

Deploying Layer 2 VPN Services with Cisco IP Solution Center

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

The Cisco® IP Solution Center provides enterprises and service providers with a robust and centralized management platform that minimizes the deployment costs of Layer 2 virtual private network (L2VPN) services and helps to guarantee the accuracy of service deployment. The solution effectively deploys and manages the entire life cycle of L2VPN technologies, including policy-based VPNs, management VPNs, and service-level agreement (SLA) and quality-of-service (QoS) provisioning. Cisco IP Solution Center is tightly integrated with Cisco CNS technology for zero-touch, plug-and-play Multiprotocol Label Switching (MPLS) VPN customer premises equipment (CPE) deployment.

Market Challenges

Conservative capital expenditure (CapEx) budgets are pushing service providers to invest only in those areas of their infrastructure directly affecting the bottom line. Moreover, several service providers are investing in network management systems (NMSs), operations support systems (OSSs), and business support systems (BSSs) to squeeze more value out of their existing networking infrastructures built during the CapEx race of the mid-to-late 1990s. To sustain high-margin revenues, however, service providers are eager to be the first to

market with new services, particularly to their business customers. These services include IP security (IPsec), MPLS VPNs, managed security services, voice over IP (VoIP), and video on demand for cable multiple system operators (MSOs).

With the rapid growth of the metro Ethernet market, service providers are increasingly challenged to manage their networks and deploy services to customers. Service providers must decide whether to deploy new metro Ethernet networks or to build out MPLS networks to phase out or complement existing Asynchronous Transfer Mode (ATM) or Frame Relay access. These existing access technologies must be migrated to an MPLS backbone network infrastructure.

Service Challenges

Service providers must ensure that there is an alignment between new services offered and 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 integration with the overall service order-to-service activation process
- Skills 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 new service are important—they are tightly related to revenue objectives, including the number of transactions to break even, time-to-provision goals, and billing accuracy. The OSS application for enabling the new service(s) is paramount in accelerating 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 network operations center (NOC) service engineer needs to keep track of network element configurations, tracking an enormous amount of information. 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 offer. This requires training the NOC staff to effectively operate the network and activate services. Critical components include rapid deployment of services, accuracy of deployed configurations, and the ability to trace network elements.

Cisco IP Solution Center L2VPN Policy Manager allows the more experienced network operator to define the services that will be offered to customers (Figure 1).

Figure 1
Cisco IP Solution Center L2VPN Policy Manager

L2VPN Service Policy (Defined by and Experienced Network Operator)	L2VPN Service Activation (Used by a Service Operator)
<p style="text-align: right;">Editable</p> <ul style="list-style-type: none"> • Premise Interface, Customer Interface <input checked="" type="checkbox"/> • Ethernet Wire Service (EoMPLS) <input checked="" type="checkbox"/> • Ethernet Relay Service (EoMPLS) <input checked="" type="checkbox"/> • Frame Relay over MPLS <input type="checkbox"/> • ATM over MPLS <input type="checkbox"/> • VLAN ID auto-pic <input type="checkbox"/> 	<ul style="list-style-type: none"> • Selection of Premise Equipment and Customer Equipment Interface • Selection of the Type of L2VPNS Service Policy • Selection of the Attachment Circuit

An L2VPN service includes:

- What the provider edge or customer edge interface is
- The type of L2VPN service policy
 - Ethernet Wire Service (Ethernet over MPLS [EoMPLS])
 - Ethernet Wire Service (EoMPLS)
 - Frame Relay over MPLS
 - ATM over MPLS
- Auto-allocation of virtual LAN (VLAN) IDs



All of the service parameters can be entered into an L2VPN service policy and left editable for the service operator who is going to use this policy. Cisco IP Solution Center MPLS VPN Policy Manager allows customers to define global technology-level policies. The software automatically generates the device-level commands and provisions all of 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 L2VPN service activation, the service operator has only to select the provider edge to customer edge attachment circuits (also called connection legs) to activate the service. Cisco IP Solution Center calculates the configurations needed for all devices to activate the service using the network topology information, provider edge to customer edge connection, and all of the intermediate switch connections. By using the live network element configurations and its just-in-time technology, Cisco IP Solution Center ensures that the generated configurations will successfully turn up the service.

Once, the L2VPN service is deployed, the service operator needs to ensure that end customers are getting the service they paid for. This step of testing is rendered by the Cisco IP Solution Center L2VPN auditing feature.

New Technology Introduction/Rapidly Changing Technologies

A new technology introduction requires acquisition of new knowledge, training the operators, and deployment experience. There is a tremendous need for automating the deployment of L2VPN services. Service providers need automated tools to help them in their migration to new technologies, as well as the ability to perform error-free service operations.

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

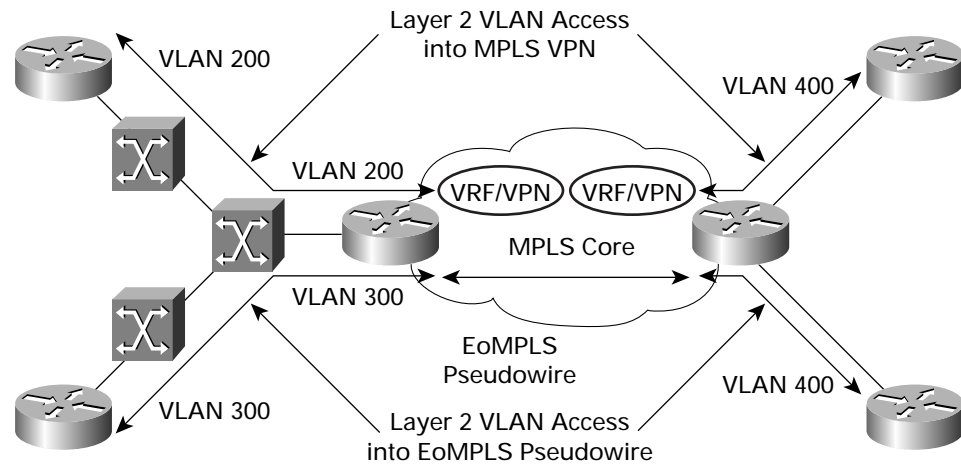
Combined Layer 2 and Layer 3 VPN Services

Service providers are increasingly offering Layer 2 and Layer 3 services using a common MPLS infrastructure. Layer 2 and Layer 3 services are different in terms of services and target customers, but both services exploit the same access and MPLS core infrastructure.

In the case of a Layer 2 switching access tied to a provider edge, the Layer 2 VPN and MPLS VPN services use the same Layer 2 switching infrastructure to offer services to customers. A VLAN would be allocated for a given service or customer and would be configured on the customer-facing port. The VLAN traffic would be brought to the provider edge via the intermediate Layer 2 switches and terminated on the provider edge.



Figure 2
Coexistence of Layer 2 and Layer 3 VPN Services



For MPLS VPNs, the allocated VLAN will be terminated on a subinterface and added to a VPN routing/forwarding instance or VPN. For a Layer 2 VPN service, the VLAN would be terminated on the provider edge and a pseudowire would be created for the end-to-end connection. The coexistence of Layer 2 and Layer 3 services on the same infrastructure could be challenging for service operators.

Combined Technologies

Service providers are challenged to deal with a combination of technologies that coexist in the same network, such as optical, switching, and routing. Service providers are also faced with customers that have been offered services with legacy technologies that have to be migrated to new technologies.

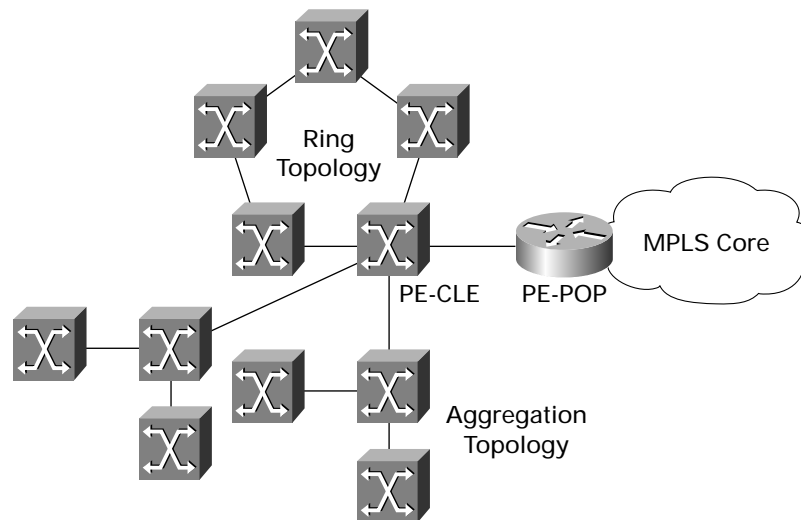
Training service and network engineers presents a learning curve that service operators have to undertake to adopt and deploy new technologies.



Complex and Diverse Access Architectures

Access architectures, such as Layer 2 access technologies with aggregation switches and Layer 2 rings of switches, can be diverse and complex (Figure 3).

Figure 3
Access Architectures Can be Diverse and Complex



Managing Layer 2 access domains, keeping track of VLAN IDs allocated for customer services, and mapping them to MPLS VPN services or L2VPNs is an increasingly difficult challenge. Cisco IP Solution Center manages these scenarios with ease, offering services for Layer 2 aggregation access domain or Layer 2 ring topologies. The Layer 2 access domain can be used for Layer 2 access into MPLS VPNs, or simply L2VPN services using EoMPLS.

Security Aspects

Security issues range from restricting Media Access Control (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 Challenges

Network operations is typically either a separate organization or part of the IT department. The type of governance is important—it affects the efficiency and alignment of the network operations organization. Depending on the scale of the network to be managed, the network operations organization may have one or more NOCs centralized, or distributed in a hierarchical manner. These NOCs usually 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.

NOC service and network engineers typically perform numerous functions, including:



Fault Management and Problem Resolution

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

Configuration management and configuration change management

Configuration management and configuration change management (moves, adds, and changes) allows service providers to manage multiple versions of hardware and software elements and make network configuration changes through element managers. The current network configuration and software versions are input into Cisco IP Solution Center and then used by service providers to modify the device configuration and process “add-and-delete” requests. This feature also maintains a configuration inventory of all monitored elements. Configuration management constitutes a part of the service activation in a provisioning order request.

Using an intelligent configuration engine, Cisco IP Solution Center supports service activation for various platforms and Cisco IOS® Software releases. This allows service providers to migrate their networks to a newer Cisco IOS Software release in a progressive fashion without disrupting customer services.

Accounting and Usage Data Collection

Cisco IP Solution Center ensures that accounting and usage data collection is done in a continuous and reliable manner (even though billing does not typically reside in the customer care organization). Cisco IP Solution Center offers the SLA probe configuration as well as VPN-aware SLA collection.

Security Management

In order for NOC staff to efficiently function, 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, and some to problem resolution. The importance of the NMS/OSS application and its usability is crucial. NOC service and network engineers expect an NMS/OSS application to meet the following requirements and features:

- An easy-to-use graphical user interface (GUI) providing clear and helpful suggestions for corrective actions in the event of error messages.

The Cisco IP Solution Center Web-based GUI is intuitive to navigate and use. The Cisco IP Solution Center Service Policy Manager simplifies activation tasks.

- Access control and partitioning of administrator domains, restricting operators to only view and access the parts of the network under their control.

Cisco IP Solution Center Role-Based Access Control (RBAC) 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 Cisco IP Solution Center administrator, for example, can create MPLS VPN or L2VPN roles and assign login users to them. An MPLS VPN user can only activate MPLS VPN services, 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.

- A 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.



The Cisco IP Solution Center Service Policy Manager helps define the service with editable and noneditable parameters. When a service operator uses this policy, the noneditable parameters will not be prompted to the user.

- A function for validating actions before any configuration change is made to the network.

Cisco IP Solution Center just-in-time technology ensures that the configuration generated is accurate, reflects what is actually in the network, and will turn up a requested service.

- A monitoring function for service requests (moves, adds, and changes).

The Cisco IP Solution Center MPLS VPN service auditing function keeps track of all the configuration changes that occur in the network elements and determines whether they affect service. The Cisco IP Solution Center MPLS VPN service auditing function ensures that the requested customer routing is happening correctly.

- A frequently updated inventory of service requests made and those being processed.

The Cisco IP Solution Center RDBMS system ensures that Cisco IP Solution Center-managed service requests are stored properly.

- A hierarchical navigation tree.

When the NMS/OSS application is rich in features and functions, a hierarchical navigation tree can 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 service and network engineers are taskmasters, not subject matter experts, and help with even the basic acronyms is an important and time-saving feature.

- A good search capability within the NMS/OSS application.

This allows the application to quickly locate objects of interest such as devices, services, and related attributes.

- Logging and audit trail capabilities.

This feature is especially important for support problem resolution purposes. All user activities are logged based on time, date, type of action, and object manipulated. This can be retrieved and queried only by the Cisco IP Solution Center administrator.

- Easy-to-use policy management function for service policy life cycle management.

Technology Overview

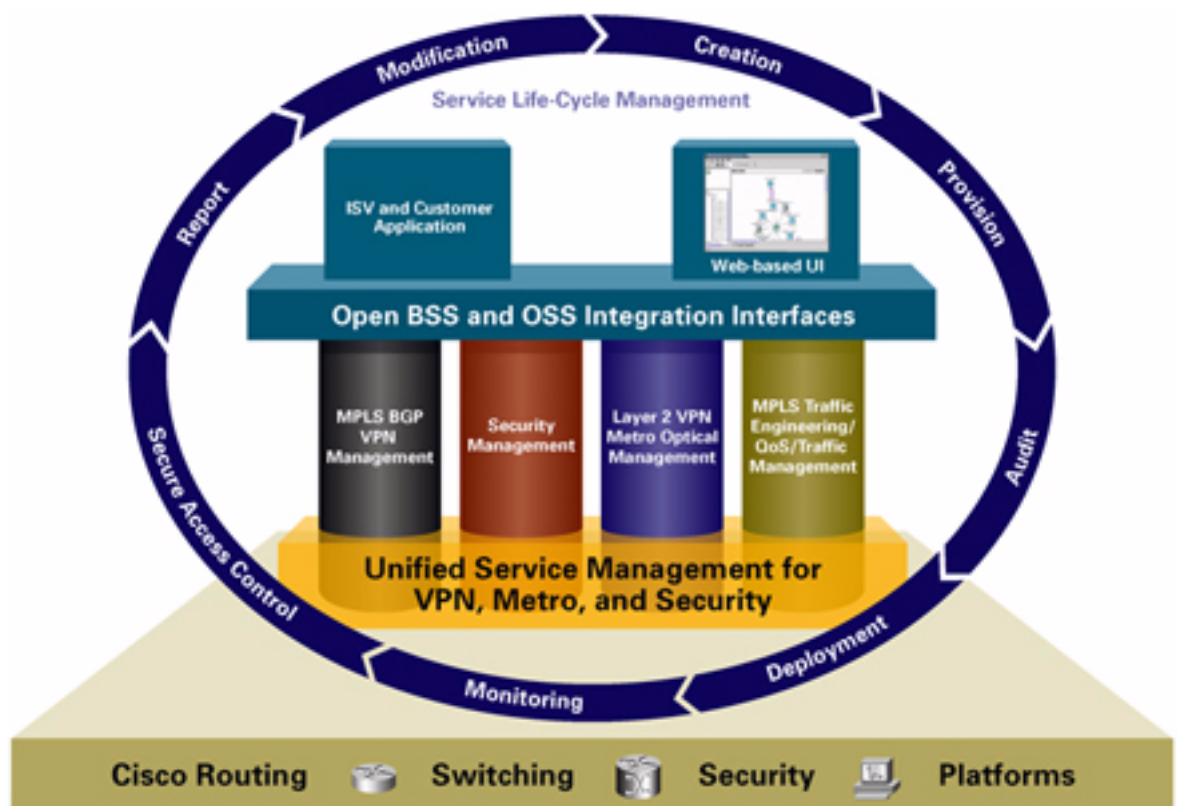
Cisco IP Solution Center is a carrier-class network and service management offering for the rapid and cost-effective delivery of IP services. IP-based services targeted to enterprise customers can represent major revenue opportunities for service providers. Success in this highly competitive market requires 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 BSS and OSS infrastructures. As these infrastructures grow in size and complexity, so does the requirement for vendors to provide more features beyond element and network management. Cisco IP Solution Center provides a robust and centralized management platform for managing the entire lifecycle of security services (Figure 4).

Figure 4
Cisco IP Solution Center



Deploying and offering MPLS VPN services for enterprise customers requires planning of network resources and 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 of these steps in order to stay competitive in this high-touch market.



Cisco IP Solution Center System Architecture

Cisco ISC is a distributed, 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 application servers (Web server and EJB container)
- *Control Tier*—Repository, task manager, watchdog, and scheduler
- *Distribution Tier*—Task worker and collection domain servers

Figure 5
Cisco IP Solution Center Architecture

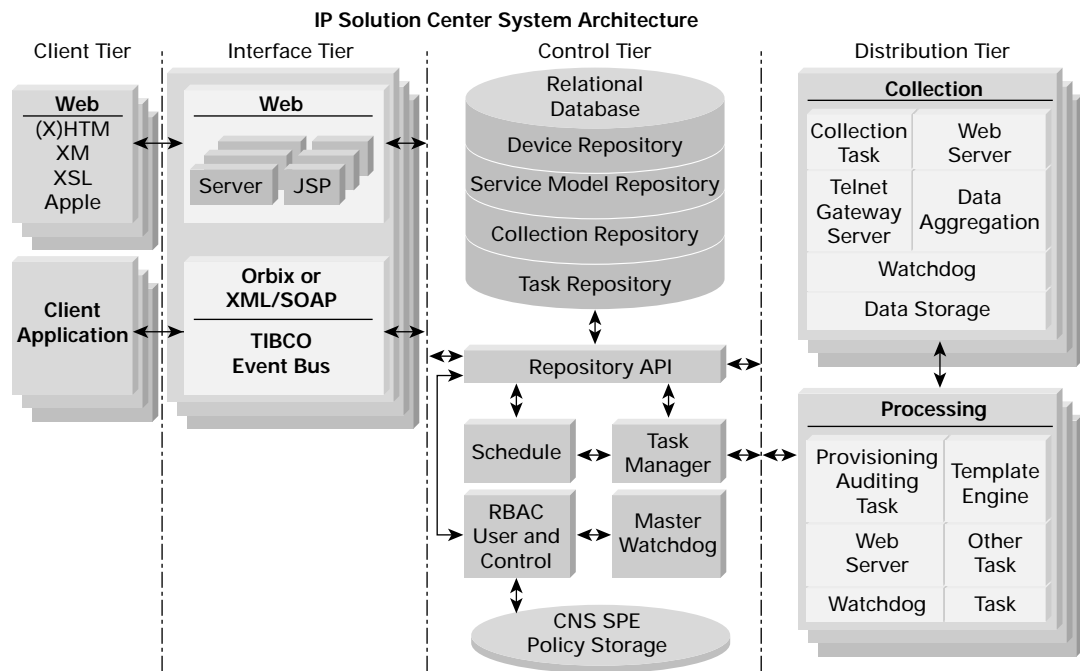




Table 1 lists features of Cisco IP Solution Center L2VPN.

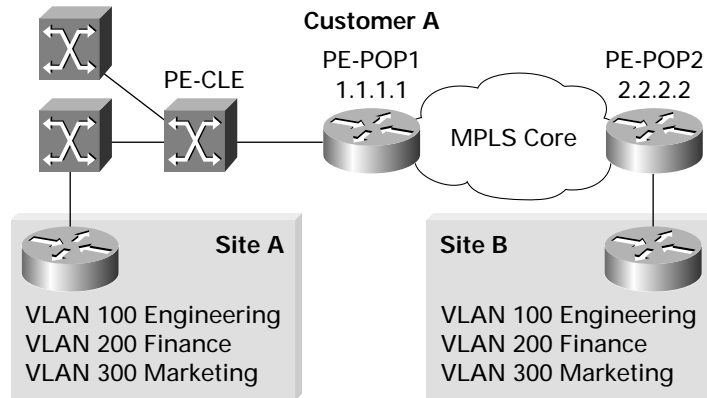
Table 1 Cisco IP Solution Center L2VPN Service Management Features

Policy-based provisioning	<ul style="list-style-type: none"> • All service-offering-related parameters can be included in an L2VPN service policy • When a service operator uses this predefined policy, all of the complexities of service activation are hidden from the operator
Easily managed full-mesh, hub-and-spoke, and partial-mesh VPN topologies	<ul style="list-style-type: none"> • Cisco IP Solution Center generates the entire configuration for routers and switches for full-mesh, hub-and-spoke, or partial-mesh L2VPN configurations
Configuration audit	<ul style="list-style-type: none"> • Cisco IP Solution Center ensures for each deployed L2VPN service that the routers' configuration is correct and that the routing between the customer edges is what the service operator requested
L2VPN discovery	<ul style="list-style-type: none"> • Cisco IP Solution Center autodiscovers EoMPLS predeployed services
Services supported: <ul style="list-style-type: none"> - Ethernet Wire Service - Ethernet Wire Service - Layer 2 access into MPLS VPN - ATM over MPLS - Frame Relay over MPLS 	<ul style="list-style-type: none"> • Cisco IP Solution Center supports single provider edge or Layer 2 access distributed provider edge for Ethernet Wire Services and Ethernet Wire Services
Auto-allocation of VLAN	<ul style="list-style-type: none"> • When a Layer 2 access domain is attached to a provider edge, Cisco IP Solution Center can Auto-allocate a VLAN from the VLAN ID pool that is tied to the provider edge access domain
Auto-allocation of Virtual Circuit Identifier	<ul style="list-style-type: none"> • Cisco IP Solution Center offers the capability of Auto-allocating the virtual circuit ID for all of the pseudowires in the MPLS core (Martini draft pseudowire)



Using Cisco IP Solution Center L2VPN for a Large EoMPLS Deployment: Case Study
A customer (Customer A) wants the engineering, finance, and marketing departments at two sites (Site A and Site B) to be able to communicate (Figure 6).

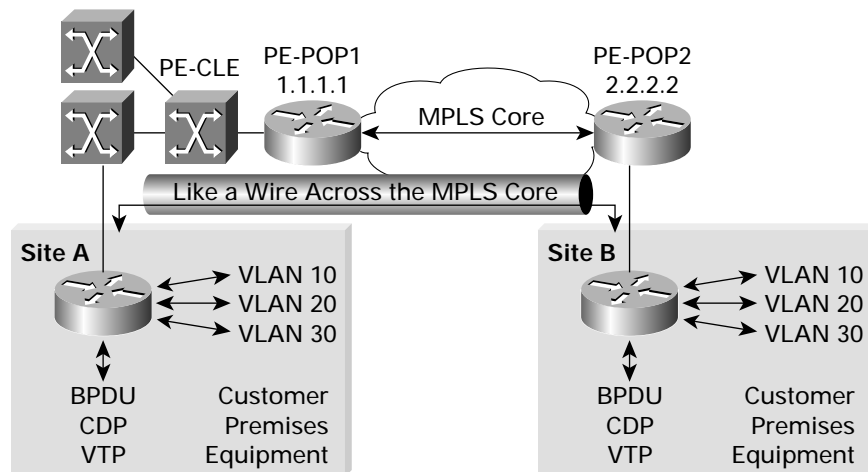
Figure 6
Existing Customer A Network Configuration



Customer A contacts service provider ABC's customer service department and is told that the service they are requesting can be provided with an Ethernet Wire Service.

With Ethernet Wire Service, the endpoints of the network look and behave as though they were on the same Ethernet wire. All traffic, including Bridge Protocol Data Units (BPDUs), is tunneled. Exceptions include IEEE 802.1x, IEEE 802.2ad, and IEEE 802.3x frames, which can be argued to have local significance only. Ethernet Wire Service is similar to having a wire from site to site.

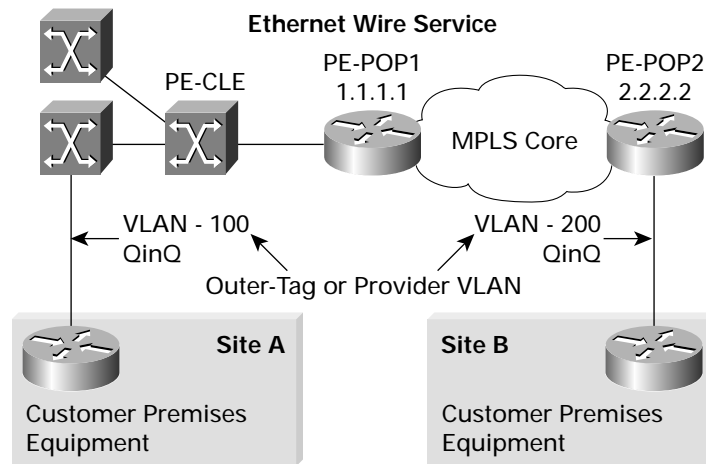
Figure 7
Ethernet Wire Service for Customer A





Ethernet Wire Service can be offered to a customer in a single provider edge or distributed fashion. The allocated VLAN for the customer is used for the tag stacking or QinQ the customer-facing user network interface (UNI) port. All customer traffic is tagged with an 802.1q outer-tag (also called a provider VLAN or P-VLAN), so that the provider edge point of presence (POP) Ethernet Wire Service is similar to having a wire from site to site.

Figure 8
All Customer Traffic is Tagged with a Provider VLAN



Cisco IP Solution Center manages the complete deployment of an Ethernet Wire Service, providing a point-to-point wire across access domains and the MPLS core.

Defining the Services That Service Provider ABC Wants to Offer

Cisco IP Solution Center enables service provider ABC to define all of the service-related parameters of the service deployment using the Cisco IP Solution Center Service Policy Manager. ABC decides to offer the following L2VPN services:

- Ethernet Wire Service
- Ethernet Wire Service
- Frame Relay over MPLS
- ATM over MPLS

Following are the parameters that have been entered in the Cisco IP Solution Center L2VPN Policy Manager, defining the Ethernet Wire Service to be offered to Customer A:

- Service type: Ethernet Wire Service
- Customer edge is present, as ABC offers a managed CPE option
- VLAN Auto-allocation

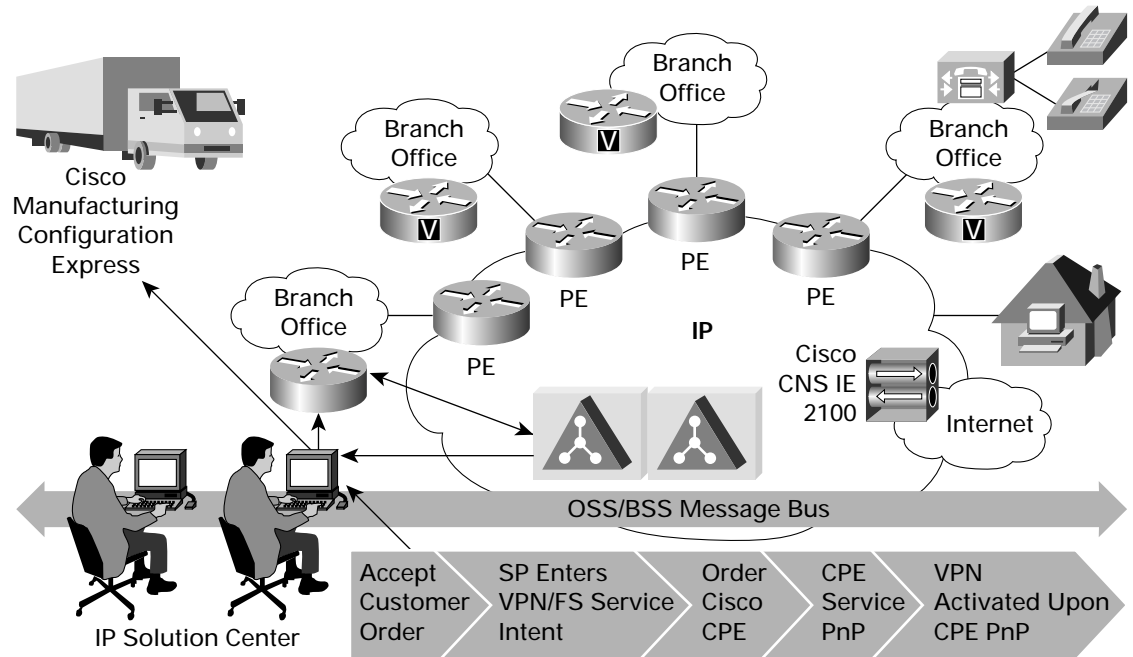
By defining the service policies, ABC's service operators who are going to deploy the services will not have to perform all of the steps to activate the service. Service policies represent the service that the service provider wants to offer its customers.



Rapid Deployment of CPE

Service provider ABC wants to deploy routers as CPE and offer EoMPLS services to its corporate customers (Figure 9).

Figure 9
Cisco IP Solution Center Enables Rapid Deployment of CPE



The deployment process includes the following steps:

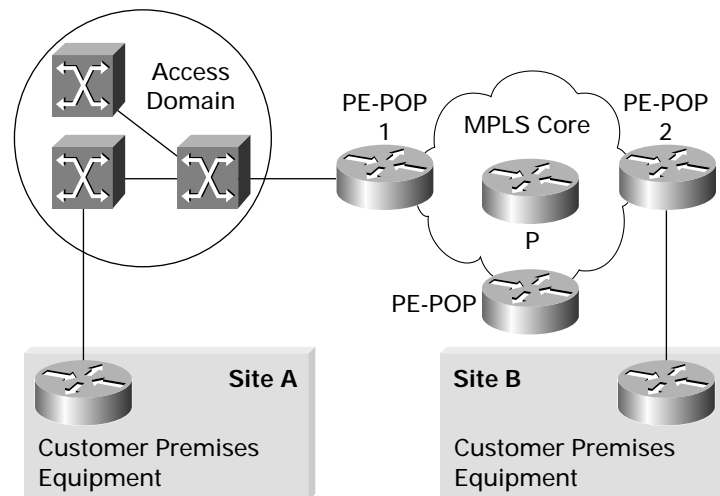
- CPE is shipped out of the Cisco manufacturing facility with minimal configuration in the network element, which is needed for the CPE to become active in the network
- The customer receives the CPE and plugs it into the service provider's Ethernet uplink
- The CPE is powered up and contacts the network appliance that is programmed in the configuration
- The Cisco CNS 2100 Series 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 L2VPN Service for Customer A

Customer A wants to enable two-way traffic between sites A and B (Figure 10).

Figure 10
Deploying L2VPN Service for Customer A



Following are the steps required to turn up service for Customer A:

1. The service operator receives an order form with the two sites to be connected. The order form also contains the network elements that are closest to sites A and B.
2. The service operator selects the L2VPN service policy defined for this customer.
3. The service operator selects site A CPE and site B CPE, which are customer edges.
4. The service operator activates the service.
5. Cisco IP Solution Center allocates a VLAN for site A, as site A is connected via Layer 2 access switches. This VLAN is added and allowed to pass all the intermediate switches up to the provider edge routers.
6. Cisco IP Solution Center collects just-in-time configuration from all the network elements that are involved in the service.
7. Based on the current switch/router configuration, Cisco IP Solution Center generates the IOS CLI Configlets needed to activate the service request.
8. Cisco IP Solution Center applies the generated IOS CLI Configlets to all of the devices participating in the service.
9. The applied configurations will configure the customer-facing port on the last switch to QinQ mode, and the allocated VLAN will be assigned for this customer traffic.
10. All customer traffic will be brought up to the provider edge routers.
11. A Layer 2 pseudowire will be created to provide an end-to-end connection.
12. Cisco IP Solution Center uploads the configuration to verify that the downloaded configuration is actually present in the network elements. This is the configuration audit phase.
13. The customer now has the equivalent of a wire from site A to site B (Figure 11).

Cisco IP Solution Center simplifies management of complex multiaccess, multiplatform IP services and reduces management costs. Cisco IP Solution Center service options provide service-level provisioning, service-aware performance and 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 IP Solution Center 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 IP Solution Center enables rapid and accurate deployment of security services. The Cisco IP Solution Center L2VPN Services Module provides full support for the provisioning and management of L2VPN services, MPLS VPN, remote-access VPN, Layer 2 access into MPLS, and various access technologies for provider edge to customer edge interfaces such as ATM, Frame Relay, serial, VLAN, and Ethernet. Cisco IP Solution Center hides the complexity of provisioning L2VPN 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](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

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