols in production networks introduces a significant investment for customers and partners. To satisfy the production quality level Cisco customers have today with IPv4, the integration of the new IPv6 protocols requires a series of deployment steps. Therefore to successfully deliver comprehensive IPv6 integration, Cisco has defined a three-phase roadmap for IPv6.

Cisco IOS Release	Target Market
Phase I Release 12.2(2)T DONE	Early Adopter Deployment
Phase II Ongoing	Production Backbone Deployment
Phase III CY 2002 and Later	Enhanced IPv6 Services

Cisco IOS Roadmap Details

Below is a list of IPv6 Specifications as they will be introduced on Cisco IOS software.

Cisco IOS 12.2(2)T—Phase I, Early Adopters—IPv6 Specifications Support

Cisco IOS officially support IPv6 beginning with Technology release 12.2(2)T

Feature Name	RFC (if applicable)	Cisco IOS Release
IPv6 Services		
Internet Protocol version 6	RFC 2460	12.2(2)T
IPv6 Addressing Architecture	RFC 2373	12.2(2)T
ICMPv6	RFC 2463	12.2(2)T
Neighbour Discovery	RFC 2461	12.2(2)T
IPv6 Stateless Auto-configuration	RFC 2462	12.2(2)T
MTU Path Discovery for IPv6	RFC 1981	12.2(2)T
ICMPv6 Redirect	RFC 2463	12.2(4)T
IPv6 Duplicate Address Detection		12.2(4)T
IPv6 Standard Access Control List (ACL)		12.2(2)T
Manual Configured Tunnel	RFC 2893	12.2(2)T
Automatic IPv4 Compatible Tunnels	RFC 2893	12.2(2)T
6to4 Tunnels	RFC 3056	12.2(2)T
IPv6 over IPv4 GRE Tunnels		12.2(4)T
IPv6 Routing		
Static Routes	N/A	12.2(2)T
RIPng	RFC 2080	12.2(2)T
MP-BGP4	RFC 2545 and 2858	12.2(2)T
Link-local address to do MP-BGP4 peering		12.2(4)T
Encapsulation		

Feature Name	RFC (if applicable)	Cisco IOS Release
Loopback	N/A	12.2(2)T
Ethernet 10 Mb/s	RFC 2464	12.2(2)T
Ethernet 100 Mb/s	RFC 2464	12.2(2)T
Ethernet 1000 Mb/s	RFC 2464	12.2(2)T
IPv6 over ISL	N/A	12.2(2)T
IPv6 over IEEE 802.1Q	N/A	12.2(2)T
FDDI	RFC 2467	12.2(2)T
ATM PVC	RFC 2492	12.2(2)T
ATM Ethernet LAN-E	Using packet format RFC 2464	12.2(2)T
Cisco HDLC	N/A	12.2(2)T
PPP	RFC 2472	12.2(2)T
Frame Relay PVC	RFC 2590	12.2(2)T
Switching		
Process Switched		12.2(2)T
IPv6 Management & Applications		
Ping		12.2(2)T
Traceroute		12.2(2)T
Telnet		12.2(2)T
TFTP		12.2(2)T
DNS Client AAAA record over IPv4 transport	RFC 1886	12.2(2)T

Cisco Hardware Platform Details

In keeping with the Cisco philosophy of providing customers with the broadest choice of platforms and protecting their investment, IPv6 support was introduced across the majority of the strategic Cisco IOS-based products and associated releases. Platforms to support IPv6 are:

Cisco IOS 12.2T

- Cisco 800 Series Routers
- Cisco 1400 Series Routers
- Cisco 1600 Series Routers
- Cisco 1700 Series Routers
- Cisco 2500 Series Routers [12.2(4)T]
- Cisco 2600 Series Routers
- Cisco 3600 Series Routers
- Cisco 4500/4700 Series Routers [12.2(2)T only]
- Cisco 7100 Series Routers
- Cisco 7200 Series Routers
- Cisco 7500 Series Routers

Cisco IOS 12.0ST

- Cisco 12000 Internet Router Series



Cisco IOS 12.2S

- Cisco 7200
- Cisco 7500
- Cisco 7600
- Catalyst 6500 Series

Cisco IOS 12.2B

- Cisco 7400

Cisco IOS 12.2(4)XF1

- Cisco ubr7100, ubr 7200, and ubr10012 Router Series running IPv6 over IPv4 tunnels only

Any other Cisco platforms not able to run one of these releases (IP Plus package as minimum) will not offer IPv6 support.

- Any other Cisco platforms not able to run Cisco IOS 12.2(2)T technology release (IP Plus package as minimum) will not offer IPv6 support, e.g. Cisco 1000 series, Cisco 4000.

Layer 2 LAN Switches

IPv6 traffic forwarding does not impact Layer 2 LAN switches since these devices do not look the Layer 3 header before to forward an IPv6 frame. Thus IPv6 hosts can be transparently attached to the following Cisco products:

- Catalyst® 2900XL series
- Catalyst® 3500XL series
- Catalyst® 4000 series
- Catalyst® 5000 series
- Catalyst® 6000 series

Cisco IOS IPv6 Images and License

Cisco IOS IPv6 support requires the following licenses and images:

- IP Plus, –is image only
- Service Provider, –p image only
- Enterprise, –js image only

Memory Size

As IPv6 protocols are part of Cisco IOS releases, each router on which IPv6 is configured must conform to the minimum memory size as defined on CCO Software Center (www.cisco.com) for those particular Cisco IOS release and platform. Refer to <http://www.cisco.com/go/fn> to find the image and release supporting IPv6 on a specific platform.

Unsupported Data Link Layers for Cisco IOS IPv6

At this stage, Cisco does not plan to incorporate IPv6 support for the following data link layers:

- ATM LAN Emulation Token-Ring, ATM SVC: RFC2491 and RFC2492
- ATM MPOA: No definition of IPv6 in MPOA specification 1.1
- Frame Relay SVC
- SMDS
- Token-Ring: RFC2470
- X.25

Cisco IOS IPv6 Phase II Features—Production Backbone

Cisco IOS IPv6 Phase II deliverables are planned for second half of CY 2001 with the availability of the Cisco IOS 12.2T maintenance releases.

Feature Name	RFC (if applicable)
IPv6 Services	
IPv6 extended ACL	
NAT-PT	RFC 2766
IPv6 Routing	
IS-ISv6	
Encapsulation	
Dialer Pool + IPv6 AAA attributes	
Switching	
CEFv6	
dCEFv6	
IPv6 MPLS	
IPv6 Provider Edge Router (6PE) over MPLS	
IPv6 Management & Applications	
SSH over IPv6	
DNS Client AAAA record over IPv6 transport	RFC 1886
IPv6 MIBs	
CDP IPv6 address family support	

It is important to note that the information contained within this section previews Cisco's IPv6 plans and details, they could be modified to reflect customers' requirements or market and technology evolution.



Cisco IOS IPv6 Phase III Features Preview—Enhanced Services

As market requirements mature and adoption continue to grow, Cisco plans to deliver additional standards-compliant IPv6 features. The following section is a preview of enhanced IPv6 services under evaluation for Cisco IOS IPv6 Phase III, scheduled for CY 2002.

Feature Name	RFC (if applicable)
IPv6 Services	
Anycast address support	RFC 2373
IPv4 over IPv6 GRE Tunnels	RFC 2473
IPv6 over IPv6 GRE Tunnels	RFC 2473
ISATAP	
NAT-PT additional ALGs	
IPv6 Routing	
OSPFv3	RFC 2740
Cisco EIGRP for IPv6	N/A
Encapsulation	
Ethernet 10 Gb/s	RFC 2464
DPT	N/A
xDSL PPPoA	
xDSL PPPoE	
xDSL RBE	
Native IPv6 over Cable	
Mobile IPv6	
Mobile IPv6 Home Agent	draft-ietf-mobileip-ipv6-13
IPv6 Netflow	
Quality of Services (QoS)	
Classification	
Policing	
DSCP Marking/Remarking	
Queuing	
Security	
IPsec Transport Mode	RFC 2401, RFC 2402, RFC 2406
Multicast	
MLDv2	RFC 2710 + draft v2
PIMv2-SM	
PIM-SSM	
IPv6 Management & Applications	
FTP	
SNMP over IPv6 Transport	

It is important to note that the information contained within this section previews Cisco's IPv6 plans and details, they could be modified to reflect customers' requirements or market and technology evolution.

Conclusion: Cisco IOS Software, the Confluence of IPv4/IPv6

Cisco is taking a leadership role in delivering comprehensive IPv6 services as part of Cisco IOS software. This IPv6 Statement-of-Direction targets customers considering IPv6 deployment, driven by their specific requirements and is intended to provide sufficient information to enable IPv6 adoption with Cisco IOS platforms.

Customers interested in testing or deploying Cisco's IPv6 solution should contact their local sales office.

Appendixes

Appendix A—IPv6 Interoperability

For several years, Cisco IOS IPv6 prototype software has been deployed across the 6Bone. Interoperability testing is one of the most important considerations before deploying new technologies. Cisco participates in various IPv6 interoperability tests and multiple pilot networks are running Cisco IOS IPv6 Software. Cisco IOS IPv6 is known to inter-operate with:

- *BSD
- Compaq (formerly Digital) Tru64 Unix and OpenVMS
- HP-Unix
- IBM AIX
- Linux
- Microsoft Windows NT
- SUN Solaris

Appendix B—IPv6 Documentation

IPv6 documentation are available with software release associated with IPv6 on specific product; i.e. Cisco IOS release 12.2(2)T manuals and release notes.

Appendix C—References

- Cisco IPv6 Web page
<http://www.cisco.com/ipv6>
- IPv6 Specifications
<http://www.ietf.org/html.charters/ipngwg-charter.html>
- IPv6 Forum
<http://www.ipv6forum.com>
- 6REN
<http://www.6ren.net/>
- 6Bone
<http://www.6bone.net/>
- 6TAP
<http://www.6tap.net/>
- IPv6 information
<http://www.ipv6.org/>

Appendix D—How to Register for an IPv6 Address Block

- 6Bone ‘How to Join the 6Bone’ section
<http://www.6bone.net>
- IPv6 ARIN Registration Services
<http://www.arin.net/regserv/ipv6/ipv6-regserv.html>
- IPv6 RIPE Registration Services
<http://www.ripe.net/ripencec/mem-services/registration/ipv6/ipv6.html>
- IPv6 APNIC Registration FAQ
<http://www.apnic.net/drafts/ipv6/IPv6-FAQ.html>



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 Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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 © 2001, Cisco Systems, Inc. All rights reserved. AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARtner, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn and Discover All That's Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0110R)