

IP Solution Center—MPLS VPN

Deploying MPLS VPN Services

Today's service providers are facing significant market-, operations-, and service-related challenges that are impacting every aspect of how they invest in, deploy, and manage their networks. To be successful, service providers require a solution that addresses each of these challenges.

Market-Related Challenges

Conservative capex budgets are pushing service providers to invest only in those areas of their infrastructure directly impacting the bottom line. Moreover, several service providers are investing in network management systems/operations support systems/business support systems (NMS/OSS/BSS) to squeeze more value out of their existing networking infrastructures built during the capex race of the mid-to-late 90s. To sustain high-margin revenues, however, service providers are eager to be the first to market with new services, particularly to their business customers. Some of these services include IPsec and MPLS VPNs, managed security services, and VoIP and Video On Demand for Cable MSOs.

The Cisco® IP Solution Center (ISC) MPLS VPN technology solution provides enterprises and service providers with a robust and centralized management platform that minimizes the deployment cost of MPLS VPN services, guarantees accuracy of service deployment, and effectively deploys and manages the entire lifecycle of MPLS VPN technologies including policy-based VPN, management VPN, SLA, QoS provisioning, and MPLS VPN routing audit. Cisco ISC has also been

tightly integrated with Cisco CNS technology for zero-touch, plug-and-play MPLS VPN CPE deployment.

Service-Related Challenges

When planning the introduction of new services, service providers must ensure there is an alignment with their business objectives and processes. A Services Creation Environment must be in place where the following elements are elaborated:

- New service definition, creation, and testing
- Marketing plan
- Support structure and how this integrates with the overall Service-Order to Service Activation workflow process
- Skill and training to deploy, sell, and support the new service
- Required investment in the network infrastructure for service deployment and provisioning

Business metrics or performance targets for the service are important because they are tightly related to revenue objectives. These include the number of transactions to break even, time-to-provision goals, billing accuracy, and so on. The OSS application for enabling the new service(s) will be



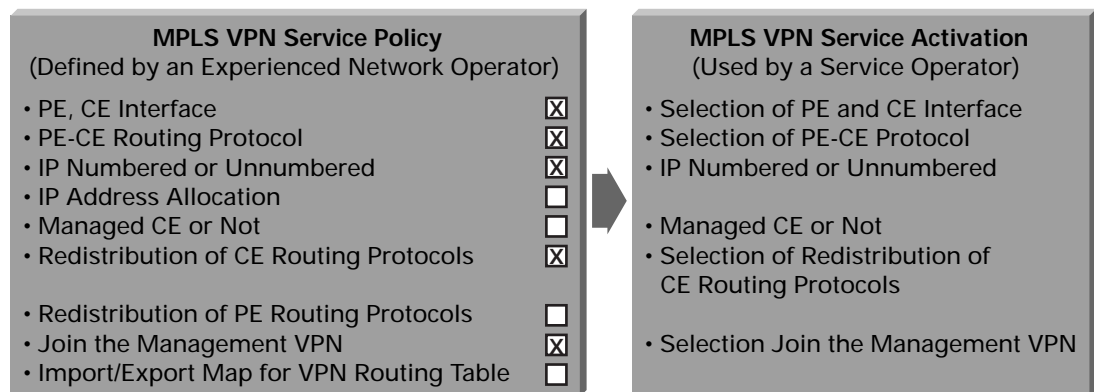
paramount in accelerating the time to revenue. The complexity and troubleshooting of extensive networks with large customers can become an inextricable problem. For each customer or each site, the service operator needs to keep track of network element configurations. The amount of information that must be tracked is enormous. There is a clear need to automate these processes from Service-Order to Service Activation.

New Service Definition, Creation, and Testing

Service providers have to define, create, test, and deploy every new technology that they think will make them competitive in the marketplace. This requires training the network operator and developing the skill set needed to effectively operate the network and activate services. The key aspects are rapid deployment of services, accuracy of deployed configurations, and traceability of what happened in the network elements.

Cisco ISC MPLS VPN Policy Manager allows the more experienced network operator to define the services that will be offered to customers.

Figure 1
Cisco ISC MPLS VPN Policy Manager Allows Network Operators to Define the Services That Will be Offered



The definition of an MPLS VPN service encompasses:

- PE-CE protocol and the protocol-specific configuration
- IP Address allocation
- Configuration of the CE router in the case of managed CE
- Redistribution of CE routing protocols
- Redistribution of PE routing protocols
- Option of joining the Management VPN
- Configuration of the VRF configuration on the PE (maximum number of routes on the VRF, import and export maps for the VRF routing table)

All the services parameters can be entered into an MPLS VPN service policy and left editable for the service operator who is going to use this service policy. ISC MPLS VPN Policy Manager allows customers to define global, technology-level policies. The software automatically generates the device-level commands and provisions all the devices involved in a service through its powerful internal parallel computation engines. Once the global policies are defined, they can be reused across multiple networks.



During MPLS VPN service activation, the service operator has only to select the PE-CE attachment circuits (also called connection legs) to activate the service. Cisco ISC calculates the configurations needed for all the devices to activate the service using the network topology information, PE-CE connection, and all the intermediate switch connections. By utilizing the live network element configurations and its just-in-time technology, ISC ensures that the generated configurations will successfully turn up the service.

Once the MPLS VPN service is deployed, the service operator needs to ensure that the end customers are getting the service they paid for. This step of testing and auditing is rendered by ISC's industry-tested MPLS VPN auditing technology.

New Technologies Introduction/Rapidly Changing Technologies

A new technology introduction requires acquisition of a new knowledge, training of the operators, and deployment experience. There is also a tremendous need for automating the deployment of MPLS VPN services. Service providers need automated tools to help them in their migration to new technologies as well as the ability to perform error-free operations in their service operations.

With the introduction of MPLS in service operator networks, technical staff must be trained to meet the challenges of a successful service deployment. The flexible architecture of ISC allows the network and service operator to be trained quickly. Network operators handle more complex tasks, while service operators, assisted by ISC, perform repetitive service-activation tasks. ISC keeps track of the configurations generated based on the service-activation intent.

Combined L2 and L3 VPN Services

More and more service providers are offering L2 and L3 services using a common MPLS infrastructure. L2 and L3 services are very different in terms of services and target customers. Both services exploit the same access and MPLS core infrastructure. For example, L2 switching access is tied to a PE and L2 VPN, and MPLS VPN services use the same L2-switching infrastructure to offer services to customers. A VLAN would be allocated for a given service/customer and would be configured on the customer-facing port. The VLAN traffic would be brought up to the PE via all the intermediate L2 switches and terminated on the PE.

For MPLS VPN, an L3 termination would be configured and added to a VPN. For an L2 VPN service, the VLAN would be terminated on the PE and a pseudo-wire would be created for the end-to-end connection. The co-existence of L2 and L3 services on the same infrastructure could be challenging for service operators.

Combined Technologies

Service providers are facing a mounting challenge dealing with a combination of technologies such as Optical, switching, and routing that co-exist in the same network. Service providers are also faced with customers that have been offered services with legacy technologies that have to be migrated to new technologies.

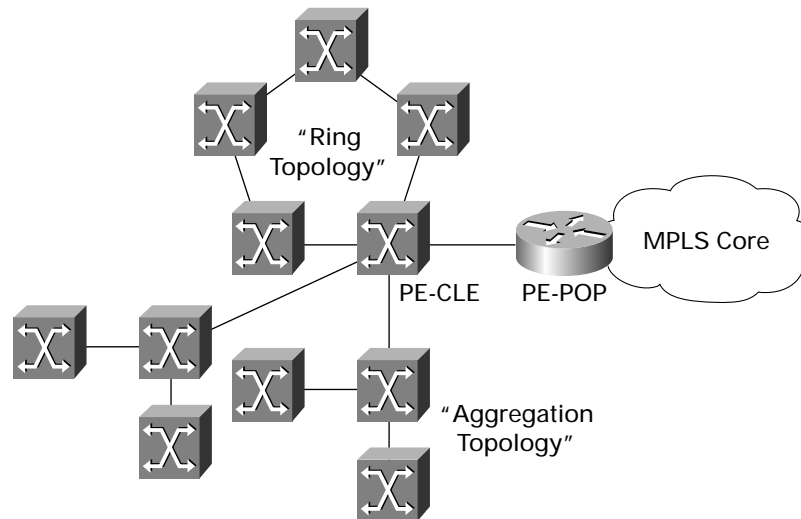
Training network and NOC operators presents a learning curve that the service operators have to undertake to adopt and deploy new technologies.



Complex and Diverse Access Architectures

Access architectures, such as L2 access technologies with aggregation switches and L2 rings of switches, can be diverse and complex.

Figure 2
Access Architectures Can be Diverse and Complex



Managing L2 access domains, keeping track of VLAN IDs allocated for customer services, and mapping them to MPLS VPN services or L2VPN is an increasingly difficult challenge that some service operators are facing.

ISC manages these scenarios with extreme ease. ISC can offer services for L2 aggregation access domain or L2 ring topologies. The L2 access domain can be used for L2 access into MPLS VPN or simply L2VPN services using EoMPLS.

Security Aspects

Security issues range from restricting MAC addresses and controlling the VLAN traffic that was allocated for a given customer to detecting an intrusion in the network. Service providers need automated tools to provision and track these security issues in the network.

Operations-Related Challenges

Network Operations, commonly known as NetOps, is typically either a separate organization or part of the Information Technology department. The type of governance is very important because it does indeed impact how efficient and aligned the Network Operations organization is. Depending on the scale of the network to be managed, NetOps may have one or more NOCs centralized, or distributed in a hierarchical manner. These NOCs in almost all cases operate 24x7. NOCs of global service providers also implement a follow-the-sun concept where some or all NOC functions are “handed over” to other NOCs when time zone shifts occur.



Depending on the governance and workflow process, NOC operators tend to perform a number of functions:

Fault management and problem resolution

When a service-affecting fault occurs in the network, the NOC operator must respond rapidly. ISC provides the service operator with a summarized report of the deployed service containing all the parameters needed to troubleshoot the problem. ISC also has a functional audit to detect if the requested customer service is actually working.

Configuration management and configuration change management

Configuration management and change management (moves/adds/changes) allows service providers to manage multiple versions of hardware and software elements and make network configuration changes through the Element Managers. The data concerning the current network environment is input and used by the service providers to modify the device configuration and process “adds-and-deletes” requests. This feature also maintains a configuration inventory of all monitored elements. Note that configuration management constitutes a part of the service activation in a provisioning order request.

Using an intelligent configuration engine, ISC supports service activation for various platforms and Cisco IOS versions. This allows service providers to migrate their networks to a newer version of Cisco IOS in a progressive fashion without disrupting customer services.

Accounting and usage data collection

ISC ensures that accounting and usage data collection is done in a continuous and reliable manner (not that billing will typically reside in the customer care organization). ISC offers the SLA probe configuration as well as VPN-aware SLA collection.

Security management

In order for NOC staff to efficiently perform the above tasks, roles and associated tasks are clearly delineated between operators to minimize errors. For instance, some operators are dedicated to trouble ticketing, some to configuration changes, while others focus on problem resolution. The importance of the NMS/OSS application and its usability is crucial.

NOC operators expect an NMS/OSS application to meet the following requirements and features:

- Easy-to-use GUI providing clear and helpful user suggestions for corrective actions in the event of error messages
ISC’s web-based GUI is very intuitive to navigate and use. ISC’s Service Policy Manager makes the activation tasks very easy to use.
- Access control and partitioning of admin domains restricting operators to only view and access parts of the network under their control

ISC’s Role-based Access Control defines user roles, user-group roles, and users. Users with a certain role, or credential, can only view and work within the credential given by their role. Only the ISC administrator, for example, can create MPLS VPN or L2VPN roles and assign login users to them. A MPLS VPN user can only activate MPLS VPN service, and can access any L2VPN policies and service activation. A user assigned to a given customer can only view and work on the services and policies for that customer.

- Minimum number of steps to accomplish a given function such as creating a service or change request. When several steps are required and a parameter change is needed, users prefer a way of back tracking to make the changes



ISC's Service Policy Manager helps define the service with editable and non-editable parameters. When a service operator uses this policy, the non-editable parameters will not be prompted to the user.

- Function for validating actions before any configuration change is made to the network

ISC's just-in-time technology ensures that the configuration generated is accurate, reflects what is actually in the network, and that the generated configuration will turn-up a requested service.

- Monitoring function for service requests (moves, adds, and changes)

ISC's MPLS VPN Service Auditing function keeps track of all the configuration changes that occur in the network elements and determines whether they are service effecting. ISC's MPLS VPN Service Auditing ensures that the requested customer routing is happening correctly.

- A frequently updated inventory of the service requests made so far or those being processed

ISC's RDBMS system ensures that ISC-managed service requests are stored properly.

- When the NMS/OSS application is rich in features and functions, a hierarchical navigation tree is desirable to remind the user of what navigation level they are at
- Access to a pull-down menu of network devices and services or protocols to be configured for newly deployed services
- Context-sensitive help whenever possible

NOC operators are taskmasters, not subject matter experts, and help with even the basic acronyms is an important feature to have. Operators don't have the time to research what a given term or concept means.

- A good search capability within the NMS/OSS application to quickly locate objects of interest such as devices, services, and related attributes
- Logging and audit trail capabilities to be able to trace back who did what and when

This is important especially for support problem resolution purposes. All the users' activities are logged based on time, date, type of action, and object manipulated. This can be retrieved and queried only by the ISC administrator.

- Easy-to-use policy management function for service policy lifecycle management

Technology Overview

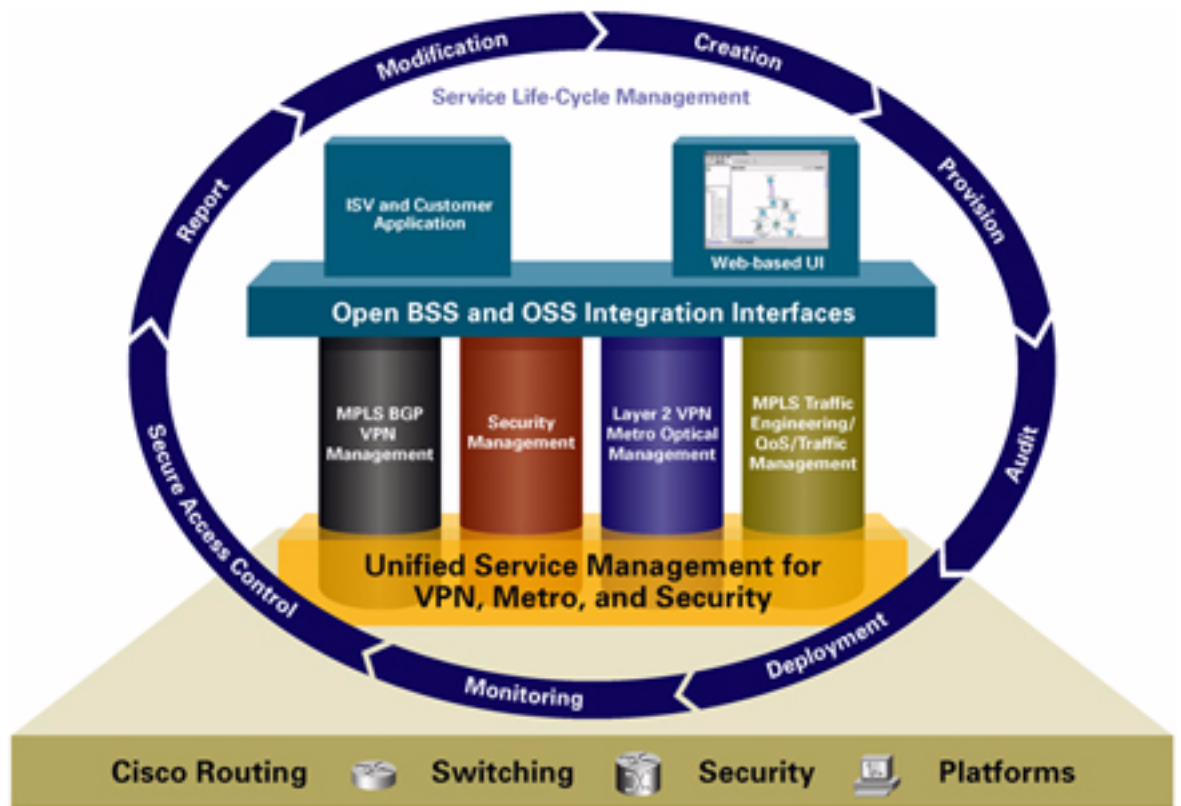
Cisco's IP Solution Center is a carrier-class network and service-management offering for the rapid and cost-effective delivery of IP services. IP-based services targeted to enterprise customers can represent major revenue opportunities for service providers. Success in this highly competitive market requires the ability to effectively plan, provision, operate, and bill for such IP services.

Service providers are required to deliver advanced and reliable telecommunications services in a timely manner to demonstrate leadership in a competitive market. This competitive environment has created new business opportunities and new challenges for communications equipment providers. In addition to manufacturing hardware to support new communications technologies, communications equipment providers are expected to provide associated management products to enable rapid service delivery.



Service providers rely upon communications equipment vendors to provide management systems that enable and simplify the task of operating the network and its services. Service providers also require these management products to be integrated with their existing Business Support Systems and Operations Support Systems infrastructure. As this infrastructure grows in size and complexity, so does the requirement for vendors to provide much more functionality beyond element and network management.

Figure 3
Cisco ISC Provides a Robust and Centralized Management Platform for Managing the Entire Lifecycle of MPLS VPN Services



Deploying and offering MPLS VPN services for enterprise customers requires planning of network resources, deploying, maintaining, and finally configuring the network elements and services. This manual procedure can be time consuming and inaccurate. A service provider needs to automate all these steps in order to stay competitive in this high-touch market.

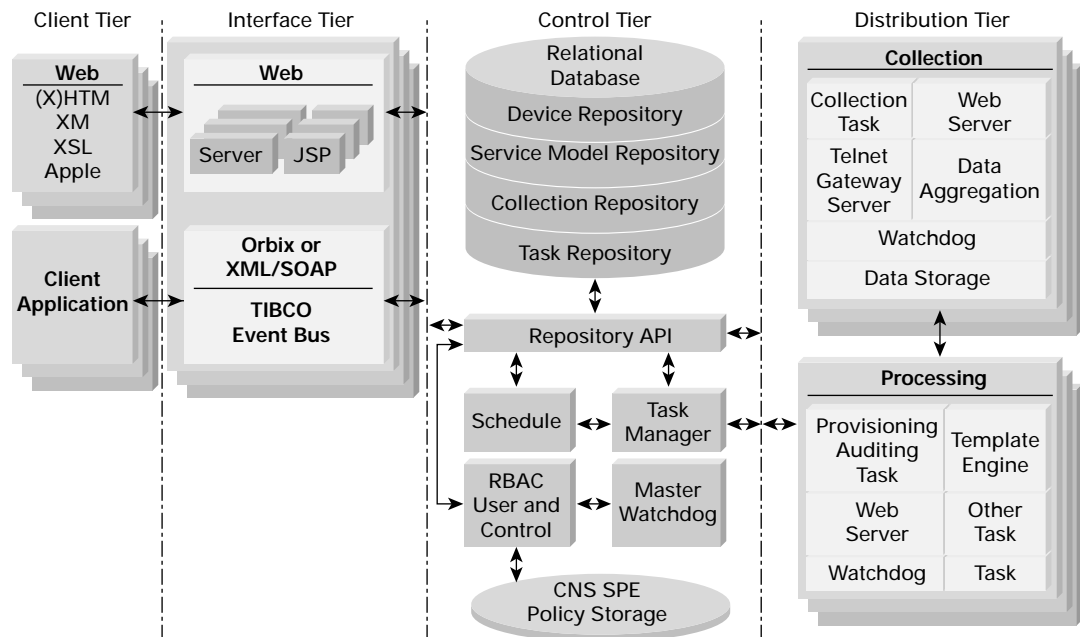


ISC System Architecture

Cisco IP Solution Center is a four-tiered architecture for maximizing scalability, redundancy, and robustness. The four tiers are: Client, Interface, Control, and Distribution. This architecture provides the modular framework that is the foundation of this scalable, carrier-class system:

- *Client Tier*—Web-based GUI (HTTP to Web server) or client application (RMI to EJB container)
- *Interface Tier*—Scalable J2EE AppServers (Web server and EJB container)
- *Control Tier*—Repository, task manager, watchdog, and scheduler
- *Distribution Tier*—Task worker and collection domain servers

Figure 4
IP Solution Center Architecture





ISC MPLS VPN Service Management

Feature	Description	Advantage/Value
Distributed Architecture	ISC 3.0 is a 4-tiered system: Client, Interface, Control, and Distribution tier	ISC's four-tier architecture offers a scalable and reliable architecture for large-scale operations.
PE-CE Routing Protocols	<ul style="list-style-type: none">• OSPF• EIGRP• RIP• Static• BGP	
VRFLite/Multi-VRF CE Support	ISC enables the management of VRF-lite CE	A VRF-lite CE offers an enhanced VPN traffic separation up to the CE, enhancing security for business customers.
Various PE-CE Routing Protocols	In MPLS VPN architecture, various routing protocols such as RIP, OSPF, BGP, and EIGRP are allowed as PE-CE routing protocols	ISC offers complete PE-CE protocol configuration.
Multicast VPN Support	Multicast VPN allows service providers to configure and offer multicast traffic in a MPLS VPN environment	MPLS VPNs only support unicast traffic connectivity. Deploying the Multicast-VPN feature in conjunction with MPLS VPN allows service providers to offer both unicast and multicast connectivity to MPLS VPN customers. ISC offers the configuration and monitoring of Multicast MPLS VPNs.
Thin-web GUI Client	ISC's user interface is a thin web-based client	A thin web-based client is much easier to utilize. Training the network operator is easier.
Policy-based Provisioning	A Service Policy captures all the provisioning parameters such as PE-CE protocol, IP numbering, and VLAN Auto-Allocation. These provisioning parameters can be defined in a Service Policy and used during service activation	Using Service Policies for service activation greatly reduces the service operator's tasks as the only parameters required for service activation have already been captured in the service policy. Only information that is particular to the service is requested from the service operator.
Managed and Unmanaged CE Option	ISC's smart management can handle the managed and unmanaged CE scenario	Service providers that want to manage CPE can do so with ISC.
Provisioning Based on Current Network	Prior to service activation, ISC always uploads the configuration of the network elements to calculate the delta configuration needed to have a successful service activation	There is always a possibility that the network configuration could have varied since the last snap-shot. By uploading the configuration prior to applying the configuration, ISC ensures that the service activation configuration will be successfully applied and will not collide with the existing configuration.
Auto-Discovery of MPLS VPN Services	ISC can discover MPLS VPN services that were configured prior to ISC's activation on the service provider's network	Service providers could have manually configured several MPLS VPN services for customers. To continue managing these services, ISC's MPLS VPN Service Discovery can be used to discover these services and continue managing them using ISC.
Role-based Access Control	ISC implements Role-based Access Control that gives very granular access privileges to ISC users	Role-based Access Control gives access control to the service providers who want to implement strict operational processes.



Feature	Description	Advantage/Value
Automatic Allocation of RD, RT, AS, and VRF	ISC allows the automatic allocation of parameters during MPLS VPN provisioning such as Router Target (RT), Route Distinguisher (RD), AS (Autonomous System Number for BGP Version 4), and VRF name	
Automatic Resource Allocation	ISC enables the service operator to automatically allocate resources such as IP addresses, VLAN, Route Distinguisher, and Router Target	Automatic Resource Assignment relieves the service operator from manually entering certain parameters during service activation. ISC keeps track of all the allocated resources and to which service, customer, or site these resources were allocated.
Grey Management VPN	• ISC supports the management MPLS VPN. All the CEs that are managed by service providers can also be added to the management VPN	All service provider managed CEs can be added to the grey management VPN in order to be managed and monitored.
Inter-AS Management	The provisioning across AS can be problematic. In MPLS VPN, multiple providers can inter-operate their network using different BGP Autonomous System numbers	ISC seamlessly manages the provisioning of inter-AS MPLS VPN Services.
L2 Access into MPLS VPN	In more and more cases, service providers utilize L2 Ethernet switches to distribute their services to customers. L2 Access Domain can be in an aggregation or ring topology	Using Ethernet switches to distribute service to customers is one of the most cost-effective ways to deliver services. ISC can handle L2 Access Domain with aggregation or ring topologies. ISC seamlessly allocates VLANs for customers and maps the VLAN to a MPLS VPN at the PE level.
Northbound Interface CORBA and XML over HTTP	In order to integrate with other OSS FCAPS applications, ISC provides CORBA for backward compatibility with VPNSC 2.2 and, going forward, provides XML over HTTP/HTTPS	Other FCAPS OSS applications need access to ISC's VPN topology information, via its northbound interface, to offer flow-through provisioning, extracting the VPN customer information, for example, for any fault application.

Leveraging ISC MPLS VPN for a Large MPLS VPN Deployment—Case Study

A service provider, ABC, provides site-to-site IP connectivity to an existing customer base. ABC's infrastructure is all IP based.

Recently, ABC has been losing customers to a new competitor, XYZ, who is offering IP MPLS VPN services. Many of ABC's customers have switched to XYZ. ABC wants to upgrade its network to offer MPLS VPN services. ABC decides to upgrade its network and provide a differentiated MPLS VPN Service to its customers.

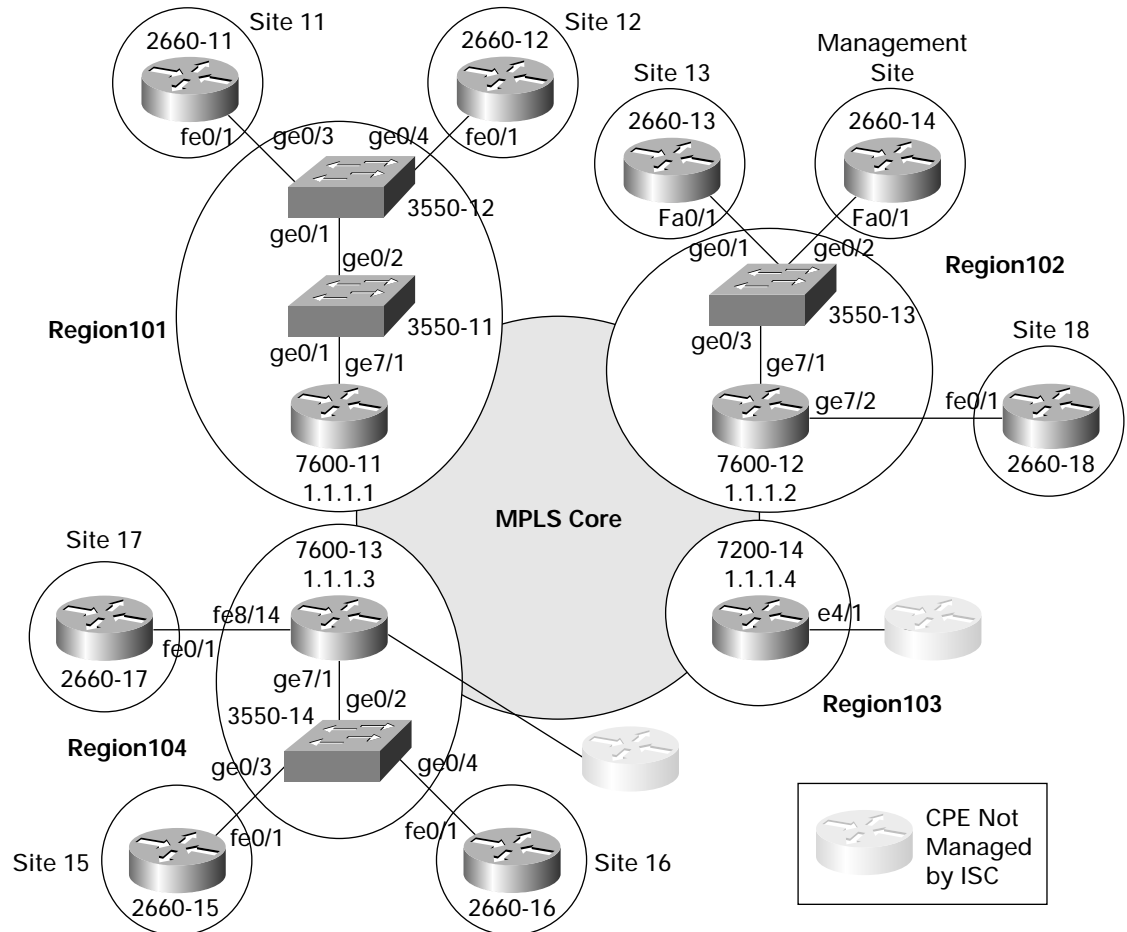
ABC takes the following steps to successfully compete with XYZ:

- Upgrades its core network to be MPLS-enabled
- Uses L2 access switches to distribute Ethernet services to its customers
- Hires knowledgeable network engineers to train its NOC operators and field staff
- Explain to its customers the services it wants to offer

Figure 5 illustrates what ABC's network would look like.



Figure 5
Service Provider ABC's MPLS VPN Network



Advantages of Having Chosen This Network

Turning on MPLS in the core of its network, ABC is able to offer very good security due to the isolation of VRF routing (for example, only routing inside a VPN is seen and published to the customer-connected sites). Using an L2 access switch to distribute access to its customers is a very savvy choice. L2 Access Ethernet has an excellent ROI model, and advanced QoS can be applied to customer traffic to guarantee QoS.

Defining the Services That ABC Wants to Offer

Service provider ABC can define all details of the service deployment in ISC's Service Policy. ABC decides to offer MPLS VPN services with the following parameters:

- L2 access into MPLS VPN
- BGP is the default protocol for PE-CE connection
- VLAN ID will be auto-allocated for customers
- IP Addresses for PE-CE connections will be auto-assigned
- Offer VRF-Lite CE for building co-resident customers

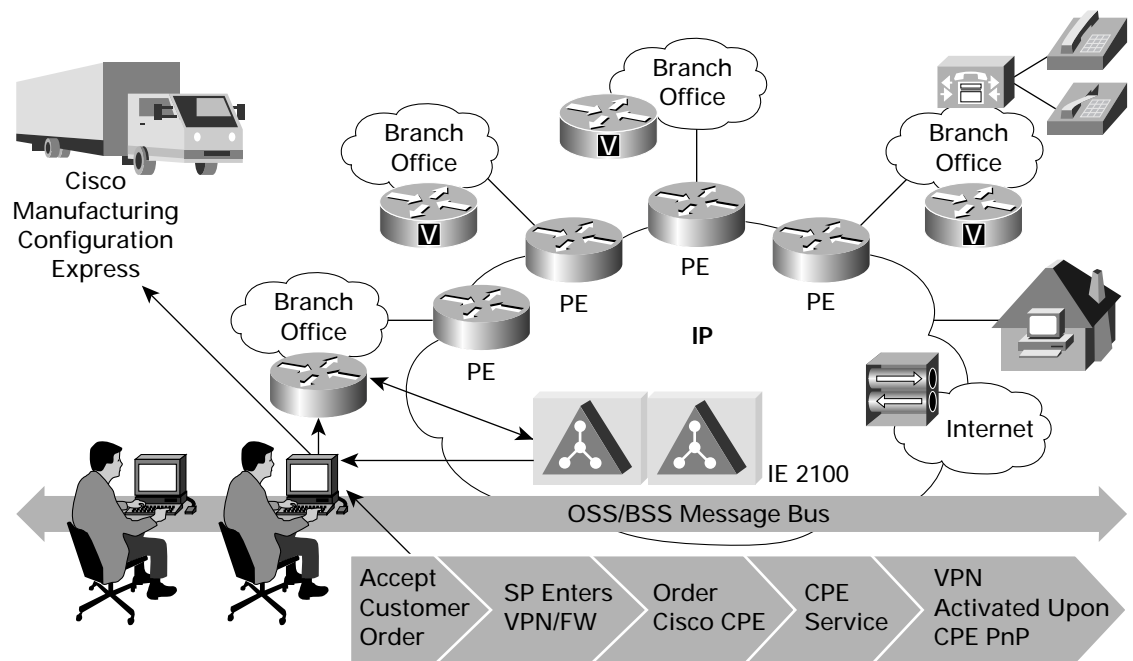


ABC defines all these service-related parameters in ISC's MPLS VPN Service Policy. By defining the service policies, ABC's service operators who are going to deploy the services will not have to go through all the steps to activate a service. Service policies represent the service that the service provider wants to offer its customers.

Rapid Deployment of CPE

ABC wants to deploy Cisco 3550 switches as CPE and offer MPLS VPN services to its corporate customers.

Figure 6
ISC Enables Rapid Deployment of CPE



The deployment process includes the following steps:

- CPE is shipped out of Cisco's manufacturing facility with a minimal configuration in the network element, which is needed for the CPE to become active in the network
- The customer receives the CPE and plugs it into the service provider's Ethernet uplink
- The CPE is powered up and contacts the network appliance that is programmed in the configuration
- The Cisco CNS IE 2100 network appliance responds with the CPE's configuration
- The CPE is now ready for service activation, and can participate in the service provider's network

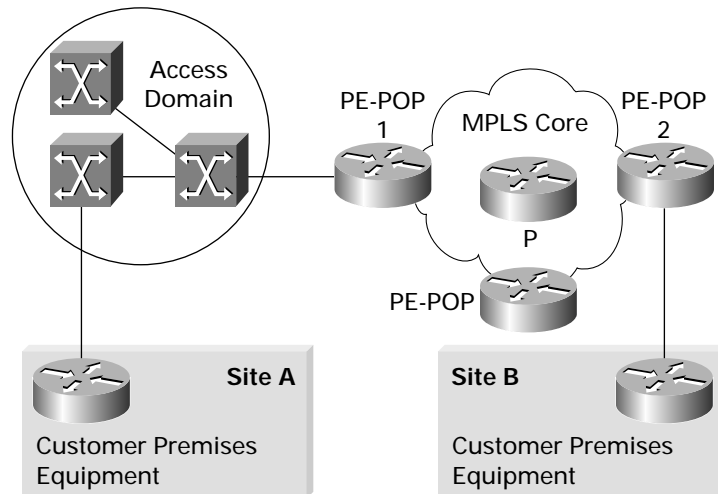


Turning Up MPLS VPN Service

A customer has requested service provider ABC to provide MPLS VPN service between sites A and B.

Figure 7

Customer Deployment of MPLS VPN



The MPLS VPN Service Policy for this customer is defined below:

- RIP as PE-CE protocol
- Redistribute connected on the CE, redistribute OSPF from the CE
- Auto-Allocation VLAN for the L2 access domain
- Automatic assignment of IP address for the PE-CE connection
- Automatic join of CE IP address into Management VPN

ABC is also offering its customers the option of managed CEs (for example, the customer premises equipment is owned by the service provider, but is leased by the customer). Deployment is as follows:

1. The service operator receives an order form with the two sites to be connected and the network elements closest to sites A and B.
2. The service operator selects the MPLS VPN service policy defined for this customer.
3. The service operator selects both sites A and B as MPLS VPN hubs.
4. The service operator activates the service.
5. ISC allocates a VLAN for site A, as site A is connected via L2 access switches. This VLAN is added and allowed to pass all the intermediate switches up to the PE routers.
6. An IP address is allocated for the PE-CE connection (for example, this IP address is taken out of the IP address pool associated with the PE in this case). This IP address allocation is performed for both sites A and B.
7. ISC collects just-in-time configuration from all the network elements that are involved in the service. Based on the actual Cisco IOS configuration, ISC generates IOS CLI Configlets needed to activate the service request.
8. ISC applies the generated IOS CLI Configlets to all the devices participating in the service.



9. ISC uploads the configuration to verify that the configuration that got downloaded is actually present in the network elements. This phase of the service activation is called Configuration Audit.
10. After a configurable time, ISC proceeds with a Functional Routing Audit to verify the routing information has actually propagated as the customer requested.

If ABC's customer wants to add more sites to their VPN, this is as easy as adding additional attachment legs to the existing service and redeploying the service.

Business Benefits

Cisco ISC offers complete MPLS VPN services management with rapid deployment and error-free provisioning capabilities. ISC also provides scalability and redundancy with its distributed architecture. A service operator can begin with a single machine where ISC is installed and add processing servers that will be used by the ISC's master machine to off-load processing and monitoring. ISC's master machine controls and monitors all its processing servers to deliver load-balancing and error-free provisioning.

ISC's MPLS VPN service blade can be deployed with ISC's other service blades such as L2VPN that supports ATOM features, as well as QoS, IPsec, and Firewall service blades.

The benefits of utilizing Cisco ISC for deploying and managing MPLS services include time to market, improved network quality, reduced operational costs, and a lower total cost of ownership. The comprehensive management functionality of Cisco ISC also enables customers to minimize initial investments by taking full advantage of existing infrastructures and devices. Cisco ISC provides flexibility as well as allowing customers to implement the most suitable framework—MPLS VPN services that require robust authentication, confidentiality, and secure scanning. Cisco ISC ensures that customers can meet both current and future service requirements without having to undergo “forklift” upgrades.

Conclusion

Cisco ISC eliminates common deployment and management issues by elevating the service administrator's role to that of business manager, as opposed to low-level device-specific policy manager and administrator. Cisco ISC implements a business-centric, service-level management model that allows customers to define high-level policies, while the application of those policies to specific network devices is offloaded to the ISC software.

ISC simplifies management of complex multiaccess, multiplatform IP services, and reduces management costs. Cisco ISC service options provide service-level provisioning, service-aware performance and service-level assurance, and service-aware usage. Accepted worldwide by over 160 leading corporations, Cisco IP Solution Center (evolution of well-established Cisco VPNSC) is the standalone management solution for effective management of converging services, supporting a unified view of MPLS VPN, Metro Ethernet, Security, and QoS services through a common repository of information across all these packet-based services.

Cisco ISC simplifies and speeds the deployment and management of packet-based services for faster time to revenue while increasing operating efficiencies. It is an end-to-end network management solution that scales as an organization evolves.

Cisco ISC provides the software management application that enable rapid and accurate deployment of security services. Simultaneously, the solution simplifies management of complex, multiaccess, multiplatform security services. The Cisco ISC MPLS VPN Services module provides full support for the provisioning and management of MPLS VPN services, Remote Access VPN, L2

Access into MPLS, and various access technologies for PE-CE interfaces such as ATM, Frame Relay, Serial, VLAN, and Ethernet. ISC hides the complexity of provisioning MPLS VPN services.

For More Information

Visit the [Cisco IP Solution Center](#) product page for more information.



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo 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.
(0304R) VT/LW4442 0403