Cisco IP Solution Center 6.0

Cisco IP Solution Center Overview

Q. What is Cisco® IP Solution Center (ISC)?

A. Cisco IP Solution Center is a family of intelligent network management applications that can manage Multiprotocol Label Switching (MPLS) and Carrier Ethernet networks. The applications can operate as a suite or as standalone products; they provide planning, provisioning, automated diagnostics,[1] and traffic engineering for Layer 3 and Layer 2 VPNs, Any Transport over MPLS (AToM), and Carrier Ethernet services. Cisco IP Solution Center includes the following applications:

- Cisco IP Solution Center MPLS VPN Management
- Cisco IP Solution Center L2 VPN and Carrier Ethernet Management
- Cisco IP Solution Center Traffic Engineering Management (TEM)
- Cisco IP Solution Center MPLS Diagnostics Expert

Q. What is new in Cisco IP Solution Center 6.0?

A. The following new features and updates are available in Cisco IP Solution Center 6.0. A complete list of feature updates is available in the Cisco IP Solution Center 6.0 Release Notes. A complete list of platform and Cisco IOS® Software releases is available in the Cisco IP Solution Center 6.0 Installation Guide.

- Full support of the ASR 9000, now extended to cover Carrier Ethernet features
- 6VPE support, extended to cover Cisco IOS platforms
- FlexUNI/EVC ATM-Ethernet Interworking
- Support for Ethernet access networks, giving access to dual MPLS provider edge routers, and creation of Layer 2 services, such as pseudowires with pseudowire redundancy, or VPLS, which benefit from fast restoration in case of a failure on the provider edge router

Q. What are the major features and benefits of Cisco IP Solution Center?

A. Cisco IP Solution Center management applications help reduce overall administration and management costs by providing automated resource management and rapid profile-based provisioning capabilities that help enable fast deployment and time to market of MPLS and Carrier Ethernet technologies. Cisco IP Solution Center also helps reduce network operational costs by providing automated, workflow-based troubleshooting and diagnostic capabilities for MPLS VPNs. Cisco IP Solution Center provides a flexible application set for managing MPLS technologies in service provider and customer networks.

Cisco IP Solution Center offers an intuitive web-based GUI and open APIs to help enable integration of IP services operations into existing service provider operations support systems (OSSs). Open APIs and OSS interfaces help service providers to easily integrate IP VPN services into their OSS and management infrastructure. Cisco IP Solution Center has also been integrated with Cisco Info Center for VPN-aware fault correlation.

See a complete list of features and benefits in the Cisco IP Solution Center overview data sheet at http://www.cisco.com/go/isc.

[1] Automated diagnostics features are not available in Cisco IP Solution Center today for Layer 2 and Carrier Ethernet VPNs.

Q. What are the minimum recommended system requirements for a production environment?

A. For Cisco IP Solution Center 6.0, the recommended platforms are listed in the Cisco IP Solution Center 6.0 Installation Guide under the System Recommendations section. Please use these recommendations whether you are conducting a product trial, test environment setup, or production setup. The Cisco IP Solution Center 6.0 Installation Guide is available at http://cco/en/US/products/sw/netmgtsw/ps4748/prod_installation_guides_list.html.

Q. What type of database is shipped with Cisco IP Solution Center 6.0?

A. Cisco IP Solution Center 6.0 ships with Sybase (Sybase ASA, 11) embedded. Note that Cisco IP Solution Center can also work with an external Oracle database.

Q. What version of Oracle is supported by Cisco IP Solution Center 6.0?

A. Cisco IP Solution Center 6.0 testing has been performed on Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - 64 bit Production. If you would like to use another version of Oracle, see Oracle's compatibility information.

Q. What features are available in Cisco IP Solution Center APIs?

A. Cisco IP Solution Center APIs allow you to use OSS client programs to connect to the Cisco IP Solution Center system. The APIs provide a mechanism for inserting, retrieving, updating, and removing data from Cisco IP Solution Center servers using an XML interface request/response system.

The Cisco IP Solution Center APIs optionally use Secure HTTP (HTTPS) for message encryption and Cisco role-based access control (RBAC) for user authentication. The APIs use an HTTP/HTTPS/Simple Object Access Protocol (SOAP) interface. API requests are executed using a combination of HTTP/HTTPS and SOAP by sending the XML data to the API server. The server returns an XML response, which is also an encoded SOAP message, to indicate if the request is successful or to return data.

Cisco IP Solution Center Demonstration Software, Training, Pricing, and User Documentation

Q. How can I obtain a demonstration copy and a demonstration license of Cisco IP Solution Center?

A. Contact your local Cisco sales representative or contact the Cisco IP Solution Center marketing team at isc-mktg@cisco.com.

Q. If I am a current Cisco IP Solution Center 4.x or 5.x customer with Cisco Software Application Support (SAS), how can I obtain a no-charge Cisco IP Solution Center 6.0 update kit?

A. Cisco IP Solution Center 4.x or 5.x to 6.0 is a major upgrade and as such is not covered under SAS; please contact your local Cisco sales representative for upgrade purchase details.

Q. Are there any training classes available for the operation and deployment of Cisco IP Solution Center?

A. Yes. Please contact your local account representative or the Cisco IP Solution Center Marketing team (isc-mktg@cisco) for more details.

Q. Where is the user documentation for Cisco IP Solution Center 6.0 located?

A. User documentation is available at http://www.cisco.com/go/isc/.

Q. Where can I find the list of platforms, Cisco IOS Software and Cisco IOS XR Software releases, and Cisco Catalyst® OS releases supported by Cisco IP Solution Center?

A. Product specifications for each of the management applications are found in the respective applications' data sheets at Cisco.com and in greater detail in the Cisco IP Solution Center Installation Guide, also at Cisco.com.

Q. Where can I find the Cisco IP Solution Center 6.0 overview data sheet?

A. The Cisco IP Solution Center 6.0 data sheet is available at http://www.cisco.com/go/isc.

MPLS VPN Management

Q. Where can I find additional details on the technical features that the Cisco IP Solution Center MPLS VPN Management application offers?

A. The Cisco IP Solution Center Release Notes provide a summary of all the new features and updates. You can also check the Cisco IP Solution Center MPLS VPN Management data sheet for details. They are both available at http://www.cisco.com/go/isc.

Q. What types of provider edge-to-customer edge routing protocols does Cisco IP Solution Center MPLS VPN Management support?

A. Cisco IP Solution Center MPLS VPN Management currently supports Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), static routing, and Border Gateway Protocol (BGP).

Q. Does IP Solution Center support IPv6?

A. Yes, IP Solution Center supports the creation of 6VPE MPLS VPN networks; these create an IPv6 VPN, over an IPv4 core. It is possible to add IPv6 to an existing VPN, creating a dual-stack VPN, or just to create independent IPv6 VPNs. The provider edge-to-customer edge routing and the topology created by the route targets of a dual-stack VPN can be specified independently for IPv6 and IPv4.

Q. Does IP Solution Center support dual-homed customer edges?

A. Yes, it does. IP Solution Center has support for the BGP Site of Origin feature to prevent routing loops, can use a unique route distinguisher allocation, and can control the maximum number of routes stored to any prefix within the VPN, providing control of load balancing.

Q. How are resources allocated in the Cisco IP Solution Center MPLS VPN Management environment?

A. The Cisco IP Solution Center Automatic Resource Assignment feature relieves the service operator from manually entering certain parameters (such as IP addresses, VLAN, route distinguisher, and route target) during service activation. Cisco IP Solution Center keeps track of all of the resources allocated and knows to which service, customer, or site these resources were allocated.

Q. Does Cisco IP Solution Center MPLS VPN Management support Ethernet access networks?

A. Yes. It supports Layer 2 access domain into MPLS VPN. Layer 2 access domain can be in an aggregation or ring topology. Cisco IP Solution Center MPLS VPN Management smoothly allocates VLANs for customers and maps the VLAN to an MPLS VPN at the provider edge.

Q. Does the Cisco IP Solution Center MPLS VPN Management application support MPLS VPN Carrier Supporting Carrier (CSC)?

A. Yes, the application supports the CSC deployment scenario using Label Distribution Protocol/Interior Gateway Protocol (LDP/IGP) and BGP/MPLS.

Q. Does Cisco IP Solution Center MPLS VPN Management support multicast for MPLS/BGP VPNs?

A. The application provisions multicast support for MPLS/BGP IPv4 and IPv6 VPNs, resulting in customer multicast traffic being carried in the provider core with the help of multicast tunnels created in the provider core. To use this feature, the provider core network must be multicast-enabled.

Q. Does Cisco IP Solution Center MPLS VPN Management support Virtual Route Forwarding Lite (VRF Lite)?

A. Yes, it supports VRF Lite and Multi-VRF at the customer-edge device. A single service request provisions a multi-VRF customer edge.

Q. How does Cisco IP Solution Center MPLS Diagnostics Expert work with the Cisco IP Solution Center MPLS VPN Management application?

A. Cisco IP Solution Center MPLS Diagnostics Expert is a software application for troubleshooting and diagnosing connectivity problems in IP/MPLS VPNs. It works with the Cisco IP Solution Center family of applications. It can be used on its own or together with Cisco IP Solution Center MPLS VPN Management.

Cisco IP Solution Center MPLS Diagnostics Expert can be used in conjunction with the VPN provisioning capabilities of the Cisco IP Solution Center MPLS VPN Management application and will use the customer and VPN data provided by Cisco IP Solution Center as a starting point for troubleshooting, in order to locate the endpoints (customer-edge devices) between which reachability is tested. In addition to troubleshooting, Cisco IP Solution Center MPLS Diagnostics Expert can also be used in conjunction with the Cisco IP Solution Center MPLS VPN Management application for VPN postprovisioning checks. After deploying a VPN using the Cisco IP Solution Center MPLS VPN Management provisioning features, a reachability test can be run to verify that the VPN has been provisioned successfully.

Q. Where can I get more information about Cisco IP Solution Center MPLS Diagnostics Expert?

A. For detailed information, please visit the Cisco IP Solution Center MPLS Diagnostics Expert product page at http://www.cisco.com/go/mde.

L2VPN and Carrier Ethernet Management

Q. What types of Carrier Ethernet services does Cisco IP Solution Center support?

A. Cisco IP Solution Center can provision point-to-point and multipoint-to-multipoint services. The access ports can be physical ports, carrying all tagged or untagged traffic into the service, or they can be virtual, in which case the services are identified by VLAN tags, and multiple services can exist on the same port.

The services are implemented using a choice of VPLS, pseudowires with or without bridge domains and pseudowire redundancy, as well as local interconnects.

ISC can also provision the Ethernet access network, including QinQ, and flexible matching and translating of VLAN tags. It can also provision the security attributes of the interface towards the customer on an Ethernet access switch.

Q. What type of AToM provisioning does the Cisco IP Solution Center L2 VPN Management application support?

A. The following AToM services are supported:

- ATM over MPLS (ATMoMPLS)
- ATM to Ethernet Layer 2 interworking
- Frame Relay over MPLS (FRoMPLS)

Q. Can Cisco IP Solution Center manage the provisioning of multiple Layer 2 VLAN circuits and Layer 3 MPLS VPN circuits such that they can be achieved through a single service request for a particular customer?

A. Yes. A single service request can be used to provision and activate multiple Layer 2 VLAN circuits or multiple MPLS VPN circuits.

Q. Does Cisco IP Solution Center support full-mesh, hub-and-spoke, and partial-mesh Layer 2 VPN topologies?

A. Yes. Cisco IP Solution Center supports configuration generation for routers and switches in full-mesh, hub-and-spoke, or partial-mesh Layer 2 VPN topologies.

Q. What type of deployment assurance does Cisco IP Solution Center provide for service operators?

A. Cisco IP Solution Center helps ensure that, for each deployed Layer 2 VPN service, the router's configuration is correct and the routing between the customer edges is what the service operator requested through the configuration audit.

Q. How can policy-based provisioning benefit activation efficiency?

A. All of the service-offering-related parameters can be included in a Layer 2 VPN service policy. When a service operator uses this predefined policy, the complexities of service activation are hidden from the operator.

Q. What types of access architectures do the Cisco IP Solution Center Carrier Ethernet features support?

A. Topologies currently supported are hub-and-spoke, hub-and-spoke with Network Interface Device (NID), Ethernet access rings connected to a single MPLS provider-edge router, and dual-homed segments connecting to two MPLS provider-edge routers. Topologies can be created as combinations of these elements.

Q. Does Cisco IP Solution Center facilitate flow-through provisioning of Carrier Ethernet for Layer 2 and a core network for Layer 3?

A. For Carrier Ethernet access, Cisco IP Solution Center provisions the Layer 2 switches by allocating VLANs and provisioning the provider edge (subinterface). Cisco IP Solution Center does this during the provisioning of Layer 2 VPN/Layer 3 MPLS VPN services.

Quality of Service

Q. What type of quality of service (QoS) can Cisco IP Solution Center configure?

A. To provision QoS with Cisco IP Solution Center, templates should be used. Templates can accommodate the many differences in platforms and applications that may be encountered. Templates in ISC are attached to services or service polices, so the service lifecycle can be used to make sure the template is applied and removed as required. It is recommended that customers engage the Cisco Advanced Services group if assistance is required in developing templates for individual applications.

Traffic Engineering Management

General Questions

Q. What are the primary features offered by the Cisco IP Solution Center Traffic Engineering Management application?

A. The application simplifies visualization, configuration, and management of MPLS traffic engineering tunnels on a network. It integrates the configuration of Cisco MPLS traffic engineering features (Autoroute Announce, Auto-Bandwidth, DiffServ-Aware Traffic Engineering, and Fast Reroute [FRR]) into a single management tool. It also uniquely provides the ability to compute and configure primary tunnels to meet user-specified constraints and to compute FRR bypass tunnels for network element protection (node, links, or Shared Risk Link Groups [SRLGs]), helping to ensure bandwidth availability during normal and element failure conditions.

Q. Can Cisco IP Solution Center Traffic Engineering Management support secure router communications such as Secure Shell (SSH) Protocol?

A. Cisco IP Solution Center Traffic Engineering Management uses either SSH or Telnet to communicate with the routers. This is configurable by the user.

Q. Can IP Solution Center Traffic Engineering Management work in a multivendor environment?

A. Yes. The application has been enhanced to support multivendor environments. It can configure and plan MPLS traffic engineering tunnels in Cisco devices that reside in a multivendor environment. The functionality includes:

- Discovering and displaying third-party devices in the network
- Providing full network visibility, with tunnels overlaid on topology that includes third-party devices

- Routing tunnels optimally through third-party devices with the paths fully visualized in the network topology viewer

MPLS Traffic Engineering

Q. What is Multiprotocol Label Switching traffic engineering?

A. Traffic engineering is the ability to route traffic away from the Shortest Path First (SPF) path in order to use a network according to an operator's policies and to help guarantee service-level requirements such as bandwidth and latency. Traffic engineering is not specific to MPLS, but MPLS provides one of the most powerful and detailed ways to support traffic engineering. IGP metric manipulation has also been used for some level of traffic engineering.

A good reference is Eric Osborne's and Ajay Simha's Cisco Press book *Traffic Engineering with MPLS*, ISBN 1-58705-031-5.

Q. Why use MPLS traffic engineering?

A. In a converged network carrying high-QoS services, MPLS traffic engineering can be used to deliver bandwidth and latency guarantees to the relevant traffic. It also provides a way of protecting bandwidth reserved for high-QoS traffic, thereby providing guarantees in normal and failure conditions. MPLS traffic engineering can be effectively applied to optimization of network utilization. Results show that this can deliver major cost savings over alternative approaches. It has also been suggested as a way to determine the end-to-end traffic matrix, by collecting counters at tunnel headend devices.

Q. What is the difference between online and offline path calculation?

A. Online refers to the routers in the network calculating paths for tunnels using Constraint Shortest Path First (CSPF). Offline represents a centralized server doing the path calculation. Cisco IP Solution Center Traffic Engineering Management is an example of offline traffic engineering calculations being done for primary paths and for paths for bypass tunnels. Regardless of where the calculation is done, the signaling on the network is the same, Resource Reservation Protocol (RSVP)-Traffic Engineering reserves bandwidth down the calculated path, and then the router puts traffic on the tunnel.

Fast Reroute

Q. How does MPLS Fast Reroute work?

A. FRR is a facility within MPLS to provide network protection with switching times comparable to SONET/SDH Layer 1 protection. A set of backup tunnels is preinstalled on the network to protect against network element (link and node) failure. When one of these elements fails, the local router, the point of local repair (PLR), switches the primary traffic onto the backup tunnels. The backup tunnel reroutes the traffic around the failure and merges the traffic back into the original tunnels on the other side of the failure point, the merge point.

Q. What is the difference between FRR bypass and FRR detour tunnels?

A. Each detour tunnel protects a single primary tunnel. As an example, if two tunnels are going through a router, you will calculate two backup tunnels around that router, one for each primary tunnel. If you change the primary tunnels or add new ones, you will need to calculate a new layout of detour tunnels. There is no label stacking involved in detour tunnels, only label swapping. FRR bypass tunnels provide many-to-one backup; you need only one protection path for an element, and all primary tunnels follow that path. The technology used is MPLS label stacking; this is further described in the IETF draft, draft-ietf-mpls-rsvp-lsp-fastreroute-01.txt.

Bandwidth Protection

Q. What is bandwidth protection?

A. With FRR, it is possible to have defined "a priori" backup tunnels for local protection. In the case of the failure of a given element, all traffic on a given tunnel will be routed down a defined backup tunnel. This is known as

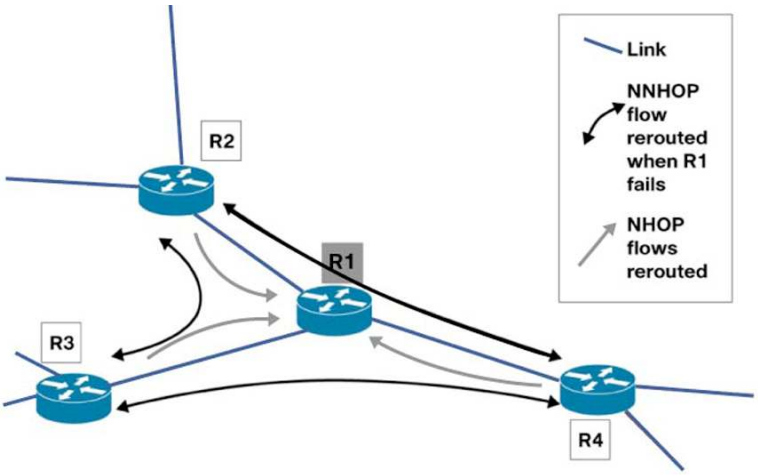
connectivity protection. Bandwidth protection adds to this the assurance that the backup tunnels have enough bandwidth on all links in the path so that when an element fails, there is no congestion. Bandwidth protection is the combination of connectivity protection and bandwidth accounting in failure cases.

Q. What traffic flows are rerouted when protecting against an element failure?

A. There can be a router, link, or SRLG failure. Following are scenarios related to each:

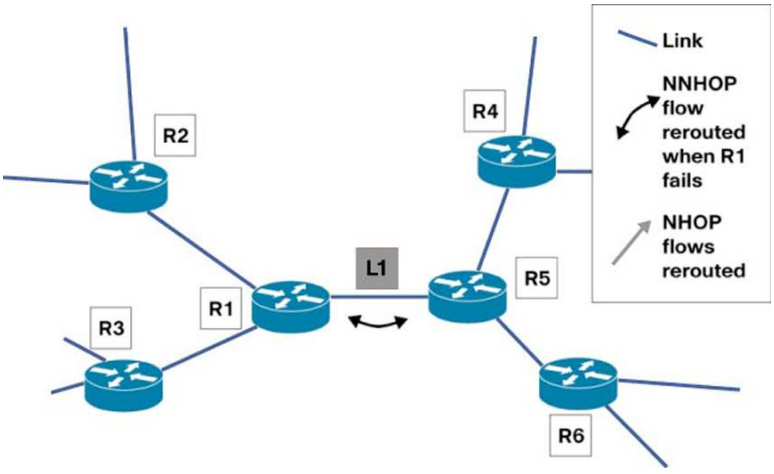
- **Router:** Figure 1 shows router R1 failing. The black and red arrows show the flows that need to be rerouted to successfully reroute all traffic. The goal is to protect the bandwidth between the pairs of adjacent routers around the node under test.
- If a router could be distinguished from a link failure in milliseconds, then the black flows would be the only flows that needed rerouting. However, distinguishing router from link failure in the order of milliseconds is not possible; when, for example, R2 loses connectivity to R1, it must have backup tunnels that protect next-next-hop (NNHOP) flows from R2 through router R1 and the next-hop (NHOP) flow from R2 through link R1<->R2. In the short timeframe, it is not possible to determine whether the cause of failure relates to the router or the link. Therefore, the flows represented by the red arrows must also be handled.

Figure 1. Flows Rerouted in a Router Failure Case



- **Link:** Figure 2 addresses link failure. The black arrows show the flows that need to be rerouted in the case of the failure of link R1<->R5.

Figure 2. Flows Rerouted in a Link Failure Case



In this scenario, the focus is on protecting against link failure. Because there is no need to worry about NNHOP flows, there are no red arrows.

- **Shared Risk Link Group:** This refers to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may fail too. Links in the group have a shared risk. In this case, all bypass tunnels must avoid all links in the SRLG, making this a more difficult problem to solve than single-link protection.

Q. What are side-effect tunnels?

A. Side-effect tunnels are tunnels triggered in a failure case that are not directly involved in the protection of an element. For example, in Figure 1, the backup tunnels protecting the black flows are directly associated with the protection of the router. Backup tunnels protecting the red flows are side-effect tunnels. Similarly, in a link-failure case, any NNHOP tunnels triggered by the failure are considered side-effect tunnels; for bandwidth protection, they must be accounted for in the path calculations.

Q. Sometimes Cisco IP Solution Center Traffic Engineering Management suggests deleting some FRR backup tunnels when protecting an element. Why?

A. Cisco IP Solution Center Traffic Engineering Management can sometimes find that backup tunnels are inconsistent and must be removed or rerouted. That is, they are inconsistent with the flows that may be directed down them in failure cases and do not provide the required bandwidth protection. Such tunnels can appear if they have been configured by hand or if there has been a change to bandwidth pool sizes. Note: Cisco IP Solution Center Traffic Engineering Management will attempt to use existing tunnels, where possible.

Q. How does Cisco IP Solution Center Traffic Engineering Management help ensure that the bandwidth is protected without reserving bandwidth for backup tunnels?

A. Cisco IP Solution Center Traffic Engineering Management is an offline tool that has its own local bandwidth accounting mechanism. When calculating backup tunnels to protect a given element, it helps ensure that the placement of these backup tunnels does not conflict with each other and that they remain within the specified available backup bandwidth on the links.

Because this is all accounted for in the tool, there is no need to reserve the bandwidth for backup tunnels. They are all signaled with zero bandwidth. Signaling backup tunnels with zero bandwidth allows the available bandwidth to be used for best-effort traffic when elements have not failed. It also allows the same bandwidth to be reused for different failure cases.

Q. How long does the bandwidth protection algorithm take to solve failures (that is, to generate required FRR bypass tunnels)?

A. Typically, the algorithm requires only a few seconds to solve a single failure case. For an entire network, this means that the time to solve is on the order of seconds to minutes, even for fairly large networks. Note: Load balancing has an effect on the speed of the algorithm; the space of possible solutions grows as the load balancing increases.

Q. How does Cisco IP Solution Center Traffic Engineering Management cope with delay when placing backup tunnels?

A. For each traffic engineering-enabled interface in the network, there are two parameters (in the Cisco IP Solution Center Traffic Engineering Management database) associated to delay, propagation delay, and maximum delay increase. When the routing algorithm calculates an FRR bypass tunnel for a link, it determines the paths such that the sum of the propagation delay of the link and the maximum delay increase is less than the sum of the propagation delays of the links used by the bypass tunnels.

Primary Tunnel Placement

Q. How does Cisco IP Solution Center Traffic Engineering Management take into account CSPF tunnels?

A. Cisco IP Solution Center Traffic Engineering Management allows you to discover, create, and view primary tunnels, supporting CSPF and explicitly routed tunnels.

Q. How is delay supported when placing primary tunnels?

A. Each interface in Cisco IP Solution Center Traffic Engineering Management has an associate delay field representing the propagation delay typically experienced by traffic traversing this link. Each tunnel has an associated service policy. In the service policy there is a maximum delay parameter specifying the maximum one-way delay acceptable for a given service across a tunnel. The path calculated for a tunnel must not exceed the maximum delay parameters.

Q. How do traffic engineering tunnels relate to MPLS Layer 3 VPNs?

A. There are two ways that Cisco IP Solution Center Traffic Engineering Management currently supports placing Layer 3 VPN traffic onto traffic engineering tunnels. The first is Autoroute Announce. The tunnels are locally announced to IGP routing. A packet arriving on a router destined for the tail of a tunnel starting at that router will go directly into that tunnel. Thus, an autoroute announced tunnel from provider edge to provider edge will carry all Layer 3 VPN traffic between those provider edge devices. The other method of “traffic admission” onto tunnels is static routing. Here, all traffic destined for a particular router can be directed onto a given tunnel.

Q. What about Layer 2 VPNs, Pseudowire 3, and others?

A. Traditional Layer 2 VPN services, such as ATM, Frame Relay, and time-division multiplexing (TDM), and Carrier Ethernet services, such as VPLS, are carried across an MPLS core using pseudowires, provider edge-to-provider edge connections that encapsulate these different types of traffic. This Layer 2 traffic can be admitted to tunnels by associating pseudowires and traffic engineering tunnels. Many pseudowires can be assigned to a single traffic engineering tunnel. Traffic engineering is a critical component in guaranteeing the level of service for such traffic. In the Cisco IP Solution Center Traffic Engineering Management application, you can now select a specific traffic engineering tunnel you want to use for point-to-point transport on Layer 2 Any Transport over MPLS.

Cisco IP Solution Center MPLS Diagnostics Expert

For information about Cisco IP Solution Center MPLS Diagnostics Expert, please see the separate Q&A at http://www.cisco.com/go/mde.

For More Information

For more information about Cisco IP Solution Center, visit http://www.cisco.com/go/isc, contact your local account representative, or send an email to the product marketing group at isc-mktg@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C67-620145-00 09/10