

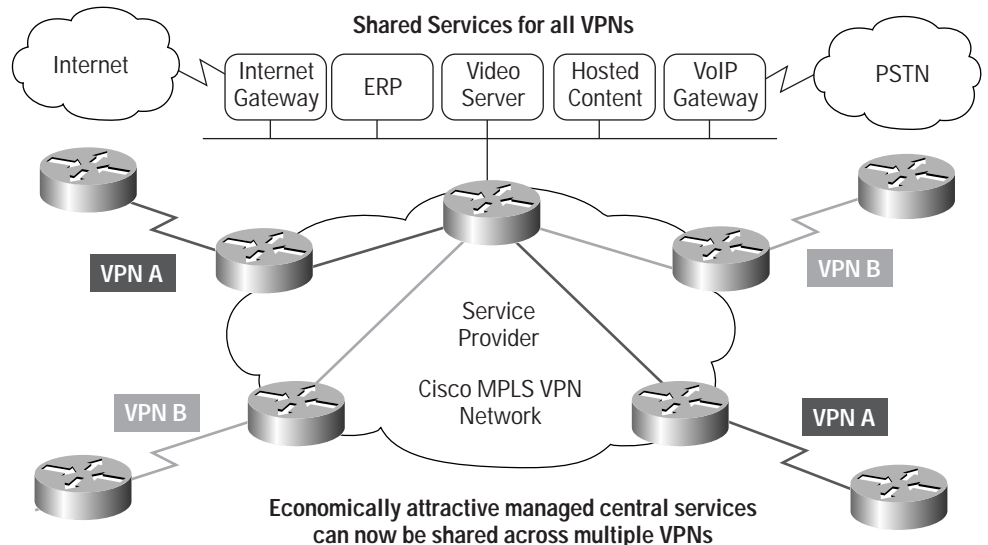
# Cisco MPLS For Managed Shared Services Frequently Asked Questions

## Cisco MPLS For Managed Shared Services

Q. What is Cisco MPLS For Managed Shared Services?

A. Cisco MPLS for Managed Shared Services is a set of features delivered in Cisco IOS<sup>®</sup> Software for enabling managed shared services for Multiprotocol Label Switching Virtual Private Networks (MPLS VPNs). Building on our leading MPLS capabilities, service providers now can provide their enterprise clients all the connectivity benefits associated with Cisco MPLS VPNs while creating additional revenue streams by providing economically attractive, IP services. Cisco has expanded its widely deployed MPLS VPN solution to include the following four technologies in Cisco IOS Software: Network Address Translation (NAT) for MPLS VPNs, On Demand Address Pools (ODAP) for MPLS VPNs, Multicast VPNs, and VPN Select. With these key new technologies, enterprise IP services can now be moved from the enterprise network into the service provider's MPLS VPN network, and shared across multiple VPNs for greater operational leverage and economies of scale.

Figure 1  
 Shared Services for all VPNs





Q. What customer problem does Cisco MPLS for Managed Shared Services solve?

A. Cisco MPLS for Managed Shared Services eliminates many of the problems that are commonly associated with delivering advanced services to MPLS VPN customers, including poor efficiency in resource utilization, high traffic loads, and management complexity. Cisco MPLS technology incorporates functionality that enables effective management of central IP services, enhanced delivery of multicast-based services, and added flexibility to client service selection.

Q. Who are the target customers?

A. Service providers that have deployed MPLS VPNs can benefit from the features in Cisco MPLS for Managed Shared Services to enhance their current offerings and to create additional revenue streams. They can use Multicast features to leverage existing infrastructure resources, and offer competitive services in video conferencing and other Internet-based streaming applications.

Q. What are the key benefits of Cisco MPLS For Managed Shared Services technology?

A. Cisco MPLS For Managed Shared Services features give service providers powerful new MPLS VPN functionality and versatility, without deployment or management complexity:

- Service providers can now monetize IP services inside MPLS VPNs with Managed IP Services
- Multicast-based services lead to a dramatic reduction in complexity, thus yielding OPEX savings for enterprises and creating new revenue stream for service providers
- VPN Selection opens new broadband market
- Support for expanded service offerings such as Multicast VPNs, and broadband services utilizing VPN Select
- Simpler implementation and scaling of full-mesh topologies
- Increased capability to attract and retain enterprise customers that require robust functionality and broad protocol support

### Cisco MPLS For Managed Shared Services Technologies

Q. What features are available in this release?

A. The table below lists new Cisco MPLS features, and the following questions provide additional details.

Table 1 Key Features of Cisco MPLS For Managed Shared Services

Categories and Features	Function	Benefits
<b>NAT</b>	NAT for MPLS VPNs creates unique translations per VPN, allowing access to shared services even though addresses overlap	Increased SP revenues with outsourcing of NAT services; efficient shared services delivery; simpler central management of resources; reduced network complexity and costs for the enterprise
<b>DHCP Relay</b>	Enables a DHCP relay agent to forward VPN association to a DHCP server so that addresses can be allocated per VPN	Availability of enterprise-essential protocols/ services; maintenance of existing DHCP/ addressing plans; conservation of address space



Table 1 Key Features of Cisco MPLS For Managed Shared Services

Categories and Features	Function	Benefits
<b>ODAP</b>	On-demand creation and assignment of addresses from pool; addresses are assigned per subnet, per VPN	Automates IP address assignment from shared DHCP server or RADIUS server; necessary for efficiently implementing and managing VPNs
<b>HSRP</b>	Provides first hop redundancy to VPN sites	High network availability and transparent topology changes
<b>VRRP</b>	Enables a group of routers to function as a single router, sharing one virtual IP address and one virtual MAC address	High network availability; protocol selection to match environmental requirements
<b>Multicast VPN</b>	Native, integrated support for multicast with MPLS VPNs	Better utilization of infrastructure resources for enterprises; broader application services (videoconferencing, e-learning) availability from service providers
<b>Ping and Traceroute</b>	Enables monitoring of packet transmissions and device status on a per VPN basis	Rapid fault detection
<b>VPN Select</b>	Switches packets to the appropriate VRF Selection table based on source IP address of the packets	Support for client preferences in ISPs; remote connection to VPNs, irrespective of access provider; support for multiple VPNs per interface; greater scalability and redundancy

Q. What is Network Address Translation (NAT) for MPLS VPNs?

A. In today's MPLS networks, enterprises have to pay for leased links and router ports for internet connectivity in addition to VPN connectivity, as well as the operational expenses associated with internally managing NAT. While service providers can currently provide NAT services to their enterprise clients with additional router/NAT devices, it is a highly complex design. NAT for MPLS VPNs is a simpler and more flexible way to integrate NAT services within MPLS VPNs with a single network connection that provides both MPLS VPN connectivity and access to shared services.

Q. What are the benefits of NAT for MPLS VPNs?

A. Because NAT for MPLS VPNs offers more economical NAT services, these services can be made more appealing to enterprise clients with a resulting revenue opportunity for service providers.

Cisco NAT for MPLS VPNs:

- Provides a simple and more flexible way of integrating NAT with MPLS VPNs
- Automatically manages the overlapping of VPN address spaces (allowable in MPLS VPNs) to ensure addresses are mapped correctly in shared-services applications
- Provides centralized delivery of full-VPN NAT services
- Enables NAT redundancy (NAT can be configured on one or more provider edge routers)
- Eliminates the requirement for physical connectivity between a shared service and the provider network that is performing network address translations



Q. What is Dynamic Host Configuration Protocol (DHCP) Relay?

A. Service providers can take advantage of another centralized service to support Dynamic Host Configuration Protocol (DHCP) clients. DHCP Relay for MPLS VPNs enables a DHCP relay agent to forward information about the DHCP request and the VPN association when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can then use that information to interpret IP addresses or other parameter-assignment policies. The DHCP relay agent information option is organized as a single DHCP option that contains one or more suboptions (VPN identifier, subnet selection, and server identifier override) to convey information known by the relay agent.

In some environments, a relay agent resides in a network element that also has access to one or more MPLS VPNs. A DHCP server that must offer service to DHCP clients on those different VPNs must know about the VPN association of the DHCP and therefore includes this information in the relay agent.

Q. What are the benefits of DHCP Relay?

A.

- Enables network administrators to conserve address space by allowing overlapping addresses (clients on multiple VPNs can share IP addresses)
- Enables host identification in multiple VPNs or global spaces
- Maintains integrity of existing enterprise customer DHCP/addressing schemes

Q. What is On-Demand Address Pools (ODAP)?

A. Today, service providers face challenges when it comes to efficient management of IP address space for customers. With MPLS VPNs SPs will have to allocate their IP address pools to independent RADIUS or DHCP servers for each VPN. Once the site threshold has been reached, new addresses have to be provided manually. With ODAP for MPLS VPNs, this process can now be fully automated and offered as a shared service on one or more servers. Once the site threshold is exceeded, ODAP for MPLS VPNs automates the process of expanding the overall address pool, reducing network loading and manual configuration effort.

Q. What are the benefits of ODAP?

A.

- Capabilities for automated control
- Support for MPLS VPNs, with addresses assigned per subnet, per interface
- Easy monitoring capabilities (pool manager can assess address utilization and expand the pool as needed)
- Simplified VPN setup (upon configuration, pool manager can request an initial subnet from the address pool server)

Q. What is Hot Standby Router Protocol (HSRP)?

A. Cisco MPLS For Managed Shared Services also provides Hot Standby Router Protocol (HSRP) support on MPLS VPN interfaces. This feature provides transparent “first-hop IP routing” redundancy for workstations or routers connected to interfaces within the MPLS VPN. HSRP creates a hot standby router group with a lead router that services all packets sent to the hot standby address. Other routers within the group monitor the lead router. If the lead fails, a standby router inherits the lead position as well as the hot standby address. The HSRP protocol allows specification of active routers, preemption delays, hold times, and interface status tracking.



Q. What are the benefits of HSRP?

A.

- Improved network availability
- Transparent network topology modifications
- Simple, centralized control of hot standby parameters

Q. What is Virtual Router Redundancy Protocol (VRRP)?

A. Similar to HSRP, Virtual Router Redundancy Protocol (VRRP) allows a group of routers to function as one virtual router. Cisco MPLS For Managed Shared Services includes VRRP for MPLS VPNs by enabling the group of routers to share one virtual IP address and one virtual MAC address. One master router performs packet forwarding for the local hosts, and the rest of the routers within the group can act as backup routers to protect from failures of the master. With VRRP, the backup routers stay idle as far as packet forwarding is concerned.

Q. What are the benefits of VRRP?

A.

- Improved network availability
- Standards based protocol
- The flexibility to choose the protocol that best suits each environment

Q. What are Multicast VPNs?

A. Without integration of multicast support with MPLS VPNs, wide-scale distribution of large data, voice, and video streams is extremely inefficient. For example, full mesh GRE tunnels are currently required to send multicast traffic between sites within a VPN. This results in an unscalable and inefficient network design. By implementing native multicast functionality inside their MPLS VPN networks, service providers can now monetize multicast services. SPs can utilize current resources to support bandwidth-hungry streaming services such as telecommuting, video conferencing, e-learning, and a host of other business applications. Cisco Multicast VPN technology helps improve efficiency of bandwidth-hungry applications of enterprise networks by eliminating the packet replication and performance issues associated with distribution of multicast traffic.

Q. What are the benefits of Multicast VPNs?

A. Multicast VPN benefits service providers by:

- Enabling service provider's with MPLS VPN networks to offer multicast services to their enterprise clients
- Minimizing configuration time and complexity—configuration is required only at edge routers
- Ensuring transparency of the service provider network
- Providing the ability to easily build advanced enterprise-friendly services such as Virtual Multicast Networks
- Increasing network scalability

Q. What are Ping and Traceroute?

A. These enhancements provide simple-to-use mechanisms for testing network connections. By sending out short messages to designated servers (Ping) or along specified routes (Traceroute), the utilities allow network managers to quickly assess that a server or connection is up and running. These features are now VPN aware and can detect VPN specific faults.



Q. What are the benefits of Ping and Traceroute?

A.

- Rapid fault detection for MPLS VPNs
- Ease of use with a variety of servers and network equipment

Q. What is VPN Select?

A. VPN Select allows access providers to offer VPN connectivity to broadband customers by extending the VPNs offered by SPs into access network. Broadband customer can now connect to any ISP that provides VPN capabilities. This opens a new market for service providers, who can now offer corporate VPN connectivity to broadband users. VPN Select removes the restrictive association of a VPN to a single interface. A specified interface can route packets to any number of different VPNs, based on the source Internet Protocol (IP) address of the packet. This capability adds versatility to the service offering, and of particular importance for the global enterprise, allows remote users to connect to the corporate VPN irrespective of their access providers.

Q. What are the benefits of VPN Select?

A.

- Decoupling of the association between a VPN and a single interface
- Cable and DSL environment support of multiple customers on a single interface (customers are placed within a VPN context based on their source IP address)
- Mapping of DSL and cable customers to any ISP that provides VPN capabilities
- Remote user connection to VPNs, regardless of the access provider

Q. What is VPN Routing and Forwarding (VRF)?

A. VPN Routing and Forwarding (VRF) is a VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that uses the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) router.

Cisco MPLS includes several VRF features that present opportunities for new IP services revenue streams, as well as for cost savings.

- NAT for MPLS VPNs: allows service providers to more cost-effectively support services such as content hosting, ERP application hosting, and Managed Internet access.
- Other features add support in the MPLS network for industry-standard protocols, as well as improve or automate routing control.

## Resources

Q. Where can I more information?

A. For more information, please visit <http://www.cisco.com/go/mpls/>, or contact [mpls-shared@cisco.com](mailto:mpls-shared@cisco.com).



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](http://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