

Cisco IP Solution Center 4.2

Cisco IP Solution Center overview

Q. What is Cisco® IP Solution Center?

A. Cisco IP Solution Center is a family of intelligent network management applications that can manage Multiprotocol Label Switching (MPLS) and Metro Ethernet networks. The applications can operate as a suite or as standalone products; they provide planning, provisioning, automated diagnostics¹, and traffic engineering for Layer 3 and Layer 2 VPNs, Any Transport over MPLS (AToM), Layer 2 Tunneling Protocol Version 3 (L2TPv3), and Metro Ethernet services. Cisco IP Solution Center includes the following applications:

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

Q. What is new in Cisco IP Solution Center 4.2?

A. The following new features and updates are available in Cisco IP Solution Center 4.2. A complete list of feature updates is available in the Cisco IP Solution Center 4.2 Release Notes. A complete list of platform and Cisco IOS® Software releases is available in the Cisco IP Solution Center 4.2 Installation Guide.

- Cisco MPLS Diagnostics Expert 2.0 provides a new set of automated diagnostics and troubleshooting capabilities of MPLS/BGP VPNs (edge, access, and core). It can be used on its own, or together with Cisco IP Solution Center MPLS VPN Management. For more information check the Cisco MPLS Diagnostics Expert 2.0 product bulletin at <http://www.cisco.com/go/mde>.
- Cisco IP Solution Center 4.2 is based on Release 4.1 with the addition of new and changed features and updates that were introduced in Releases 4.1.1, 4.1.2, and problems fixed since Release 4.1. A complete list of updates is available in the Cisco IP Solution Center 4.2 Release Notes.

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 enable fast deployment and time to market of MPLS and Metro 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 also offers a scalable and reliable architecture for large-scale operations by providing a four-tiered system, Web GUI, and open APIs to enable integration of

¹ Automated Diagnostics features are not available in Cisco IP Solution Center today for Layer 2 and Metro Ethernet VPNs.

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. Performance management applications that are integrated with Cisco IP Solution Center are available from independent software vendors (ISVs) Concord and Infovista.

See a complete list of features and benefits in the Cisco IP Solution Center Overview Data sheet at www.cisco.com/go/isc.

Q. What are the main differences between Cisco VPN Solution Center and Cisco IP Solution Center?

- A.** Cisco IP Solution Center is a family of intelligent network management applications for managing MPLS and Metro Ethernet networks. It is built on the Cisco VPN Solution Center infrastructure. The Cisco VPN Solution Center only supports MPLS VPN and IP Security (IPSec) technology. Cisco IP Solution Center supports the following technologies:
- Layer 3 VPN (including automated troubleshooting and diagnostics)
 - AToM and Metro Ethernet
 - Layer 2 Tunneled VPNs
 - MPLS Traffic Engineering
- A.** In addition to the set of supported technologies, other main differences are Cisco IP Solution Center's infrastructure features, including a four-tiered architecture, off-the-shelf Relational Database Management Systems (RDBMSs) such as Sybase and Oracle, a Web-based GUI, an XML-over-HTTP northbound API, and Role Based Access Control (RBAC). Cisco VPN Solution Center customers that upgrade to Cisco IP Solution Center can make use of additional network management applications such as Cisco IP Solution Center L2 VPN and Metro Ethernet Management application, Traffic Engineering Management, and the new Cisco MPLS Diagnostics Expert. The Cisco MPLS Diagnostics Expert provides automatic diagnostics of MPLS VPN connectivity problems.

The Cisco VPN Solution Center end of life and end of sale was announced in April 2003. Cisco VPN Solution Center customers are encouraged to migrate to Cisco IP Solution Center 4.2. The end of software maintenance for Cisco VPN Solution Center products began on August 1, 2005. For additional details on the end-of-sale and end-of-life program for Cisco VPN Solution Center 1.x and 2.x, please visit:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps2327/prod_eol_notices_list.html

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

- A.** For Cisco IP Solution Center 4.2, the recommended platforms are listed in the Cisco IP Solution Center 4.2 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 4.2 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 4.2?

A. Cisco IP Solution Center 4.2 comes embedded with Sybase (Sybase ASA, 8.0.1). 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 4.2?

A. Cisco IP Solution Center 4.1 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 is the preferred Web browser client for the Cisco IP Solution Center Web GUI?

A. Internet Explorer 6.0 and Netscape 7.0 are supported.

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 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 Demo software, Training, Pricing, and user documentation**Q. How can I obtain a demo copy and demo 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 4.0 or 4.1 customer with Cisco Software Application Support (SAS), how can I obtain a no-charge Cisco IP Solution Center 4.2 update kit?

A. Cisco IP Solution Center 4.0 and 4.1 customers with Cisco SAS contracts can request the minor update kits from the Cisco Product Upgrade Tool at <http://www.cisco.com/upgrade>. For additional ordering details, please refer to the Cisco IP Solution Center 4.2 Product Bulletin at: http://www.cisco.com/en/US/products/sw/netmgts/ps4748/prod_bulletins_list.html

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.com) for more details. Cisco currently has several qualified training partners:

- Harbrook Consultants, based in the United Kingdom. Target theaters: Americas and Europe: <http://www.harbrook.net/>
- Fastwire, based in Australia. Target theaters: Asia Pacific and the Middle East: <http://www.fastwire.com.au/>

- Technology Development Center (TDC), based in the United States. Target theaters: Americas: <http://www.tdcinc.net/index.html>
- Cisco Customer Advocacy Global OSS/NMS Practice provides deployment services for Cisco IP Solution Center. Target theaters: Americas, EMEA, and Asia Pacific. Contact your local account representative for more information; have them send e-mail to isc-rapidresults@cisco.com.

Q. Where is the user documentation for Cisco IP Solution Center 4.2 located?

- A.** User documentation is available at Cisco.com:
<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/index.htm>.

Q. Where can I find the list of platforms, Cisco IOS 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 application's 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 4.2 overview data sheet?

- A.** The Cisco IP Solution Center 4.2 data sheet is available at Cisco.com:
<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 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 Initiation Protocol (RIP), static routing, and Border Gateway Protocol (BGP).

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

- A.** Cisco IP Solution Center's 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 tracks of all of the resources allocated and knows which service, customer, or site to which these resources were allocated.

Q. Does Cisco IP Solution Center MPLS VPN Management support Ethernet switch service distribution?

- 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 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 the Cisco MPLS Diagnostics Expert work with the Cisco IP Solution Center MPLS VPN Management application?

A. Cisco 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.

The Cisco 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 MPLS Diagnostics Expert can also be used in conjunction with the Cisco IP Solution Center MPLS VPN Management application for VPN post-provisioning checks. After deploying a VPN using 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 the Cisco MPLS Diagnostics Expert?

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

Layer 2 Vpn Management

Q. What type of Layer 2 provisioning does the Cisco IP Solution Center L2 VPN Management application support?

A. Layer 2 service provisioning for Cisco IP Solution Center consists of the Layer 2 VPN service, the L2TPv3 service, and the Virtual Private LAN Service (VPLS). Layer 2 VPN services are point-to-point and include Ethernet, Frame Relay, and ATM services. L2TPv3 services provide Layer 2 point-to-point connectivity over a pure IP (non-MPLS) infrastructure. VPLS services are multipoint and include Ethernet services over an MPLS core or an Ethernet core.

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)
- Frame Relay over MPLS (FRoMPLS)

Point-to-Point Ethernet Wire Service (EWS) and Point-to-Point Ethernet Relay Service (ERS) are delivered with the Cisco Metro Ethernet offering. See the Metro Ethernet Q&A section below.

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 and 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.

Metro Ethernet Services

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

A. In the Metro Ethernet arena, Cisco IP Solution Center supports the following services:

- Ethernet Wire Service (EWS)
- Ethernet Relay Service (ERS)—802.1q between service provider and customer
- Ethernet access into MPLS VPN
- Multipoint to Multipoint (MP2MP) service with switching core
- VPLS support for Cisco 7600 Series Routers (802.1Q-in-802.1Q [QinQ] and dot1Q encapsulation)

Q. What types of access architectures are supported by Cisco IP Solution Center Metro Ethernet features?

A. Topologies currently supported are hub-and-spoke, hub-and-spoke with Network Interface Device (NID), and Gigabit Ethernet Access Ring.

Q. Is Cisco IP Solution Center compliant with the Cisco Metro Ethernet Solution 3.1?

A. Cisco IP Solution Center is compliant with the Cisco Metro Ethernet Solution 3.1, except for Metro Optical support and interworking. Additional feature support for services, QoS, and platforms has been added in the Cisco IP Solution Center L2 VPN and Metro Ethernet Management application in order to support the Cisco Metro Ethernet Solution 3.1. Some of the newly supported features are: one-to-one or two-to-one VLAN translation, storm control settings, enhanced policy for virtual circuit ID (VC ID) attributes, UNI port security, and support

for the Cisco Catalyst 6500 Series Supervisor Engine 720, Catalyst 3750 Metro Series Switches, Cisco ME 3400 Series Ethernet Access Switches, and the Cisco ME 6524 Ethernet Switch. Check the Cisco IP Solution Center L2 VPN and Metro Ethernet Management data sheet for more details at www.cisco.com/go/isc.

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

A. For Metro Ethernet access, Cisco IP Solution Center provisions the Layer 2 switches by allocating VLANs and provisioning the provider edge (sub-interface). 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. Cisco IP Solution Center supports both IP QoS and Ethernet QoS. Cisco IP Solution Center configures QoS at the access circuit, which involves the access router (provider edge device) in the service provider network and the customer premises equipment (CPE) in the customer network. A QoS policy is applied to the selected set of access circuits using a QoS service request.

Q. What are the main QoS components that Cisco IP Solution Center can provision?

A. There are three primary configuration components to QoS—classification, scheduling, and resource management. In Cisco IP Solution Center, the QoS components used to achieve classification, scheduling, and resource management are:

- Traffic classification
- Marking
- Rate limiting
- Traffic shaping
- Congestion management
- Congestion avoidance
- Link efficiency

Q. Does Cisco IP Solution Center support deployment of traffic marking on the provider-facing interface of a CPE device instead of on the LAN-facing ports?

A. Cisco IP Solution Center currently supports traffic marking on either side of the CPE:

If there are LAN-facing interfaces specified for marking (in the device editor), marking is done there and not on the provider-edge-facing interface. Otherwise, marking is done on the provider-edge-facing interface.

Q. What management capabilities are available for QoS and class of service (CoS) monitoring and performance reporting?

A. Currently, Cisco IP Solution Center does not have this type of management capability. A partner application commonly used for QoS and CoS monitoring and performance reporting is Agilent FireHunter.

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 (MPLS-TE) tunnels on a network. It integrates the configuration of Cisco MPLS-TE features (Autoroute Announce, Auto-Bandwidth, DiffServ-Aware Traffic Engineering [DS-TE], 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 Link Risk Groups [SRLGs]), helping to ensure bandwidth availability during normal and element failure conditions.

Q. What releases of Cisco IOS Software does Cisco IP Solution Center Traffic Engineering Management support?

A. Cisco IP Solution Center Traffic Engineering Management has been tested with the following Cisco IOS Software Releases. Check the Cisco IP Solution Center 4.2 Installation Guide for additional details.

Table 1. Supported Cisco IOS Software Releases

Cisco IP Solution Center Traffic Engineering Management	Cisco 7200 Series Routers, in network core	Cisco IOS Software Release 12.0(32)S
	Cisco 7200 Series Routers, on network edge	Cisco IOS Software Release 12.2(28)SB
	Cisco 7500 Series Routers, in network core	Cisco IOS Software Release 12.0(27)S4
	Cisco 7600 Series Routers, in network core	Cisco IOS Software Release 12.2(18)SXF
	Cisco 10000 Series Routers (ESR), in network core	Cisco IOS Software Release 12.0(30)S3
	Cisco 10000 Series Routers (ESR), on network edge	Cisco IOS Software Release 12.2(28)SB
	Cisco 12000 Series Routers (GSR), in network core	Cisco IOS Software Release 12.0(32)S and Cisco IOS XR Software Release 3.2
	Cisco CRS-1 Carrier Routing Systems	Cisco IOS XR Software Release 3.2

Note that Cisco IOS Software Release 12.0(21)S does provide link protection, but to use the full capabilities of Cisco IP Solution Center Traffic Engineering Management, anything earlier than Release 12.0(22)S is not recommended.

Q. What platforms does Cisco IP Solution Center Traffic Engineering Management support?

A. It has been tested on Cisco 12000, 10000, 7600, 7500, and 7200 Series Routers, and Cisco CRS-1 Carrier Routing Systems.

Q. Does Cisco IP Solution Center Traffic Engineering Management need a dedicated machine?

A. There is no need for the server to be a dedicated machine. However, the speed to generate solutions will be directly affected if the processor is shared between several processes. If time is a critical factor, then the CPU should be clear for the traffic engineering process.

Q. Can I use a file or database to provide topology information rather than having to go directly to the network?

A. Yes. Cisco IP Solution Center Traffic Engineering Management uses files that contain topology information, tunnel information, SRLGs, and MPLS data. These files can be created from an MPLS-TE network by running the relevant **show** commands on the network. These

files can then be saved for offline investigation. The following **show** commands generate all of the relevant information:

- **show mpls traffic-engineering topology** (on a seed router)
- **show mpls traffic-engineering tunnels** (on each MPLS-TE-enabled router)
- **show mpls traffic-engineering tunnels backup** (on each MPLS-TE-enabled router)
- **show running-config** (on each MPLS-TE-enabled router)

Q. Can I feed this into a simulator such as WANDL or OpNet?

A. Currently, there is no way to feed data directly from Cisco IP Solution Center Traffic Engineering Management into WANDL or OpNet for simulation. However, the above files may be fed into OpNet SPGuru.

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-TE 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
- Tunnels can be optimally routed through third-party devices and the paths can be fully visualized in the network topology viewer

MPLS-TE

Q. What is Multiprotocol Label Switching Traffic Engineering (MPLS-TE)?

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.

Q. Why use MPLS-TE?

A. In a converged network carrying high-QoS services, MPLS-TE 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-TE 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 are some of the specifics to MPLS-TE operation?

A. Traffic engineering needs to have knowledge of the MPLS-TE topology and the resources currently being used. This topology is used to create MPLS-TE paths based on a set of constraints, the most well-known being bandwidth (finding a path of 20 Mbps through the

network, for example). This topology is flooded to every MPLS-TE-enabled router in an IGP area by making use of IGP updates (OSPF or Intermediate System-to-Intermediate System [ISIS]). As a result, only link-state IGPs can be used.

Q. What is the difference between online and offline?

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)-TE reserves bandwidth down the calculated path, and then the router puts traffic on the tunnel.

Q. Where can I read about MPLS-TE?

A. The best reference is Eric Osborne and Ajay Simha's Cisco Press book "Traffic Engineering with MPLS"; ISBN: 1-58705-031-5.

Fast Reroute

Q. How does MPLS Fast Reroute work?

A. Fast Reroute (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 only need 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.

Q. What is label stacking? Why is it important for FRR?

A. Backup paths are installed to route around a failure; they have a set of labels that are swapped along the path (MPLS). In a failure, the primary tunnels are routed onto the backup path. Rather than swap the primary path label for the backup path label, the primary label is left untouched and the backup label is pushed on top of the label stack. This top label is swapped along the backup path until it reaches the last router in the path, before rejoining the primary path. This router removes the top label and forwards the packet with the same primary label that it had at the PLR to the next router. This router (where the backup path terminates and the primary path continues) is the merge point; it sees the primary label and simply forwards on the primary packet on as if nothing had happened.

Q. What type of signaling is associated with FRR?

A. RSVP-TE signaling sets up and maintains the backup paths in exactly the same way as is done with the primary tunnels. During failure, the PLR sends a "PathErr" message to the different primary tunnels' headends, just as it would without FRR. The difference is that the

message now says that local protection is active, rather than stating that the tunnel is down. At the other end of the backup path, the merge point does nothing differently. There is subtle modification to the primary traffic RSVP-TE updates going down the backup tunnel, but the amount of signaling does not change. In terms of traffic engineering topology flooding, nothing changes.

Q. What is DiffServ-Aware Traffic Engineering (DS-TE)?

A. DS-TE extends traffic engineering to allow bandwidth allocation for different classes of traffic. Basic traffic engineering allows for a reservable bandwidth to be specified for traffic-engineered traffic on each link. DS-TE extends this to give reservable bandwidth pools for different classes of traffic. There are two current IETF drafts relating to DS-TE. One looks at distinct resource allocation for each pool. The other looks at the DS-TE bandwidth reservation constraints (also known as the "Russian Doll" bandwidth constraints model). The Russian Doll model is currently supported by Cisco IP Solution Center Traffic Engineering Management. In general, this model is best used when different tunnel priorities are going to be used, and the maximum allocation model is best when priorities are not being used.

It is important to note that DS-TE does not provide a link to DiffServ. When the available subpool bandwidth is specified on a link, it is up to the operator to ensure this corresponds to the queue sizes that will service traffic from tunnels using the subpool. The headend of the tunnel needs to be policed to ensure that no more than the specified bandwidth goes down the tunnel; finally, the MPLS Experimental (EXP) bits are used to ensure that the MPLS packets go onto the correct queue.

Bandwidth Protection

Q. What is bandwidth protection?

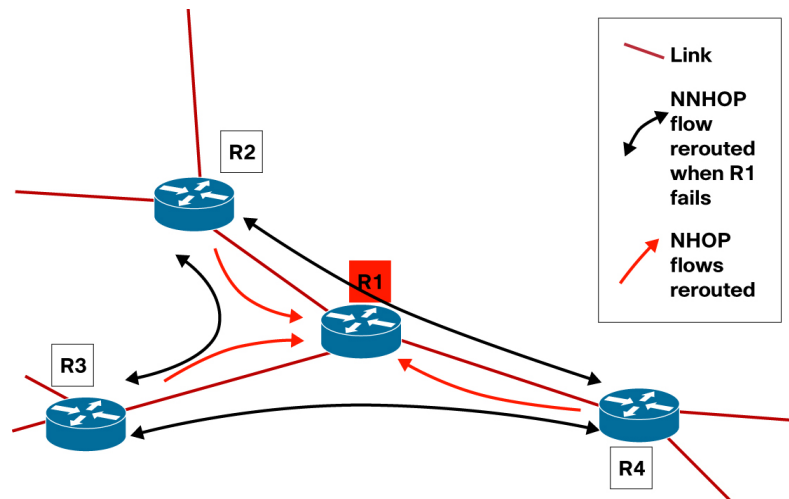
A. With FRR, it is possible to have defined "a priori" backup tunnels for local protection. In the case of the failure of a given element, all traffic on a given tunnel will be routed down a defined backup tunnel. This is known as connectivity protection. Bandwidth protection adds to this the assurance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

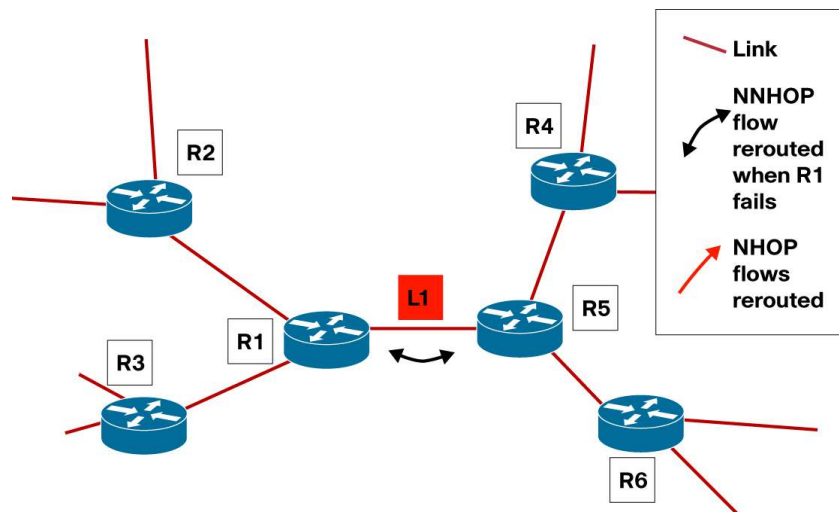
A. There can be a router, link, or SRLG failure. Following are scenarios related to each.

- *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 currently 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 (SRLG)*—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—they will be triggered by the link failure; 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 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. Is the process to ensure that bandwidth is protected without reserving bandwidth for backup tunnels a nontrivial process?

- A.** No. The process of investigating the possible backup-tunnel layouts can become very complex. Cisco IP Solution Center Traffic Engineering Management looks at single element failures and solves each problem individually. The difficulty of each problem depends upon several factors—connectivity, load balancing, and the number of possible paths for rerouting.

In Figure 1, there are nine flows to reroute to protect router R1. If there were three possible alternative paths for each flow (typically there are many more), there would be $39 = 19683$ possible backup tunnel layouts to be investigated. If load balancing of 2 were allowed, there would be twice as many flows to manage ($39 \times 2 = 387420489$ layouts to investigate). This is a nontrivial search space and is not possible for a user without the support of a tool such as Cisco IP Solution Center Traffic Engineering Management.

Q. Do I need Cisco IP Solution Center Traffic Engineering Management for a small network?

- A.** The numbers in the previous answer are typical of many simple and small networks involving as few as 10 routers.

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.

Q. How do I determine the bandwidth pool sizes when deploying traffic engineering on my network?

- A.** Cisco IP Solution Center Traffic Engineering Management is capable of helping in the analysis of different bandwidth settings to determine if the network elements are protected for different bandwidth settings. Moreover, the application allows many scenarios to be quickly analyzed, making it a useful tool for this mode of operation.

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 associated 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.

General Questions on Optimization

Q. What is an NP-complete problem?

- A.** An NP-complete problem is a combinatorial problem (where the variables have discrete values, such as integer values) that has no known algorithm that can solve the problem in polynomial time. That is, any algorithm in the worst case will require exponential time (with respect to the size of the problem) to complete its search. Essentially, there is no known scalable solution to such a problem.

These problems are also known as intractable. Here, exponential and polynomial refer to the problem size (the number of variables). In Cisco IP Solution Center Traffic Engineering Management, the size of the bandwidth protection problem (or worst-case time) to solve is exponential in the number of flows that need to be rerouted.

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 Metro 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 (AToM).

Cisco MPLS Diagnostics Expert

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

For More Information

For more information about Cisco IP Solution Center, visit www.cisco.com/go/isc and contact your local Cisco account representative or send e-mail to isc-mktg@cisco.com.



Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0609R)