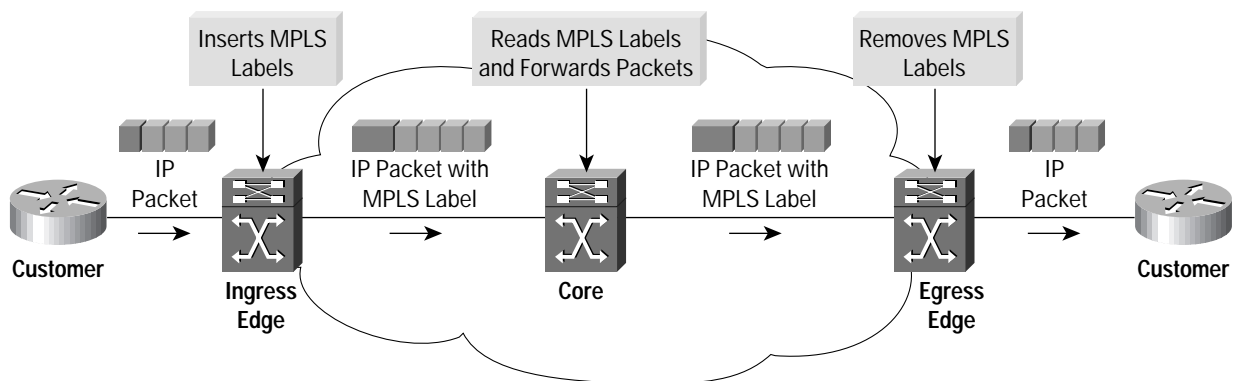


Implementing MPLS with the Cisco Catalyst 8540

Introduction

Multiprotocol Label Switching (MPLS) is a high-performance method for forwarding packets (frames) through a network. It enables devices at the edge of a network to apply labels to packets and devices at the core of a network to switch packets according to the labels with minimum lookup overhead. Labels indicate both routes and service attributes. As shown in Figure 1, incoming packets are processed and labels are selected and applied on the ingress edge. The core reads labels, applies appropriate services, and forwards packets based on the label. Processor-intensive analysis, classification, and filtering happen only once, at the ingress edge. At the egress edge, labels are stripped, and packets are forwarded to their final destination using normal routing mechanisms. Hence MPLS combines the benefits of connectionless Layer 3 routing and forwarding with connection-oriented Layer 2 forwarding.

Figure 1 MPLS Network



The MPLS architecture can be successfully deployed in a traditional service provider backbone environment. In addition, MPLS, in combination with the Border Gateway Protocol (BGP) or other routing protocols, provides support for highly scalable IP Virtual Private Network (VPN) services. IP VPN services are an invaluable development in provider networks, giving enterprise customers a service that meets their needs for private, connectionless delivery of IP services. Service providers experience immediate benefits when they add MPLS to their networks, such as:

- Scalable any-to-any connectivity for extended intranets and extranets that encompass multiple customers
- Simplified managed networks for intranet and extranet services
- Strong foundation for IP value-added services such as IP VPNs
- Standards based technology
- Integration with Cisco IOS® Software

Since MPLS offers a scalable way to deliver IP VPNs, enterprise and local governments can also use MPLS to offer VPNs to different departments or different municipalities. In this model, the large enterprise or local government acts as the service provider for all the enterprise sites or government entities. MPLS VPNs deployed in a large enterprise or local government network provide benefits, such as:

- Simplified deployment of IP VPNs to departments/municipalities by eliminating the cost of provisioning virtual circuits (VCs)
- A platform for rapid deployment of additional value-added IP services, including intranets, extranets, voice, multimedia, and network commerce
- Privacy and security equal to Layer 2 VPNs by limiting the distribution of the routes of a VPN to only those routers that are members of the VPN
- Seamless integration with customer intranets

The Cisco Catalyst® 8540 Multiservice Switch Router (MSR), Catalyst 8510 MSR, and LightStream® 1010 Switches support the MPLS implementation.

Applications for MPLS

MPLS in a Service Provider's Core Network

Application

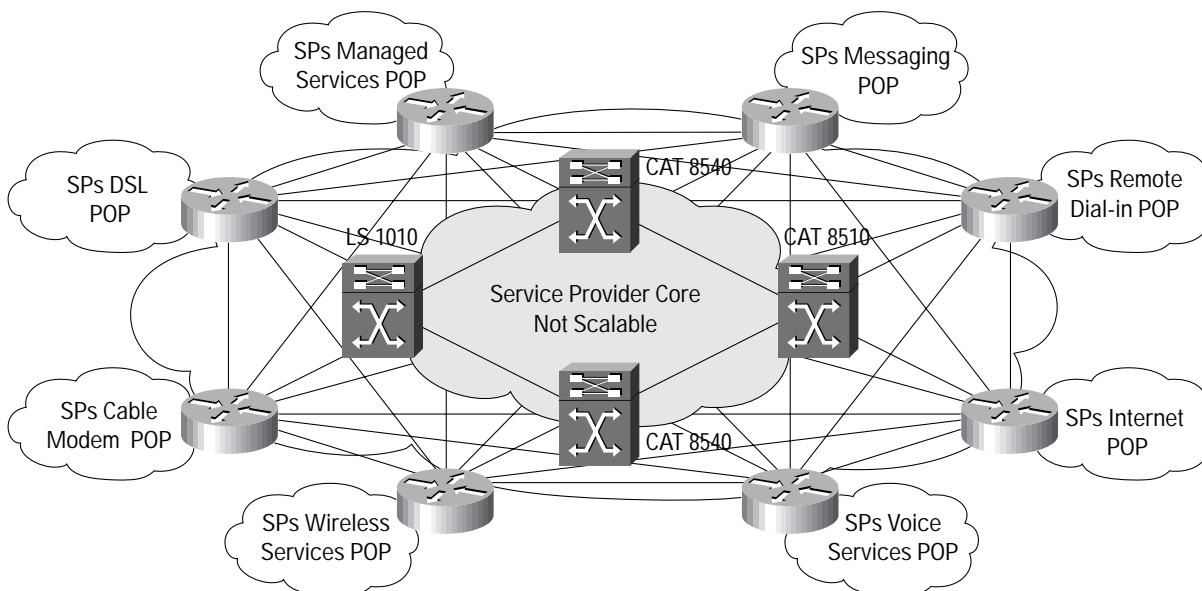
Service providers today are experiencing unprecedented demand for IP services. Factors contributing to the demand for bandwidth include broadband access to the Internet, an increase in the number of Internet users, and service-level agreements (SLAs) requested by customers to support new and emerging bandwidth-hungry applications. Service providers must find a way to accommodate the dramatic growth in network traffic and the number of users. To do so, service providers have deployed connection-oriented ATM network cores. Though this has worked well, there is a desire to simplify network operations by reducing the number of control planes operating in the network, currently ATM and IP. MPLS, as an emerging technology, has been widely identified as a new tool to help service providers create differentiated services and potentially reduce operation costs in multiservice networks.

Solution

Figure 2 depicts a core service provider network as an overlay model for providing IP services across an ATM backbone consisting of Cisco Catalyst 8500 and LightStream 1010 Switches. In this representation, we see that adding a new service involves the configuration of an increasingly complex VC mesh required by the new service.



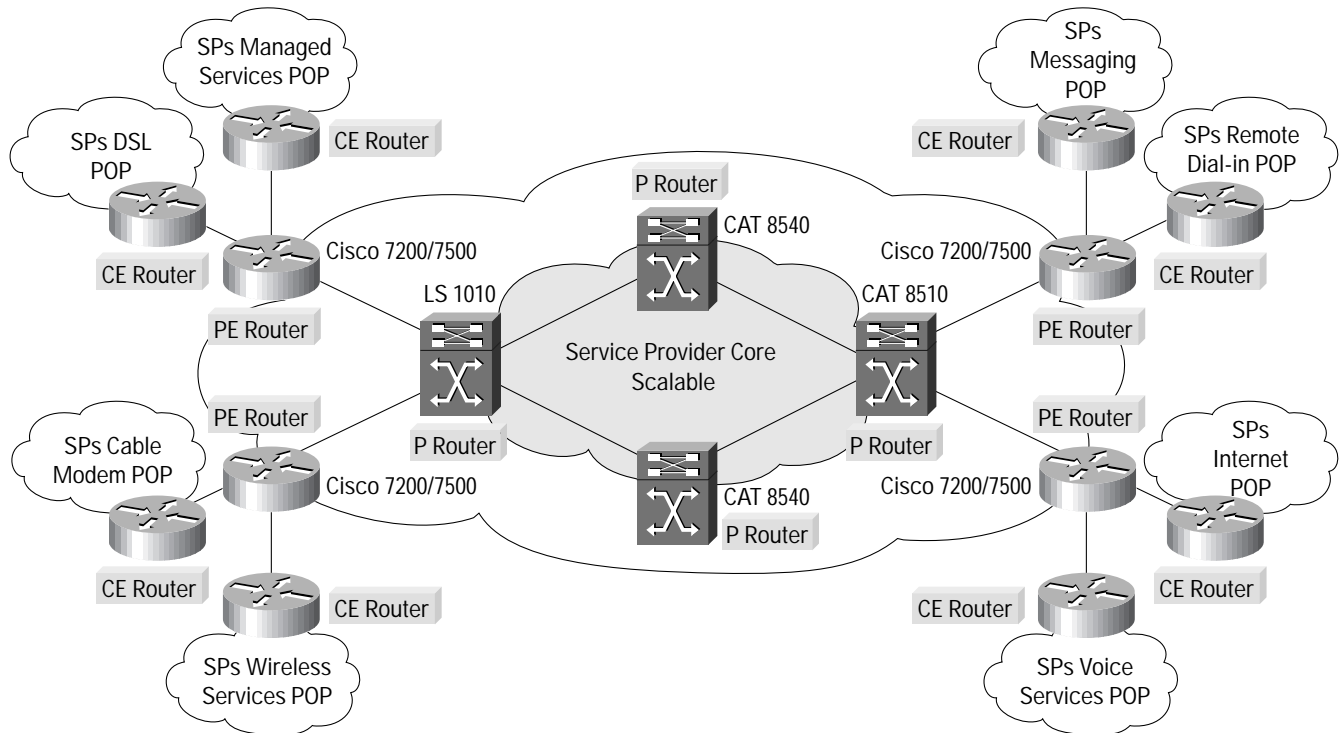
Figure 2 Service Provider Core Network without MPLS



In Figure 3, we see how MPLS has a significant advantage over the overlay model for providing IP services across an ATM backbone. With MPLS, we need to configure only the edge of the network for a new service. The routing protocol, such as BGP, interacts with MPLS and installs routes between router peers so that only these peers need to know each other. Thus we simplify routing and are able to overcome the scalable problem with the overlay model.

In this network structure, the service provider points of presence (POPs), consisting of Customer Edge (CE) devices, are connected directly to the Edge Label Switch Routers (LSRs) that comprise the Cisco 7xxx Routers. These edge LSRs are grouped together to form the Provider Edge (PE) network. The edge LSRs are connected by ATM links to the core devices that are the ATM LSRs. The core LSRs comprise the Cisco Catalyst 8500 or LightStream 1010 Switches and are referred to as the Provider (P) network.

Figure 3 Service Provider Core Network with MPLS



Benefits

- **Scalability**—MPLS scales to large IP-based ATM networks by providing any-to-any connectivity for extended intranets and extranets that encompass multiple customers.
- **Simplified managed networks**—MPLS greatly simplifies and speeds service creation, provisioning, and operation of intranet and extranet services without complex per-VC configurations; in addition, there is no traffic matrix to update, no permanent virtual circuit (PVC) mesh to resize, and no routing topology to update.
- **Foundation of IP value-added services**—MPLS brings VPN awareness to the network and allows flexible grouping of users and services.
- **Standards based**—MPLS is an Internet Engineering Task Force (IETF) standard available to all industry vendors to ensure interoperability in multivendor networks.
- **Integration with Cisco IOS Software**—MPLS teams with the robust features of Cisco IOS Software to deliver the industry’s broadest set of technologies, giving providers optimum flexibility for network design and services provisioning, and enabling seamless interoperation.

MPLS VPN in a Large Enterprise or Local Government

Application

VPNs form the infrastructure for intranets and extranets, which are IP networks on which corporations will base their whole business structures. A VPN service is a managed intranet or extranet service offered by a provider to many corporate customers. MPLS, in combination with a routing protocol such as the BGP or Open Shortest Path First (OSPF), allows one provider network to support thousands of customers’ VPNs.

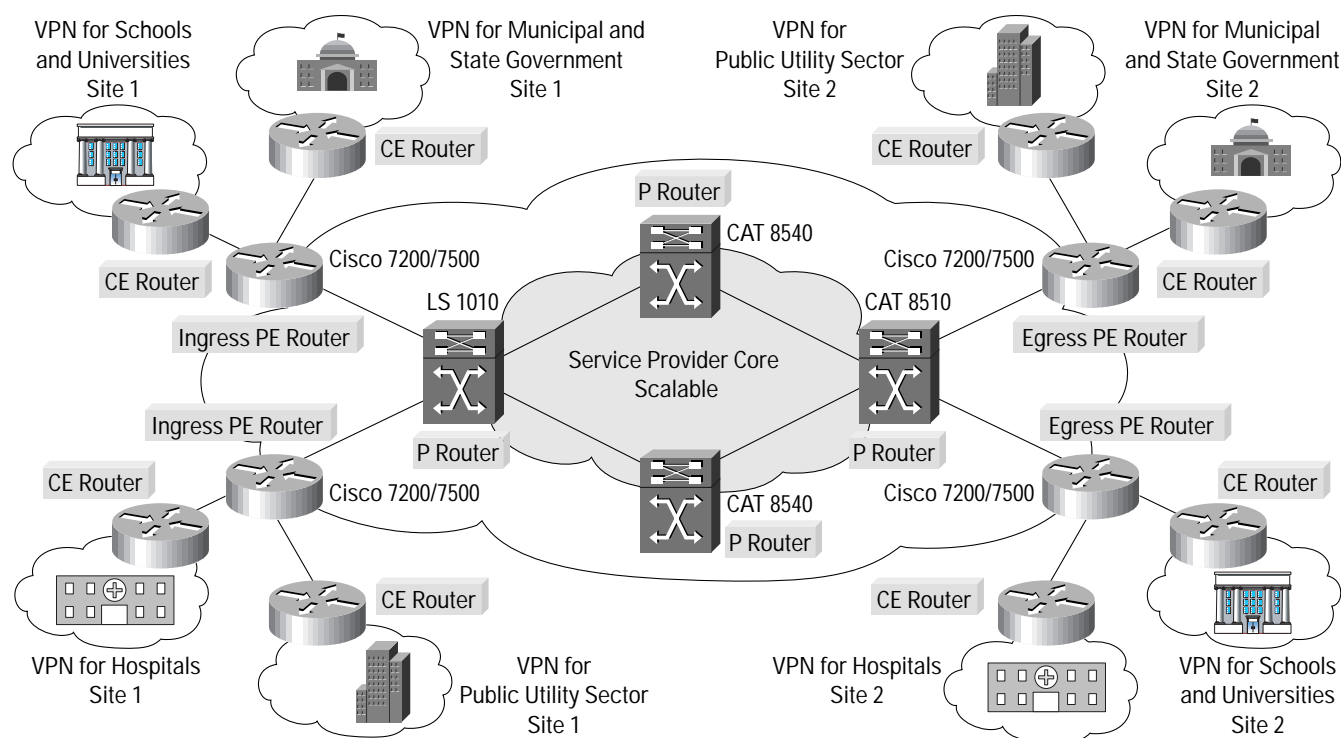


A large enterprise such as a local government can offer MPLS VPN services to the local police, schools, hospitals, utility companies, and so on. In this case, the local government acts as a small service provider and its MPLS VPN service solution benefits its customers, the end users, too. For example, it enables the municipal, state, and federal government groups to easily migrate legacy systems to packet networks. The school districts and universities can take advantage of the MPLS VPN functionality for cost-effective and easy-to-manage distance-learning solutions or interactive learning. MPLS VPN solutions can also be installed at the core of the medical networks to deliver capabilities for advanced health care applications such as telemedicine, training, and videoconferencing. In addition, the utility sector (gas, electric, water, and waste groups) can be provided with reliable MPLS VPN solutions to migrate billions of dollars of installed legacy equipment to packet networks and deliver cost-effective state-of-the-art solutions to their customers.

Solution

In Figure 4, the Catalyst 8500 and LightStream 1010 Switches, along with the Cisco 7xxx Routers, are used to provide MPLS VPN functionality to the network of a local government. In this network structure, end-user sites at each municipality (for example, hospitals, schools and universities, utilities, and police) connect into the network via a CE router, and connect into the government-owned MPLS-based network via an edge LSR. The CE devices could be Cisco 7xxx or 3600 Routers, with the Cisco 7xxx Routers providing the edge LSR or PE functionality. These edge LSRs are connected by ATM links to the core devices that are the ATM LSRs. The LSRs are the Catalyst 8500 and LightStream 1010 Switches and are referred to together as the provider (P) network.

Figure 4 MPLS VPN in a Local Government Network



A significant strength of the MPLS VPN solution is that large enterprise or local governments can use the same infrastructure to support many VPNs and do not need to build separate networks for each department, municipality, or government branch. Further, this solution has IP VPN capabilities built into the network itself, so large enterprises or governments can configure one network for all subscribers that delivers private IP network services such as intranets and extranets without complex management, tunnels, or VC meshes. Application-aware quality of service (QoS) can be added to make it possible to apply customer-specific business policies within each VPN. Adding QoS services to MPLS-based VPNs works seamlessly, since both are based on labels.

The same infrastructure now supports many VPNs for many customers, removing the burden of separately engineering a new network for each customer, as with overlay VPNs. It is also much easier to perform VPN adds, moves, and changes. If a company wants to add a new site to a VPN, the large enterprise or government only has to tell the CE router how to reach the network and configure the LSR to recognize VPN membership of the CE. The routing protocol would update all VPN members automatically. This is far easier, faster, and cheaper than the numerous operations required for adding a device to an overlay VPN.

Benefits

- *Scalability*—MPLS with a routing protocol (for example, OSPF or BGP) offers a very simplified, flexible, scalable, and manageable way of providing VPN services on both ATM and IP packet-based equipment. MPLS-enabled IP VPNs are secure, and the connectionless nature of MPLS networks removes the costs of provisioning PVCs and configuring customer equipment.
- *Stability*—Packet forwarding is highly stable. The core LSRs have no knowledge of VPNs in the network, nor do they respond to any changes in VPNs, making packet forwarding highly stable.
- *Customer independence*—CE equipment does not run MPLS or any special features. Any IP-capable equipment can be used at customer sites. Also, customers can use any type of IP addresses (that is, registered, private, or unregistered). Because the provider (P) network keeps customers' IP address ranges separate with an identifier called route distinguisher (RD), customers may use any IP addresses in their network without requiring Network Address Translation (NAT).
- *Standards based*—MPLS is an IETF standard available to all industry vendors to ensure interoperability in multivendor networks.
- *Integration with Cisco IOS Software*—MPLS teams with the robust features of Cisco IOS Software to deliver the industry's broadest set of technologies, giving providers optimum flexibility for network design and services provisioning, and enabling seamless interoperation.
- *Flexible architecture*—Cisco IOS Software and the Cisco Catalyst 8540 Switch makes it easy for providers to negotiate interconnections with other Cisco routers and switches as well as other provider networks for global IP coverage.
- *Centralized management and provisioning*—This feature greatly simplifies and speeds service creation, provisioning, and operation of intranet and extranet VPN services without complex, per-VC configurations.

Summary

The Cisco Catalyst 8500 and LightStream 1010 implementations can be used to build an entirely new class of MPLS IP VPNs. MPLS is compatible with several architectures, allowing maximum flexibility and interoperability with existing backbones.

Service providers can offer low-cost, differentiated managed IP-based VPN services because they can consolidate services over a common infrastructure and make provisioning and network operations much simpler. Similarly, large enterprises or governments can use one network infrastructure to support many VPNs, and they do not need to build a separate network for each of their departments, municipalities, or government branches.

MPLS-enabled IP VPNs are secure, and the connectionless nature of MPLS networks removes the costs of provisioning VCs and configuring customer equipment. Using MPLS, service providers and large enterprises or local governments can deliver IP VPN services across either switched or routed networks to protect today's rapidly growing revenue sources (such as Frame Relay and ATM WAN services), while paving the way for tomorrow's value-added services portfolio.

Orderability Information

The Catalyst 8500 and LightStream 1010 product family supports Cisco's feature rich Tag Switching implementation of MPLS. One of the following feature licenses are required for use of this feature.

Table 1 Catalyst 8500 MSR and LightStream 1010 MPLS Feature Licenses

Part Number	Description	Recommended Cisco IOS Release	Availability
Catalyst 8540 MSR			
FR-8540MSR-TAGSW	Catalyst 8540 MSR Tag Switching License	12.0(13)W5(19) or higher	Now
FR-8540MSR-THPNNI	Catalyst 8540 MSR Hierarchical PNNI + Tag Switching License	12.0(13)W5(19) or higher	Now
Catalyst 8510 MSR			
FR-8510-TAGSW	Catalyst 8510 Tag Switching License	12.0(13)W5(19) or higher	Now
FR-8510-THPNNI	Catalyst 8510 Hierarchical PNNI + Tag Switching License	12.0(13)W5(19) or higher	Now
LightStream 1010			
FR-WA-SX-TAGSW	LightStream 1010 Tag Switching Upgrade	12.0(13)W5(19) or higher	Now
FR-WA-SX-THPNNI	LightStream 1010 Tag Switching + Hierarchical PNNI Upgrade	12.0(13)W5(19) or higher	Now

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.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 Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • 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. Printed in the USA. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and LightStream are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other brands, names, or 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. (0010R)