



## Cisco IP Solution Center Traffic Engineering Management User Guide, 4.1

Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Text Part Number: OL-7648-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)

*Cisco IP Solution Center Traffic Engineering Management User Guide, 4.1*  
Copyright © 2005, Cisco Systems, Inc.  
All rights reserved.



<b>About This Guide</b>	<b>xi</b>
Objective and Audience	xi
How This Guide Is Organized	xi
Related Documentation	xii
Obtaining Documentation	xiii
Cisco.com	xiii
Product Documentation DVD	xiii
Ordering Documentation	xiv
Documentation Feedback	xiv
Cisco Product Security Overview	xiv
Reporting Security Problems in Cisco Products	xv
Obtaining Technical Assistance	xv
Cisco Technical Support & Documentation Website	xv
Submitting a Service Request	xvi
Definitions of Service Request Severity	xvi
Obtaining Additional Publications and Information	xvii
Conventions and Terminology	xviii

---

## CHAPTER 1

<b>Introduction to ISC TEM</b>	<b>1-1</b>
ISC TEM Overview	1-1
Process Flows	1-2
Features in ISC TEM	1-2
Licensing Schemes	1-3
ISC TEM Basics	1-3
Managed/Unmanaged Primary Tunnels	1-3
Conformant/Non-Conformant Tunnels	1-4
Defining Conformant/Non-Conformant Tunnels	1-4
Managing Non-Conformant Tunnels	1-5
Bandwidth Pools	1-5
Planning Tools	1-5

---

## CHAPTER 2

<b>Getting Started</b>	<b>2-1</b>
Prerequisites and Limitations	2-2

General Limitations	2-2
Feature-Specific Prerequisites and Limitations	2-2
Non-Cisco Devices and ISC TEM	2-2
Supported Platforms	2-3
Preconfiguration Process Overview	2-3
ISC TEM Setup and Installation	2-4
Installing an ISC TEM License	2-4
Editing DCPL Properties (Optional)	2-5
Creating a TE Provider	2-6

---

CHAPTER 3

**TE Network Discovery** 3-1

Overview	3-2
TE Discovery Prerequisites	3-2
Accessibility	3-2
Memory Shortage on Large Networks	3-2
IOS-XR and Enable Passwords	3-2
Creating a TE Discovery Task	3-3
Verifying a TE Discovery Task	3-7
Task Logs	3-7
TE Topology	3-11
View Network Element Types	3-11
Setting Up Management Interfaces	3-11
MPLS-TE Management Process	3-12
Making SSH Work With IOS-XR	3-12
Configuring Ethernet Links	3-12

---

CHAPTER 4

**TE Resource Management** 4-1

Overview	4-1
Modifying Network Resources	4-2
Change Link Status	4-6

---

CHAPTER 5

**Basic Tunnel Management** 5-1

Overview	5-2
Create TE Policy	5-2
Create Explicit Path	5-4
Primary Tunnel Operations	5-8
Create Primary Tunnel	5-8
Edit Primary Tunnel	5-16

Access from Primary Tunnel SR Window	5-16
Access from Service Requests Window	5-18
Delete Primary Tunnel	5-19
Backup Tunnel Operations	5-20
Create Backup Tunnel	5-20
Edit Backup Tunnel	5-24
From the Protection SR Window	5-25
From the Service Requests Window	5-26
Delete Backup Tunnel	5-26

---

## CHAPTER 6

### **Advanced Primary Tunnel Management** 6-1

Tunnel Operations	6-2
Create Primary Tunnel	6-2
Edit Primary Tunnel	6-8
Delete Primary Tunnel	6-8
Admit Primary Tunnel	6-8
Import Primary Tunnel	6-8
Construct XML Import File	6-9
Command Line Validation Tool	6-9
Import Procedure	6-9
Planning Strategy	6-11
Placement Tools	6-11
Tunnel Audit	6-12
Tunnel Placement	6-17
Tunnel Repair	6-22
Grooming	6-26

---

## CHAPTER 7

### **Protection Planning** 7-1

Overview	7-2
SRLG Operations	7-3
Create SRLG	7-3
Edit SRLG	7-5
Delete SRLG	7-5
Configure Element Protection	7-5
Protection Tools	7-7
Compute Backup	7-7
Audit Protection	7-12
Audit SR	7-14

## CHAPTER 8

### Traffic Admission 8-1

- Overview 8-1
- Creating a TE Traffic Admission SR 8-2
- Deploying a TE Traffic Admission SR 8-4
- Other Traffic Admission SR Operations 8-5
- Viewing the SR State 8-5

## CHAPTER 9

### Administration 9-1

- TE User Roles 9-1
- TE Policies 9-2
  - Create Policy 9-2
  - Edit Policy 9-4
  - Delete Policy 9-5
- TE Tasks 9-5
  - Creating a TE Task 9-6
    - Creating a TE Functional Audit Task 9-6
    - Creating a TE Interface Performance Task 9-11
- SR History and Configlets 9-17
- Manage Lock 9-17

## CHAPTER 10

### Task Monitoring 10-1

- TE Task Logs 10-1
  - SR Deployment Logs 10-1
  - Logs Created from Task Manager 10-2
  - Viewing a Task Log 10-2
    - From the Tasks window 10-2
    - From the Service Requests Window 10-4
- TE Performance Reports 10-4

## CHAPTER 11

### TE Topology 11-1

- Overview 11-1
- Accessing the TE Topology Tool Page 11-2
- Using the TE Topology Interface Applet 11-2
  - Displaying and Saving Layouts 11-4
- Using Maps 11-5
  - Loading a map 11-5
  - Adding new maps 11-7

Clearing Maps	11-8
Using Highlighting and Attributes	11-8
Clear Highlighting	11-9
Add/Modify Attributes	11-9
Clear Current Graph Layout	11-9
Using AntiAlias, BackingStore, DoubleBuffer	11-9
Using Algorithms	11-10

## APPENDIX A

### Traffic Engineering Management GUI A-1

Accessing the TEM GUI	A-1
TE Providers	A-3
Create/Edit TE Provider	A-3
TE Topology	A-5
Topology Display	A-5
Repository	A-7
File	A-8
Map	A-8
Graph	A-10
Tunnels	A-11
Algorithms	A-12
View	A-14
Tools	A-14
TE Nodes	A-18
Display TE Nodes	A-19
View Node Details	A-20
TE Links	A-21
Display TE Links	A-23
View Link Details	A-24
Show Tunnels	A-25
Edit Interface	A-27
TE SRLGs	A-30
Create/Edit TE SRLG	A-31
TE Explicit Paths	A-33
Create/Edit Explicit Path	A-34
TE Protected Elements	A-35
Protection Management	A-35
Compute Backup	A-37
Audit Protection	A-40
Assign TE Resources	A-40

Create Managed TE Tunnel	A-41
View Managed Primary Tunnel Details	A-43
Create TE Managed Primary Tunnel	A-44
Select Devices and Policy	A-46
Select TE Explicit Path	A-49
Explicit Path Viewer	A-49
Import Tunnel	A-50
Edit TE SR (Primary or Backup)	A-52
Planning Tools	A-52
Movable Tunnel Selection Window	A-52
TE Primary Tunnel Computation SR - Changes Window	A-54
TE Primary Tunnel Computation Results - Report	A-57
Create Unmanaged TE Tunnel	A-59
Create TE Backup Tunnel	A-59
Create TE Backup Tunnel Window	A-62
Select TE Protected Interface	A-63
TE Traffic Admission	A-64
Select TE Tunnel for Admission	A-64
TE Traffic Admission SR	A-65
Administration	A-67
Monitoring	A-67
TE Task Logs	A-67
Task Log	A-68
TE Performance Reports	A-69

## APPENDIX B

<b>Managing Service Requests</b>	<b>B-1</b>
Accessing the Service Requests Window	B-1
Service Request Operations	B-2
Viewing Service Request Details	B-3
History	B-3
Configlets	B-5
Editing a Service Request	B-6
Decommissioning a Service Request (Only Applies to TE Traffic Admission SRs)	B-7
Purging a Service Request	B-9
Verifying Service Requests	B-9
Service Request States	B-9



---

APPENDIX C**Warnings and Violations** C-1[Overview](#) C-1[Warnings](#) C-2[Protection Computation Warnings](#) C-2[Violations](#) C-3[Primary Placement Computation Violations](#) C-3[Protection Computation Violations](#) C-9

---

APPENDIX D**Document Type Definition (DTD) File** D-1[DTD File](#) D-1[Example](#) D-4

---

INDEX





## About This Guide

---

This guide describes how to administer and maintain the Cisco IP Solution Center Traffic Engineering Management (ISC TEM) software. This chapter describes how this guide is organized, who should read it, related information, and the document conventions used throughout the guide.

## Objective and Audience

The purpose of this guide is to enable users to take advantage of the features provided by ISC TEM to enhance the traffic performance and predictability in an IP network.

This book is written as a resource for experienced users and administrators who must install, configure, deploy, and monitor the ISC TEM software.

It is assumed you have a basic understanding of network design, operation, and terminology, a general familiarity with the ISC software, and that you are familiar with your own network configurations.

A general understanding of MPLS TE concepts and traffic engineering is also required.

## How This Guide Is Organized

This guide is organized as follows:

[Chapter 1, “Introduction to ISC TEM,”](#) gives an overview of the ISC TEM software.

[Chapter 2, “Getting Started,”](#) describes prerequisites and limitations and the preconfiguration process required to enable network data collection and deployment of TE configurations on the network.

[Chapter 3, “TE Network Discovery,”](#) describes the process of discovering the network for a particular TE provider.

[Chapter 4, “TE Resource Management,”](#) explains how to modify resource characteristics to optimize tunnel placement.

[Chapter 5, “Basic Tunnel Management,”](#) provides an overview of the stages required to create and deploy primary and backup tunnels with a base license.

[Chapter 6, “Advanced Primary Tunnel Management,”](#) describes the stages required to create and deploy primary tunnels using the planning functions.

[Chapter 7, “Protection Planning,”](#) explains how to compute protection tunnels for network elements and deploy these on the network.

[Chapter 8, “Traffic Admission,”](#) explains how to assign traffic to traffic-engineered tunnels.

[Chapter 9, “Administration,”](#) describes various administrative tools and features.

[Chapter 10, “Task Monitoring,”](#) explains how deployment and collection tasks are monitored and how task details are logged.

[Chapter 11, “TE Topology,”](#) explains how to use the TE Topology tool to display the layout of the network.

[Appendix A, “Traffic Engineering Management GUI,”](#) describes the ISC TEM GUI and the various fields and other GUI elements.

[Appendix B, “Managing Service Requests,”](#) covers the various operations used to manage service requests.

[Appendix C, “Warnings and Violations,”](#) lists warnings and violations that might be invoked when using the planning tools in ISC TEM.

[Appendix D, “Document Type Definition \(DTD\) File,”](#) contains a sample DTD file that specifies the structure and rules used for XML import.

## Related Documentation

The entire documentation set for Cisco IP Solution Center, 4.1 can be accessed at:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1)

The following documents comprise the ISC 4.1 documentation set.

General documentation (in suggested reading order):

- *Cisco IP Solution Center Getting Started and Documentation Guide, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/docguide/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/docguide/index.htm)
- *Release Notes for Cisco IP Solution Center, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/relnotes/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/relnotes/index.htm)
- *Cisco IP Solution Center Installation Guide, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/install/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/install/index.htm)
- *Cisco IP Solution Center Infrastructure Reference, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/infrastr/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/infrastr/index.htm)
- *Cisco IP Solution Center System Error Messages, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/mess/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mess/index.htm)

Application and technology documentation (listed alphabetically):

- *Cisco IP Solution Center L2VPN User Guide, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/l2vpn/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/l2vpn/index.htm)
- *Cisco IP Solution Center MPLS VPN User Guide, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/mpls/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mpls/index.htm)
- *Cisco IP Solution Center Quality of Service User Guide, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/qos/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/qos/index.htm)
- *Cisco IP Solution Center Traffic Engineering Management User Guide, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/tem/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/tem/index.htm)

- *Cisco MPLS Diagnostics Expert 1.0 User Guide on ISC 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/trble/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/trble/index.htm)

API Documentation:

- *Cisco IP Solution Center API Programmer Guide, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/api\\_set/api\\_gd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_gd/index.htm)
- Index: *Cisco IP Solution Center API Programmer Reference, 4.1*  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/api\\_set/api\\_ref/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_ref/index.htm)



Note

All documentation *might* be upgraded over time. All upgraded documentation will be available at the same URLs specified in this document.

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.



# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>  
or view the digital edition at this URL:  
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

# Conventions and Terminology

This section discusses conventions and terminology used throughout this manual.

- *pointer*—indicates where the mouse action is to occur
- *select*—to push and hold down the left mouse button
- *release*—to let up on a mouse button to initiate an action
- *click*—to select and release a mouse button without moving the pointer
- *double-click*—to click a mouse button twice quickly without moving the pointer
- *drag*—to move the pointer by sliding the mouse with one or more buttons selected.

This manual uses this terminology throughout (even though it is possible for individual users to customize their devices to use the buttons in an alternative manner). In situations that allow more than one item to be selected from a list simultaneously, the following actions are supported:

- To select a single item in a list, click on the entry. Clicking a second time on a previously selected entry deselects it.
- To select a contiguous block of items, click on the first entry; then, without releasing the mouse button, drag to the last desired entry and release. (A subsequent click anywhere on the screen deselects all previous selections.)
- To extend a currently selected block, hold the **Shift** key down and click on the entry at the end of the group to be added
- To add a non-contiguous entry to the selection group, press the **Ctrl** (Control) key and click on the entry to be added.

Names of on-screen elements that you click, or select (menu names and commands, and controls such as buttons, drop-down lists, and so on) are printed in **bold** font. **Bold** font is also used for keywords, names of commands, and names of keys on the keyboard. Text displayed as on-screen examples is printed in `courier` font.

When set off from the main text, words and characters you should enter by the keyboard are printed in **bold** font. When the word or character string is enclosed in angle brackets (< and >), you should substitute your own character string for the example presented in the text.

For example, when you see:

```
login: root
```

you should specify the string **root** at the **login** prompt. However, when you see:

```
password: <rootpassword>
```

you should specify your own password in place of the character string <**rootpassword**>. The *italic style* is used to emphasize words, to introduce new terms, and for titles of printed publications (however, not titles of CD-ROMs or floppy disks).



# Introduction to ISC TEM

---

This guide contains a detailed description of the Cisco IP Solution Center Traffic Engineering Management (ISC TEM) product, including the various features, the GUI, and the step-by-step processes needed to perform various traffic engineering management tasks.

This chapter includes the following sections:

- [ISC TEM Overview, page 1-1](#)
- [Process Flows, page 1-2](#)
- [Features in ISC TEM, page 1-2](#)
- [Licensing Schemes, page 1-3](#)
- [ISC TEM Basics, page 1-3](#)
  - [Managed/Unmanaged Primary Tunnels, page 1-3](#)
  - [Conformant/Non-Conformant Tunnels, page 1-4](#)
  - [Bandwidth Pools, page 1-5](#)
  - [Planning Tools, page 1-5](#)

## ISC TEM Overview

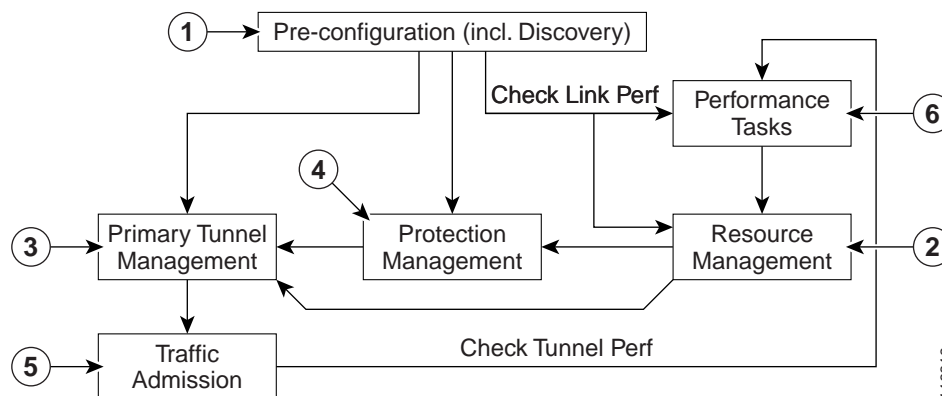
ISC TEM is the Traffic Engineering Management module of IP Solution Center. It is a tool for managing Multiprotocol Label Switching Traffic Engineering (MPLS TE) primary tunnels and backup tunnels for the purpose of offering traffic Service Level Agreement (SLA) guarantees. It provides bandwidth protection management, network discovery, and support for configuring MPLS TE. It includes a number of powerful planning tools, including a sophisticated primary path calculation tool and backup tunnel calculation for element protection.

MPLS TE mechanisms are provided to support requirements for predictability, traffic flow matched to QoS requirements, and Fast Restoration with Guaranteed Bandwidth, ensuring that strict SLA performance criteria (availability, delay, jitter) are met.

# Process Flows

The main components and flows in ISC TEM are depicted in [Figure 1-1](#).

**Figure 1-1 Main Process Flows in ISC TEM**



The illustration includes the following components:

1. **Pre-configuration**—Sets up key parameters that enable the system to collect TE network information (Discovery) and subsequently deploy TE configurations on the chosen network. (See [Chapter 2, “Getting Started”](#))
2. **Resource Management**—Tuning of certain properties on the TE interfaces to optimize the tunnel placement. (See [Chapter 4, “TE Resource Management”](#))
3. **Primary Tunnel Management**—Create and manage primary tunnels, either unmanaged (See [Chapter 5, “Basic Tunnel Management”](#)) or managed. (See [Chapter 5, “Basic Tunnel Management”](#) or [Chapter 6, “Advanced Primary Tunnel Management”](#))
4. **Protection Management**—Protect selected elements in the network (links, routers, or SRLGs) against failure. (See [Chapter 7, “Protection Planning”](#))
5. **Traffic admission**—Assign traffic to traffic-engineered tunnels. (See [Chapter 8, “Traffic Admission”](#))
6. **Performance Tasks**—Calculates interface/tunnel bandwidth utilization using the Simple Network Management Protocol (SNMP). (See [Chapter 9, “Administration”](#))

## Features in ISC TEM

ISC TEM adds a range of MPLS TE primary tunnel management features:

- **Tunnel Audit**—finding inconsistencies after making tunnel modifications
- **Tunnel Admission**—admitting new tunnels onto the network
- **Tunnel Repair**—fixing tunnel inconsistencies after network and service changes
- **Network Grooming**—optimizing global network utilization.

In addition, ISC TEM offers interaction and integration with ISC features:

- **Service activation focus**

- Integration with other ISC modules (MPLS VPN, IPsec VPN, L2VPN, QoS)
- Data Persistence
- Logging of user intent
- Service state management
- Service auditing
- Web-based GUI
- Role-Based Access Control (RBAC)

## Licensing Schemes

The ISC TEM installation comes with three types of licenses, TE, TE/RG, and TE/BRG, that gives access to all ISC TEM features, including [Planning Tools](#) for protection planning (backup tunnels).

The licensing for the TE license is based specifically on the scale of the MPLS-TE network, that is the number of nodes.

Ranges are as follows:

- Up to 20
- Up to 50
- Up to 100
- Up to 150
- Up to 200
- Up to 250
- and so on in increments of 50 nodes.

Upgrade license keys are available for the following upgrades:

- From 20 to 50
- From 50 to 100
- From 100 to 150
- From 150 to 200
- From 200 to 250
- and so on in increments of 50 nodes.

For instructions on how to install an ISC TEM license, see [Installing an ISC TEM License, page 2-4](#).

## ISC TEM Basics

To understand how ISC TEM works, certain key concepts must be explained.

### Managed/Unmanaged Primary Tunnels

In ISC TEM, the concept of managed tunnels is at the center of TE planning activities.

It is important to understand the differences:

- Managed TE tunnels:
  - (setup/hold) priority zero
  - non-zero RSVP bandwidth
  - explicit first path option
  - auto bandwidth must have a max value
- Unmanaged tunnels: All other tunnels.

In the ISC TEM Graphical User Interface (GUI), there is a separate entry point for dealing with managed and unmanaged tunnels. The GUIs are very similar and the differences are described in [Create Unmanaged TE Tunnel](#), page A-59.

## Conformant/Non-Conformant Tunnels

Understanding the concepts of conformant and non-conformant tunnels is key to making the most efficient use of ISC TEM.

ISC TEM only allows the creation of conformant tunnels. Non-conformant tunnels can be introduced through the TE Discovery process (see [Chapter 3, “TE Network Discovery”](#)).

## Defining Conformant/Non-Conformant Tunnels

In the ISC TEM design, a sharp distinction has been made between conformant and non-conformant tunnels:

- Conformant tunnel—A well-behaved tunnel that meets ISC TEM’s TE management paradigm (described below). A managed tunnel can only be a conformant tunnel. A non-zero priority unmanaged tunnel would also be a conformant tunnel. However, a conformant tunnel is not necessarily a managed tunnel.
- Non-conformant tunnel—A TE tunnel, which might impact ISC TEM’s ability to meet bandwidth guarantees. This could be due to unknown bandwidth requirements such as no max bandwidth configured for auto-bandwidth, potential for pre-emption, dynamic paths, etc. A zero priority unmanaged tunnel would also be a non-conformant tunnel.

The following are examples of non-conformant tunnels:

- a tunnel with zero setup and hold priority, an explicit path option of 1, but with zero bandwidth
- a tunnel with zero setup and hold priority, a non zero bandwidth, but with a dynamic first path option.
- a tunnel with zero setup and hold priority, an explicit path option of 1 and an auto bandwidth without a maximum defined.

Why are the above tunnels non-conformant? Because ISC TEM attempts to manage all tunnels with zero setup and hold priority, to ensure the links they pass through all have sufficient bandwidth, are affinity consistent and do not break delay or FRR constraints defined in the TE policy.

But if the tunnel’s path is dynamic or the amount of bandwidth it requires is undefined, ISC TEM does not have the information with which to manage the tunnel, so it marks it as non-conformant. All the non-conformant tunnels are displayed in the TE Unmanaged Primary Tunnels SR window.

## Managing Non-Conformant Tunnels

It is important to understand that non-conformant tunnels not only might cause the SLAs to be violated, they might also have an adverse effect on the managed tunnels (taking away bandwidth from them, for example).

However, when a non-conformant tunnel is discovered a warning is logged. ISC TEM tracks non-conformant tunnels so that they can be decommissioned.

So conformant tunnels are much preferred. They allow the system to offer bandwidth guarantees for managed tunnels. Unmanaged non-conformant tunnels might or might not provide the needed bandwidth and no bandwidth guarantees are given.

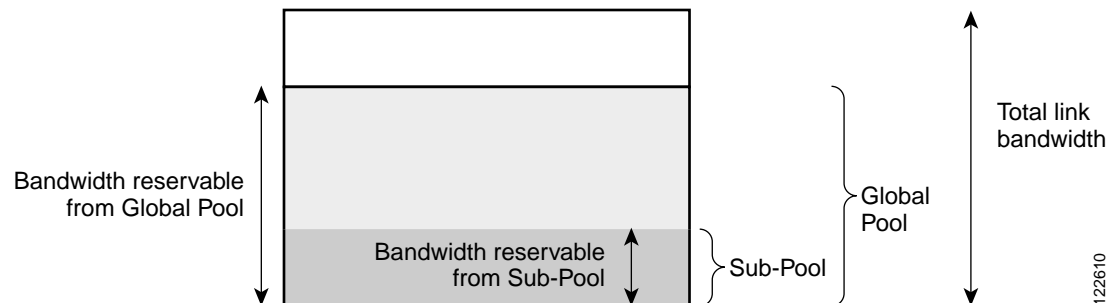
The action to take when you have non-conformant tunnels is either to change the setup and hold priorities to non-zero values (so they cannot preempt the managed tunnels) or migrate them to managed tunnels, allowing the tool to find a suitable explicit path.

## Bandwidth Pools

The bandwidth of each TE enabled interface is assigned a number of nested bandwidth pools. Currently, IOS supports two, namely Global Pool and Sub Pool.

For a better understanding of bandwidth pools, see [Figure 1-2](#).

**Figure 1-2** Bandwidth Pools



As [Figure 1-2](#) illustrates, Sub Pool is nested inside Global Pool. Thus, if a primary tunnel reserves bandwidth from the Sub Pool, it will also reserve the same bandwidth from the Global Pool.

Bandwidth reservations (primary tunnels) from the Sub Pool must not exceed, in total, the Sub Pool size. Likewise, bandwidth reservations from the Global Pool must not exceed, in total, the Global Pool size.

## Planning Tools

They are intended for evaluating planned improvements to a traffic-engineered network based on What-If scenarios .

The planning tools include the following features:

- Primary planning tools:
  - Tunnel Audit—Audits for inconsistencies in primary placement on the existing network with or without proposed tunnel or resource changes.

- Tunnel Placement—Usually for new tunnels. Tunnel Placement can generate a new route. It can be used for a tunnel that did not have a path before and needs to be placed.
- Tunnel Repair—Logically performed after Tunnel Audit (if something is wrong). Tunnel Repair has re-routing capabilities and can be used to move tunnels.
- Grooming—An optimization tool that works on the whole network. It is only available when no tunnel attributes have been changed.
- Protection planning tools:
  - Audit SR—Audits protection for manually added, modified and deleted backup tunnels before they are deployed.
  - Compute Backup—Automatically calculates the optimal backup tunnel for selected network elements.
  - Audit Protection—Audits protection of the selected elements against the existing backup tunnels.

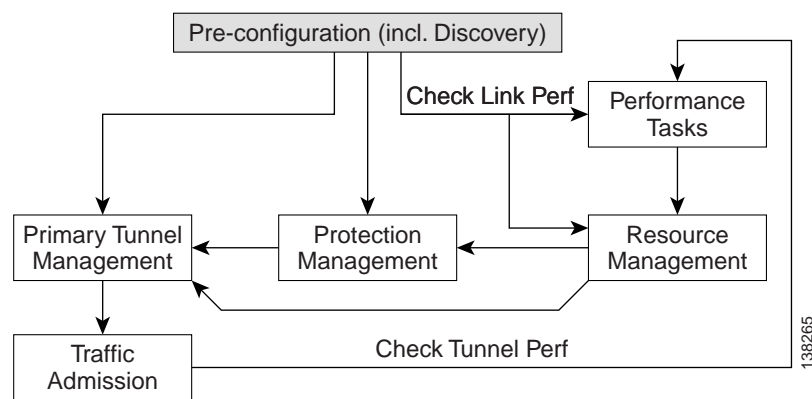
The planning tools are fully integrated within ISC TEM and are available from various locations within the GUI:

- TE Resource Modification (Tunnel Audit, Tunnel Repair)
- TE Protected Elements (Compute Backup and Audit Protection)
- Create Managed TE Tunnel (Tunnel Audit, Tunnel Placement, Tunnel Repair, Grooming)
- Create TE Backup Tunnel (Audit SR)





## Getting Started



This chapter describes the installation procedure for ISC TEM. The general installation procedure for Cisco IP Solutions Center (ISC) is described in *Cisco IP Solution Center Installation Guide, 4.1*.

This chapter includes the following sections:

- [Prerequisites and Limitations, page 2-2](#)
  - [General Limitations, page 2-2](#)
  - [Feature-Specific Prerequisites and Limitations, page 2-2](#)
  - [Non-Cisco Devices and ISC TEM, page 2-2](#)
  - [Supported Platforms, page 2-3](#)
- [Preconfiguration Process Overview, page 2-3](#)
- [ISC TEM Setup and Installation, page 2-4](#)
  - [Installing an ISC TEM License, page 2-4](#)
  - [Editing DCPL Properties \(Optional\), page 2-5](#)
- [Creating a TE Provider, page 2-6](#)

# Prerequisites and Limitations

The current release of ISC TEM involves certain prerequisites and limitations, which are described in this section.

See *Cisco IP Solution Center Installation Guide, 4.1* for general system recommendations.

## General Limitations

Concurrent use of the same installation is not supported. Let issued service requests finish deployment before issuing other service requests to avoid conflicts. This is described in more detail in the tunnel provisioning chapters.

The concurrency limitation also implies that opening multiple browsers displaying a single ISC installation is not recommended.

ISC TEM only supports MPLS-TE topology with point-to-point links.

## Feature-Specific Prerequisites and Limitations

Some features might only be available with a particular license. In addition, the number of nodes provided by the license limits the size of the network. For more information, see [Licensing Schemes, page 1-3](#).

A number of specific requirements are associated with the TE Discovery task. These are described in [TE Discovery Prerequisites, page 3-2](#).

In the Planning portion of the current implementation of ISC TEM, concurrent use is not recommended as users working simultaneously risk being unable to commit their changes.

JRE version 1.4.2\_04 or higher should be installed on the client computer, and if the user does not already have Java installed, they can use the links on the Topology Tool page to install the version that is bundled with ISC.

Non-POS interfaces cannot be protected on IOS-XR devices.

For users who have a repository that predates the ISC 4.1 release and has been upgraded to a 4.1 repository, you need to run a TE Discovery task to collect software version information from the devices before deploying service requests.

## Non-Cisco Devices and ISC TEM

ISC TEM does not manage non-Cisco devices and ISC cannot be used to provision them.

ISC will, however, discover non-Cisco devices and store them in the repository. Tunnels can be run through these devices, the bandwidth consumed can be accounted for, but the devices are not otherwise managed by ISC. TE tunnels originating from non-Cisco devices will not be discovered.

Sorting can be performed on different attributes in various parts of the ISC TEM GUI. However, due to the added support for non-Cisco devices, sorting cannot be performed on Device Name and MPLS TE ID in the TE Nodes List window.

## Supported Platforms

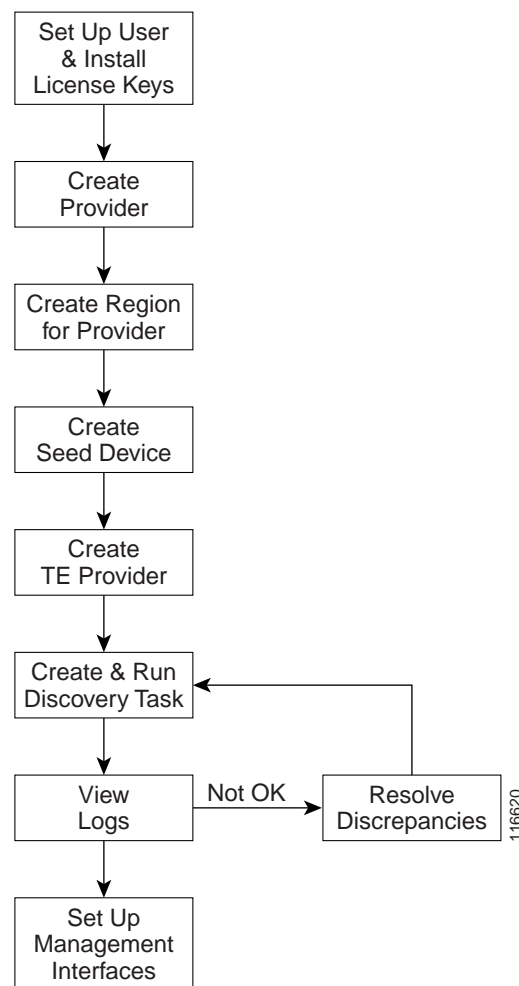
For supported devices and IOS platforms, see *Cisco IP Solution Center Installation Guide, 4.1*.

## Preconfiguration Process Overview

The preconfiguration process sets up key parameters that enable the system to collect TE network information and subsequently deploy TE configurations on the chosen network.

An overview of the preconfiguration process is provided in [Figure 2-1](#).

**Figure 2-1** Preconfiguration Process



Before commencing the preconfiguration process, MPLS-TE needs to be enabled on the network devices by making sure that the IP addresses used as devices' TE IDs are accessible from the management station (this step is not supported by ISC TEM).

The preconfiguration process includes the following steps:

- 
- Step 1 Set up new user and install license keys**—To run the TEM blade of ISC, it is necessary to create a new user and install license keys. These keys will enable the user to view and manage the TE tunnels and resources using ISC. (see [ISC TEM Setup and Installation, page 2-4](#))
- Step 2 Create a provider**—The provider is a concept designed to allow many different operators to work on ISC TEM simultaneously, each working on different networks. Thus, each provider has to be defined and used as a reference operator for future work on the system. (To create a provider, see *Cisco IP Solution Center Infrastructure Reference, 4.1.*)
- Step 3 Create a region for the provider**—The region is important because a single provider could have multiple networks. The region is used as a further level of differentiation to allow for such circumstances. (To create a region, see *Cisco IP Solution Center Infrastructure Reference, 4.1.*)
- Step 4 Create a seed device**—This IOS Device will be the seed router for network discovery. The network discovery process uses the seed router as an initial communication point to discover the MPLS TE network topology. A set of TE enabled devices, links, explicit paths, tunnels, and static routes are then populated to the database. (To create a seed router, see *Cisco IP Solution Center Infrastructure Reference, 4.1.*)
- Step 5 Create a TE Provider**—Providers can be defined as TE provider, if they are supporting MPLS TE in their network. It is necessary to create a TE provider to enable a TE network to be managed. All TE related data associated with a given network is stored under a unique TE provider. A provider and region uniquely define a TE provider (see [Creating a TE Provider, page 2-6](#)).
- Step 6 Run a Discovery Task**—Discover the TE network for a particular TE provider to populate the repository with a view to creating primary and backup tunnels (see [Chapter 3, “TE Network Discovery”](#)).
- Step 7 Set Up Management Interfaces**—Set up management interfaces for discovered devices or update server host file with resolution for all discovered devices. This step is only necessary if the devices in the TE network are not accessible via their hostnames (see [Setting Up Management Interfaces, page 3-11](#)).

**Note**

If Telnet is selected to communicate with the seed router, Telnet must also be used for the other network devices. Likewise, if SSH is selected for the seed router, SSH must be used for all other devices.

---

## ISC TEM Setup and Installation

Before setting up ISC TEM, the ISC software must be installed. To do so, see *Cisco IP Solution Center Installation Guide, 4.1.*

To set up a new ISC TEM user, one or more users with a TE role must be created. For step by step instructions, see *Cisco IP Solution Center Infrastructure Reference, 4.1.*

## Installing an ISC TEM License

Cisco IP Solution Center Traffic Engineering Management (ISC TEM) offers the license structure described in [Chapter 1, “Introduction to ISC TEM.”](#)

For an explanation of license keys in ISC, see *Cisco IP Solution Center Infrastructure Reference, 4.1.*

To install a TE license, use the following steps:

- 
- Step 1** Log into ISC with the following default values:
- User Name: **admin**
  - Password: **cisco**
- Step 2** Navigate **Administration > Security > Users**.
- Step 3** Click **Create**.
- Step 4** Fill in **User ID**, **Password**, **Verify Password**, and the **Personal Information** section.
- Step 5** Click **Edit** to edit the assigned roles.
- Step 6** Select **TERole** and click **OK**. **TERole** provides full access to ISC TEM. The **TEServiceOpRole** only has the privilege to access the tunnel admission SR.
- Step 7** Click **Save**.
- Step 8** Navigate **Administration > Control Center > Licensing**.
- Step 9** Enter the three TEM license keys for TE, TE/RG, and TE/BRG successively:
- Click **Install**.
  - Enter a license key.
  - Click **Save**.
- Repeat the procedure for each license key.
- Typing in all three license keys is the only valid installation.
- Step 10** Log out as **admin**.
- Step 11** Log in as the user created above.
- You are now ready to start using ISC TEM.
- 



**Note**

The **admin** role should only be used to manage ISC and not to perform network management operations.

---

## Editing DCPL Properties (Optional)

The ISC Dynamic Component Properties Library (DCPL) includes a wide variety of properties that are accessible from the GUI, some of which can be modified.

The various DCPL properties in ISC, including those pertaining to ISC TEM, and the process for editing these properties are described in [Cisco IP Solution Center Infrastructure Reference, 4.1](#).



**Warning**

**Do not attempt to modify the DCPL properties unless you fully understand the implications.**

---

In the ISC GUI, the DCPL properties are found in **Administration > Control Center > Hosts**. Select a check box for a specific host and click the **Config** button.

The DCPL properties pertaining to ISC TEM are found in the following folders:

- **Provisioning > Service > TE**
- **TE**
- **TETopology**

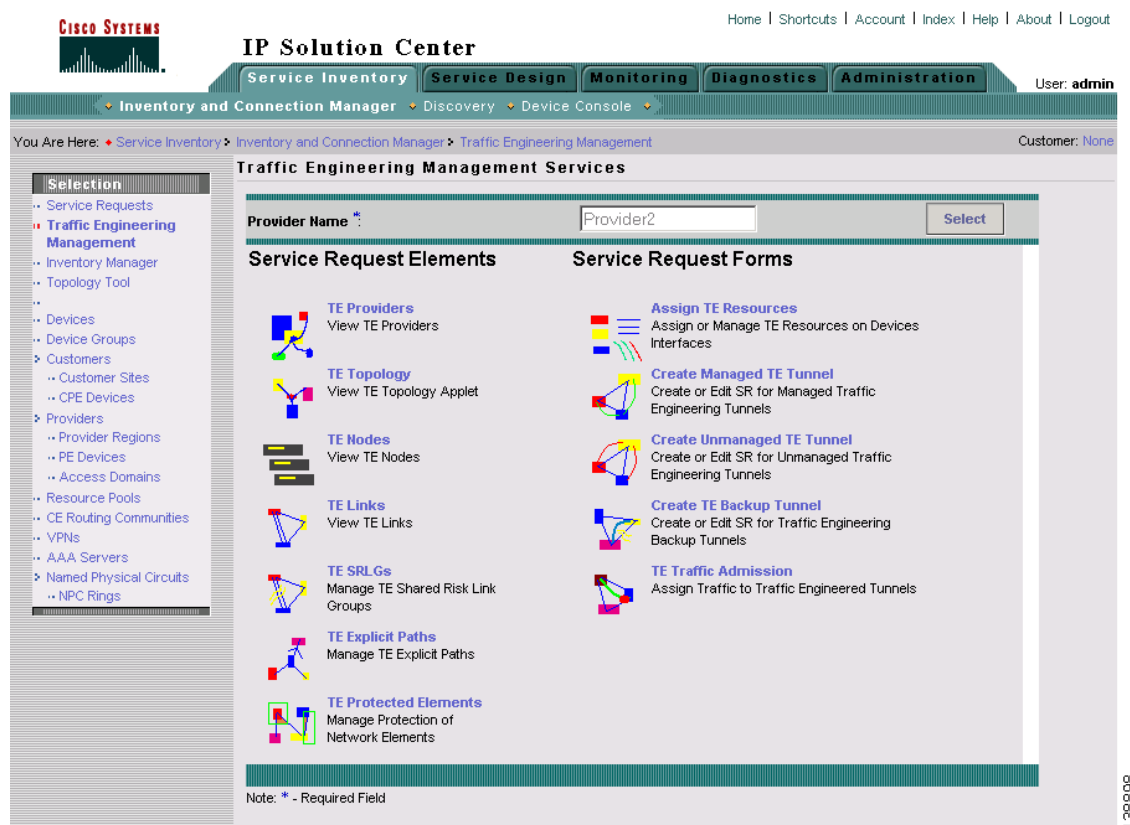
## Creating a TE Provider

After a provider and a region for that provider have been set up (see *Cisco IP Solution Center Infrastructure Reference, 4.1*), create a TE provider using the following steps:

- Step 1**    Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.

The Traffic Engineering Management Services window shown in [Figure 2-2](#) appears.

**Figure 2-2**    *Traffic Engineering Management Services*



- Step 2**    Click **TE Providers**.

The TE Providers window shown in [Figure 2-3](#) appears.

**Figure 2-3** TE Providers

The screenshot shows the 'TE Providers' window. At the top, there is a search bar labeled 'Show Providers with Provider Name matching' with an asterisk and a 'Find' button. Below this, it says 'Showing 1 - 1 of 1 record'. A table lists the providers with columns for '#', a checkbox, 'Provider Name', and 'System Lock Status'. The first row shows '1.', a checked checkbox, 'Provider2', and 'Unlocked'. Below the table, there is a 'Rows per page' dropdown set to '10' and a 'Go to page' field set to '1 of 1' with a 'Go' button. At the bottom right, there are four buttons: 'Create', 'Edit', 'Delete', and 'Manage Lock'.

For an explanation of the various window elements, see the “TE Providers” section on page A-3.

**Step 3** Click **Create** to create a TE provider.

The Create / Edit TE Provider window shown in [Figure 2-4](#) appears.

**Figure 2-4** Create/Edit TE Provider

The screenshot shows the 'Create/Edit TE Provider' window. It has several sections: 'Provider Name' with a text field and a 'Select' button; 'Primary Route Generation Parameters' with 'Default Primary RG Timeout (sec)' set to 100; 'Backup Route Generation Parameters' with 'Backup RG Timeout (sec)' set to 1000, 'FRR Protection Type' set to 'Sub Pool', 'Default Link Speed Factor' set to 1.00, 'Minimum Bandwidth Limit (kbps)' set to 10, and 'Max. Load Balancing Tunnel Count' set to 1; and 'Discovery Default Parameters' with 'Region for TE Devices' and 'Customer for Primary Tunnels', both with text fields and 'Select' buttons. At the bottom right are 'Save' and 'Cancel' buttons. A note at the bottom left states 'Note: \* - Required Field'.

For an explanation of the various window elements, see [Create/Edit TE Provider, page A-3](#).

To select a provider name, click the **Select** button next to the **Provider Name** field. The Select Provider window shown in [Figure 2-5](#) appears.

**Step 4** Add primary and backup route generation parameters.

When the FRR protection type is equal to Sub Pool, the backup tunnels generated by the tool will protect only the sub pool primary tunnels. When it is equal to Any Pool, the backup tunnels generated by the tool will protect both sub pool and global pool primary tunnels.

For more information on Fast Re-Route (FRR) protection pools, see [Bandwidth Pools, page 1-5](#).

**Figure 2-5** *Select Provider for Create TE Provider*

Showing 1 - 2 of 2 records

#	Provider Name
1.	<input type="radio"/> Provider1
2.	<input type="radio"/> Provider2

Rows per page: 10 Go to page: 1 of 1 Go

Select Cancel

138900

- Step 5** Select the desired provider using the radio buttons or search for a provider with search criteria matching a provider name and click **Find**.
- Step 6** Click **Select** to select the desired provider. The Select Provider window closes.  
The selected provider name is displayed in the **Provider Name** field.
- Step 7** Fill in the remaining required fields (marked ‘\*’) and any optional fields as desired.
- Step 8** For the required **Region for TE Devices** field, click the corresponding **Select** button. The Select Region for Create TE Provider window shown in [Figure 2-6](#) appears.

**Figure 2-6** *Select Region for Create TE Provider*

Region for Create TE Provider

Showing 1-1 of 1 records

#	Select	Region Name	Provider Name
1.	<input type="radio"/>	region_1	Provider1

Rows per page: 10 Go to page: 1 of 1 Go

Select Cancel

138901

- Step 9** Select the desired region using the radio buttons.
- Step 10** Click **Select** to select the desired region. The Region for Create TE Provider window closes.  
The selected region name is displayed in the **Region for TE Devices** field.
- Step 11** For the optional **Customer for Primary Tunnels** field, click the corresponding **Select** button. The Customer for Create TE Provider window shown in [Figure 2-7](#) appears.



**Figure 2-7**      **Select Customer for Create TE Provider**

- Step 12** If desired, select a customer using the radio buttons or search for a customer by entering customer search criteria in the **Show Customers with Customer Name matching** field and click **Find**.
- Step 13** Click **Select** to select the desired customer. The Select Customer for Create TE Provider window closes. The selected customer name is displayed in the **Customer for Primary Tunnels** field of the Create/Edit TE Provider window.
- Step 14** Click **Save**.

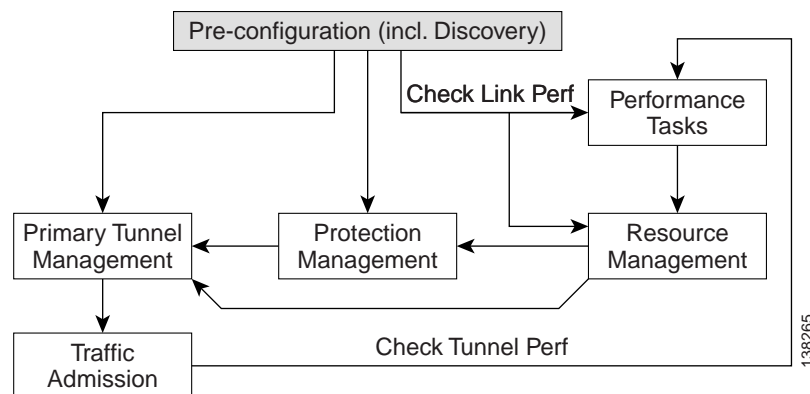
The created TE provider appears in the TE Provider window and can now be used to perform TE discovery and other TE functions.

To switch between TE providers, go to the top of the Traffic Engineering Management Services window (Figure 2-2) and click the **Select** button for the **Provider Name** field.





## TE Network Discovery



After completing the preconfiguration process and creating a seed router, you can discover the TE network for a particular TE provider. This populates the repository with the network topology. Also, you might need to set up the management interfaces. The necessary steps are described in this chapter.

This chapter includes the following sections:

- [Overview, page 3-2](#)
- [TE Discovery Prerequisites, page 3-2](#)
  - [Accessibility, page 3-2](#)
  - [Memory Shortage on Large Networks, page 3-2](#)
  - [IOS-XR and Enable Passwords, page 3-2](#)
- [Creating a TE Discovery Task, page 3-3](#)
- [Verifying a TE Discovery Task, page 3-7](#)
  - [Task Logs, page 3-7](#)
  - [TE Topology, page 3-11](#)
  - [View Network Element Types, page 3-11](#)
- [Setting Up Management Interfaces, page 3-11](#)
  - [MPLS-TE Management Process, page 3-12](#)
  - [Making SSH Work With IOS-XR, page 3-12](#)
  - [Configuring Ethernet Links, page 3-12](#)

# Overview

The purpose of the discovery process is to populate the repository with the network topology, tunnels, and static routes to tunnels present in the live network.

The discovery process uses a seed device to discover the MPLS TE network topology using either Telnet or SSH. All the Traffic Engineering routers in the network should be accessible via their TE ID if the device entry does not exist in the repository. The Management IP address will be used to access the device if the device entry exists in the Repository.

TE Discovery is a schedulable task that can be run once or on a periodic basis. Any inconsistencies between the repository and the network are reported in the Discovery log. The service state information is updated incrementally by logging tunnel in-use Label Switched Paths (LSPs) and updating the service request (SR) state.

## TE Discovery Prerequisites

The following prerequisites apply mainly to TE discovery.

For an overview of the general ISC TEM prerequisites, see [Prerequisites and Limitations, page 2-2](#).

## Accessibility

To successfully run a **TE Discovery** task, the seed router must be directly accessible from the management station.

ALL TE routers must be accessible from the ISC machine via their TE router ID. This is often the a loopback ip address, but not always.

For Telnet/SSH, there must be either direct Telnet/SSH access from the Cisco IP Solution Center Traffic Engineering Management (ISC TEM) management station to each device.

See [Preconfiguration Process Overview, page 2-3](#) for instructions on how to select Telnet or SSH when setting up a seed router.

## Memory Shortage on Large Networks

When running discovery on a large network (250+ devices or 5000+ tunnels, for example) or an `OutOfMemoryException` is encountered, do the following:

Edit the `watchdog.server.worker.java.flags` property in the `vpnsc.properties` file to a value, for example `-Xmx1024m`, instead of the default value `-Xmx512m`. This increases the heap size of the discovery task, which will clear up the `OutOfMemoryException` problem.

Revert the `watchdog.server.worker.java.flags` property back to its original value to reduce the resource usage when no longer needed.

## IOS-XR and Enable Passwords

If an IOS-XR device is to be used as a seed device, the enable password should be set in its device record even though IOS-XR does not require an enable password,for itself. That way IOS devices in the network, which do require an enable password, may be fully discovered

When creating an IOS-XR device through the **Devices** tab (**Service Inventory > Inventory and Connection Manager > Devices**) to act as a seed device for an initial discovery, it is strictly speaking not necessary to specify the enable password - ISC TEM will be able to log in and get all the data it needs.

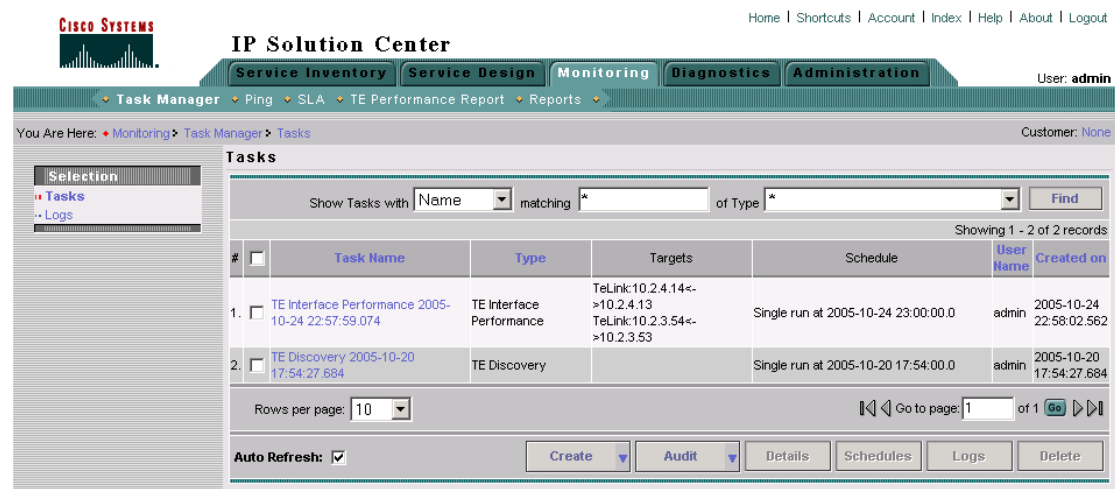
However, if there are other IOS devices in the same network, ISC TEM will not be able to enter enable mode for those devices. As a result, these are not fully discovered in the sense that the inability to enter enable mode stops ISC TEM from gathering all the relevant data. These other IOS routers will show up as **'unknown'** devices in the **Devices** window).

## Creating a TE Discovery Task

To create a TE Discovery task on the TE network, use the following steps:

- Step 1** Navigate **Monitoring > Task Manager**. The window in [Figure 3-1](#) appears.

**Figure 3-1** Tasks



- Step 2** Create a new task by selecting **Create > TE Discovery**. The window in [Figure 3-2](#) appears.

138902

**Figure 3-2** Create TE Discovery Task (Step 1)

**Create Task**

**Name \***: TE Discovery 2005-10-24 23:12:09.646

**Type**: TE Discovery

**Description**: Created on 2005-10-24 23:12:09.646

Note: \* - Required Field

- Step 1 of 2 -

< Back   Next >   Finish   Cancel

- Step 3** Optionally alter the **Name** and/or **Description** fields and click **Next**. The Select TE Provider window in [Figure 3-3](#) appears.

**Figure 3-3** Select TE Provider

**Select TE Provider**

Show TE Providers with Name matching \* Find

Showing 1 - 1 of 1 record

#	Provider Name	PE Region Name
1.	Provider2	region_2

Rows per page: 10

Go to page: 1 of 1 Go

- Step 1 of 4 -

< Back   Next >   Finish   Cancel

- Step 4** Select a TE provider and click **Next**. The Select Seed Device window in [Figure 3-4](#) appears. Non-Cisco devices, if any, are excluded from the list.

Figure 3-4 Select Seed Device

**Select Seed Device**

Show Devices with  matching

Showing 1 - 10 of 22 records

#		Device Name	Management IP Address	Type
1.	<input type="radio"/>	pe1		Cisco IOS Device
2.	<input type="radio"/>	pe3		Cisco IOS Device
3.	<input type="radio"/>	sw2		Cisco IOS Device
4.	<input type="radio"/>	sw3		Cisco IOS Device
5.	<input type="radio"/>	sw4		Cisco IOS Device
6.	<input type="radio"/>	ce3		Cisco IOS Device
7.	<input type="radio"/>	ce8		Cisco IOS Device
8.	<input type="radio"/>	ce13		Cisco IOS Device
9.	<input checked="" type="radio"/>	isctmp1		Cisco IOS Device
10.	<input type="radio"/>	isctmp11		Cisco IOS-XR Device

Rows per page:

Step 2 of 4 -

- Step 5** Select the seed device for discovery of the network and click **Next**. The Task Schedules window in [Figure 3-5](#) appears.

Figure 3-5 TE Discovery Task Schedules Window Before Scheduling

**Task Schedules**

Showing 0 of 0 records

#	<input type="checkbox"/>	Schedule	Start Date and Time	End Date and Time	Max Runs	Max Instances
---	--------------------------	----------	---------------------	-------------------	----------	---------------

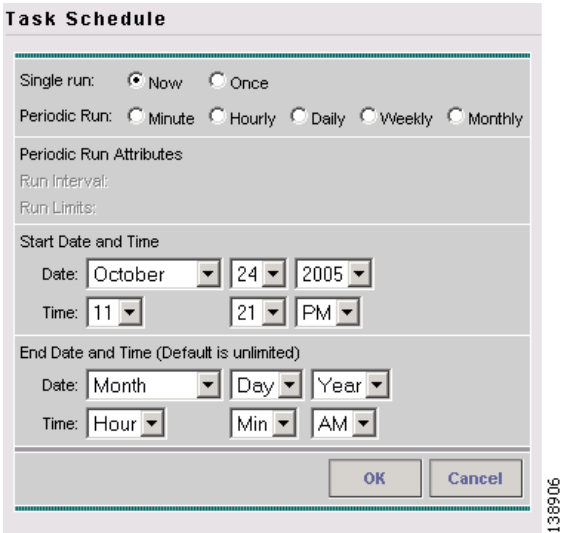
Rows per page:

Step 3 of 4 -

- Step 6** Create a task schedule in one of two ways:
- Click **Now** to schedule the task to run immediately, in which case the schedule information is automatically filled into the Task Schedules list ([Figure 3-7](#)).

- Click **Create** to create a scheduler for this task, in which case the Task Schedule window in [Figure 3-6](#) appears.

Figure 3-6 Task Schedule



The Task Schedule dialog box contains the following sections:

- Single run:** Radio buttons for **Now** (selected) and **Once**.
- Periodic Run:** Radio buttons for **Minute**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.
- Periodic Run Attributes:**
  - Run Interval:** (Empty text field)
  - Run Limits:** (Empty text field)
- Start Date and Time:**
  - Date:** Month (October), Day (24), Year (2005)
  - Time:** Hour (11), Min (21), AM/PM (PM)
- End Date and Time (Default is unlimited):**
  - Date:** Month, Day, Year
  - Time:** Hour, Min, AM/PM
- Buttons:** OK, Cancel

138906

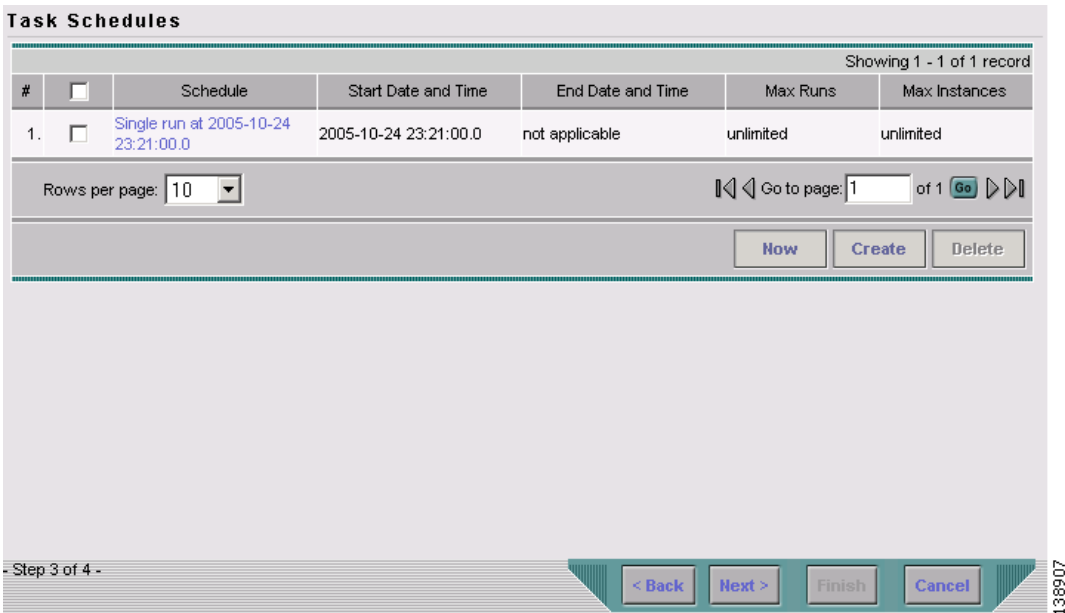
**Step 7** In the Task Schedule window, make your selections to define when and how often the task should be run.



**Note** The default setting is to schedule a single **TE Discovery** task to take place immediately (“**Now**”).

**Step 8** Click **OK**. The scheduled task should now appear in the Task Schedules table as shown in [Figure 3-7](#).

Figure 3-7 TE Discovery Task Schedules Window After Scheduling



The Task Schedules window displays a table with the following data:

#	<input type="checkbox"/>	Schedule	Start Date and Time	End Date and Time	Max Runs	Max Instances
1.	<input type="checkbox"/>	Single run at 2005-10-24 23:21:00.0	2005-10-24 23:21:00.0	not applicable	unlimited	unlimited

Showing 1 - 1 of 1 record

Rows per page: 10 Go to page: 1 of 1

Buttons: Now, Create, Delete

Step 3 of 4 -

Buttons: < Back, Next >, Finish, Cancel

138907



**Step 9** Click **Next**. A summary of the scheduled task in [Figure 3-8](#) appears.

**Figure 3-8** *Discovery Task Summary*

Discovery Task Summary	
Name:	TE Discovery 2005-10-24 23:12:09.646
TE Provider:	Provider2
Seed TE Router:	isctmp1
Schedules:	Single run at 2005-10-24 23:21:00.0

- Step 4 of 4 -

< Back   Next >   Finish   Cancel

138908

**Step 10** Click **Finish**. This will add the task to the list of created tasks in the Tasks window ([Figure 3-1](#)).

## Verifying a TE Discovery Task

The result of running the **TE Discovery** task can be assessed in three ways:

- [Task Logs](#)—View a summary log of any changes that have occurred in the network.
- [TE Topology](#)—Display the latest TE Topology from the repository.
- [View Network Element Types](#)—In the Traffic Engineering Management GUI, go to **TE Nodes**, **TE Links**, **TE Primary Tunnels**, and so on to verify the state of specific network element types.

## Task Logs

The TE Discovery log captures the state of the network and compares it with the most recent snapshot of the repository.

To view the task log for a **TE Discovery** task, use the following steps:

- Step 1** Navigate **Monitoring > Task Manager**.
- Step 2** Select **Logs** in the table of contents on the left side of the Tasks window. The Task Logs window in [Figure 3-9](#) appears.

Figure 3-9 Task Logs - TE Discovery

Task Logs

Show Runtime Tasks with Task Name matching  Find

Showing 1 - 6 of 6 records

#	<input type="checkbox"/>	Runtime Task Name	Action	Start Time	End Time	Status
1.	<input checked="" type="checkbox"/>	TE Discovery 2005-11-02 15:50:25.705_VWed_Nov_02_15:50:45_PST_2005_4	Discovery Task	2005-11-02 15:50:46.47	2005-11-02 15:55:01.306	Completed successfully
2.	<input type="checkbox"/>	TE Discovery 2005-11-02 15:48:32.554_VWed_Nov_02_15:48:54_PST_2005_3	Discovery Task	2005-11-02 15:48:55.386	2005-11-02 15:49:05.346	Failed
3.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-10-31 12:20:45.471_Mon_Oct_31_12:20:49_PST_2005_2	ConfigAudit	2005-10-31 12:21:01.944	2005-10-31 12:22:17.846	Completed with 1 errors
4.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-10-31 12:20:45.471_Mon_Oct_31_12:20:49_PST_2005_2	Deployment Phase C	2005-10-31 12:21:00.421	2005-10-31 12:21:01.92	Completed successfully
5.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-10-31 12:20:45.471_Mon_Oct_31_12:20:49_PST_2005_2	Deployment Phase B	2005-10-31 12:20:59.453	2005-10-31 12:21:00.398	Completed successfully
6.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-10-31 12:20:45.471_Mon_Oct_31_12:20:49_PST_2005_2	Deployment Phase A	2005-10-31 12:20:51.009	2005-10-31 12:20:59.425	Completed successfully

Rows per page: 10 Go to page: 1 of 1 Go

Auto Refresh: ☒ Service Requests View Log Delete

For an explanation of the various window elements, see [Task Log, page A-68](#).

The status of each task is shown in **Status** column. This updates automatically and indicates when the discovery process is complete.

If the task is not completed and **Auto Refresh** is selected, the table continues to update periodically until it is completed.

**Step 3** To view the log for a particular task, click the log name in the **Action** column. A copy of a TE Discovery log is shown in the following screenshots, starting with [Figure 3-10](#).



**Note** To find the summary of changes in the network depicted in the following screenshots, scroll to the bottom of the log .

Figure 3-10 TE Discovery Task Log - Devices/Interfaces

```
[Step 1 of 6] Process Device(s)/Interface(s)

ADD: Device(s)/Interface(s) to Repository:

SKIP: Matching Device(s)/Interface(s) in Repository:

1. isctmpl2., TEID: 192.168.118.168, Vendor: Cisco
1.1. POS0/1/0/1 -- 10.2.4.13

2. isctmpl3., TEID: 192.168.118.171, Vendor: Cisco
2.1. GigabitEthernet2/0/0 -- 10.2.4.46
2.2. GigabitEthernet1/0/0 -- 10.2.4.50

3. isctmpl., TEID: 192.168.118.176, Vendor: Cisco
3.1. FastEthernet3/1/0 -- 10.2.3.93
3.2. FastEthernet1/1/0 -- 10.2.2.110
3.3. FastEthernet3/0/1 -- 10.2.3.89
3.4. FastEthernet2/1/0 -- 10.2.3.54
3.5. FastEthernet2/1/1 -- 10.2.3.57
```

**Figure 3-11** TE Discovery Task Log - Links

```
[Step 2 of 6] Process Link(s)

ADD: Link(s) to Repository:

SKIP: Matching Link(s) in Repository:

1. 10.2.4.6 -- 10.2.4.5
2. 10.2.4.10 -- 10.2.4.9
3. 10.2.4.14 -- 10.2.4.13
4. 10.2.4.22 -- 10.2.4.21
5. 10.2.4.49 -- 10.2.4.50
6. 10.2.4.29 -- 10.2.4.30
7. 10.2.4.46 -- 10.2.4.45
8. 10.2.4.53 -- 10.2.4.54
9. 10.2.3.93 -- 10.2.3.94
10. 10.2.2.161 -- 10.2.2.174
11. 10.2.2.110 -- 10.2.2.97
12. 10.2.2.129 -- 10.2.2.142
13. 10.2.2.145 -- 10.2.2.158
```

138912

**Figure 3-12** TE Discovery Task Log - Explicit Paths

```
[Step 3 of 6] Process Explicit Path(s)

ADD: Explicit Path(s) to Repository:

1. isctmp11.
1.1. p11-p8: 10.2.4.5 :
1.2. p11-p12-p7-p8: 10.2.4.14 : 10.2.4.29 : 10.2.3.49 :
1.3. isctmp11-isctmp8-1: 10.2.4.13 : 10.2.4.30 : 10.2.2.126 :
1.4. isctmp11-isctmp12-1: 10.2.4.9 :

2. isctmp10.
2.1. p10-p12-p11: 10.2.4.21 : 10.2.4.10 :
2.2. p10-p12-p7-pl: 10.2.4.21 : 10.2.4.30 : 10.2.2.110 :
2.3. loopback-p10-p12-p11: 192.168.118.168 : 192.168.118.166 :

3. isctmp12.
3.1. p12-p7-p8-p11: 10.2.4.30 : 10.2.2.126 : 10.2.4.6 :
3.2. isctmp12-isctmp5-1: 10.2.4.50 : 10.2.4.54 : 10.2.2.81 :

4. isctmp8.
4.1. isctmp8-isctmp7-1: 10.2.2.113 :
```

138913

**Figure 3-13** TE Discovery Task Log - Primary Tunnels

```
[Step 4 of 6] Process Primary Tunnel(s)

ADD: Primary Tunnel(s) to Repository:

1. tunnel-te2 : isctmp11 -- isctmp10
2. tunnel-tel000 : isctmp11 -- isctmp1
3. tunnel-tel : isctmp10 -- isctmp6
4. tunnel-te2 : isctmp10 -- isctmp1
5. tunnel-tel33 : isctmp12 -- isctmp7
6. tunnel-te212 : isctmp12 -- isctmp7
7. tunnel-tel000 : isctmp12 -- isctmp2
8. tunnel-tel001 : isctmp12 -- isctmp2
9. Tunnel2 : isctmp1 -- isctmp8
10. Tunnel3 : isctmp1 -- isctmp5
11. Tunnel138 : isctmp1 -- isctmp3
12. Tunnel300 : isctmp1 -- isctmp2
13. Tunnel1000 : isctmp1 -- isctmp11
14. Tunnel2000 : isctmp1 -- isctmp2

SKIP: Matching Primary Tunnel(s) in Repository:
```

138914

**Figure 3-14** TE Discovery Task Log - Backup Tunnels

```
[Step 5 of 6] Process Backup Tunnel(s)

ADD: Backup Tunnel(s) to Repository:

    1. tunnel-tel002 : isctmpl1 -- isctmp8
    2. tunnel-tel005 : isctmpl1 -- isctmpl2
    3. tunnel-tel000 : isctmpl2 -- isctmp5

SKIP: Matching Backup Tunnel(s) in Repository:

MISSING: Backup Tunnel(s) from Network but Found in Repository:

    1. tunnel-te3 : isctmpl1 -- isctmpl2
    2. tunnel-tel001 : isctmpl1 -- isctmp8
    3. Tunnel2 : isctmpl3 -- isctmpl2
    4. Tunnel1 : isctmpl1 -- isctmp2
    5. Tunnel4 : isctmpl1 -- isctmp2
    6. Tunnel5 : isctmpl1 -- isctmp3
```

138915

**Figure 3-15** TE Discovery Task Log - Static Routes

```
[Step 6 of 6] Process Static Route(s)

ADD: Static Route(s) to Repository:

    1. isctmpl1
    1.1. 1.2.3.4 [255.255.255.255] -- tunnel-tel000
    1.2. 10.2.4.5 [255.255.255.255] -- tunnel-tel004

SKIP: Matching Static Route(s) in Repository:

MISSING: Static Route(s) from Network but Found in Repository:

    1. isctmpl0
    1.1. 3.3.3.3 [255.255.255.255] -- tunnel-tel -- distance -- 10

    2. isctmpl1
    2.1. 3.3.3.3 [255.255.255.255] -- Tunnel2 -- distance -- 10
```

138916

The TE Discovery task log window is organized into sections that each describes particular events in the TE network:

- either the state of the network as recorded in the repository the first time a **TE Discovery** task is run
- or changes in the network since the last time the **TE Discovery** task was run (repository delta).

The summary of changes in the network is reported in six steps:

1. Devices/Interfaces (Figure 3-10)
2. Links (Figure 3-11)
3. Explicit paths (Figure 3-12)
4. Primary tunnels (Figure 3-13)
5. Backup tunnels (Figure 3-14)
6. Static routes (Figure 3-15).

As seen in the figures, in each step a log table reports the changes in the following reporting categories:

- **ADD**—This section lists those elements that the **TE Discovery** task added to the repository. At the initial discovery, all elements should be in the ADD section as nothing existed in the repository beforehand. With every subsequent discovery, the ADD section will list elements that have been added to the network since the discovery independent of ISC TEM. Thus, the ADD function is synchronizing the repository with the network by adding these elements..
- **SKIP**—This section lists those elements that exist both in the network and in the repository and have all attributes equal. This shows that these elements have not been deleted or modified independently of ISC TEM.
- **MISSING**—This section lists those elements that exist in the repository but do not exist in the network, implying that they have been deleted independently of ISC TEM. This indicates that more investigation is required in order to correct the discrepancy.
- **MISMATCH**—This section lists those elements that exist both in the network and in the repository, but have one or more attributes that are not equal. This implies that these elements have been modified independently of ISC TEM and that you need to investigate and correct the problem.
- **MODIFY**—This section lists any network elements that have had attributes in the repository modified since the previous run of the **TE Discovery** task to synchronize with the network. These are usually dynamic attributes, such as the time when a tunnel was set up.

Step 4 Click **Return to Logs** to quit the current log with the option to open another log.

---

## TE Topology

The TE Topology tool provides a visual snapshot of the current state of the network. It cannot be used to determine changes that have taken place in the network.

The steps required to generate a topology graph of the network are described in [Chapter 11, “TE Topology.”](#)

## View Network Element Types

Another way to check the state of the network after running TE discovery is to go to the Traffic Engineering Management Services window and select the type of elements you want to verify.

For example, to check the status of the nodes after running TE discovery, navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Nodes**. Look at the updated list of TE nodes to assess which nodes are in the network.

Do the same for TE Links, TE Primary Tunnels, TE Backup Tunnels, and so on.

## Setting Up Management Interfaces

Before commencing tunnel management operations, you need to set up management interfaces. However, this step is only necessary if the network devices are not accessible by the hostname from the management station.

For a detailed description of how to set up management interfaces on specific devices, see *Cisco IP Solution Center Infrastructure Reference, 4.1* in the section on creating devices.

## MPLS-TE Management Process

The MPLS-TE management process involves the following steps:

1. Enable MPLS-TE on the network devices and make sure that the IP addresses used as the devices TE IDs are accessible from the management station (this step is not supported by ISC TEM).
2. Prepare the repository for discovering MPLS-TE network.
3. Set up management interfaces for the discovered devices or update the server host file with resolution for all discovered devices. Again, this is not needed if the hostnames are already accessible from the management station.
4. Discover the MPLS-TE network.

You will then be in a position to run the other MPLS-TE functions available in ISC TEM.



### Note

When the repository is empty, or when the management IP addresses are not configured for current devices in the TE network, make sure that the router MPLS TE ID can be reached from the management station. In other words, the TE discovery process does not support seed passthrough.

## Making SSH Work With IOS-XR

To make SSH work with IOS-XR, enter the following commands on the IOS-XR device:

```
(config)# domain name <domain name>
# crypto key gen rsa
```

Verify the crypto configuration by way of the following command:

```
# sh crypto key mypubkey rsa
```

Next, configure all links as point-to-point as described in [Configuring Ethernet Links, page 3-12](#).

## Configuring Ethernet Links

Only point-to-point links are supported in ISC TEM. POS links are point-to-point by default but otherwise Ethernet links need to be configured as point-to-point.

For IOS, enter the following command:

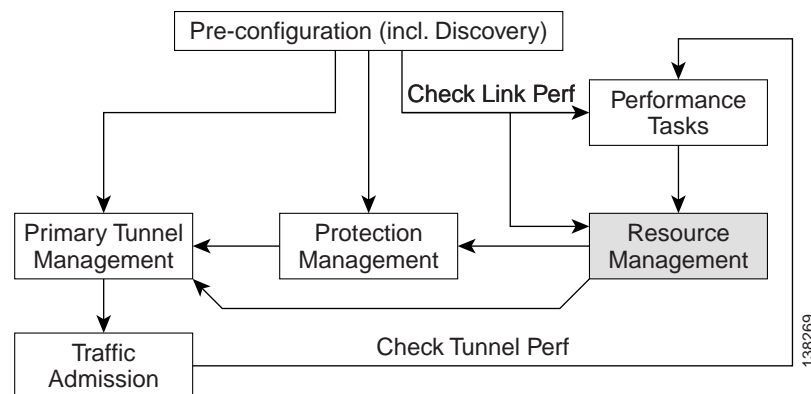
```
# ip ospf network point-to-point
```

For IOS-XR, enter the following command:

```
# router ospf <id> area 0 interface <name> network point-to-point
```



## TE Resource Management



TE resource management is defined as the tuning of certain properties on the TE interfaces to optimize the tunnel placement.

This chapter contains the following sections:

- [Overview, page 4-1](#)
- [Modifying Network Resources, page 4-2](#)
- [Change Link Status, page 4-6](#)

## Overview

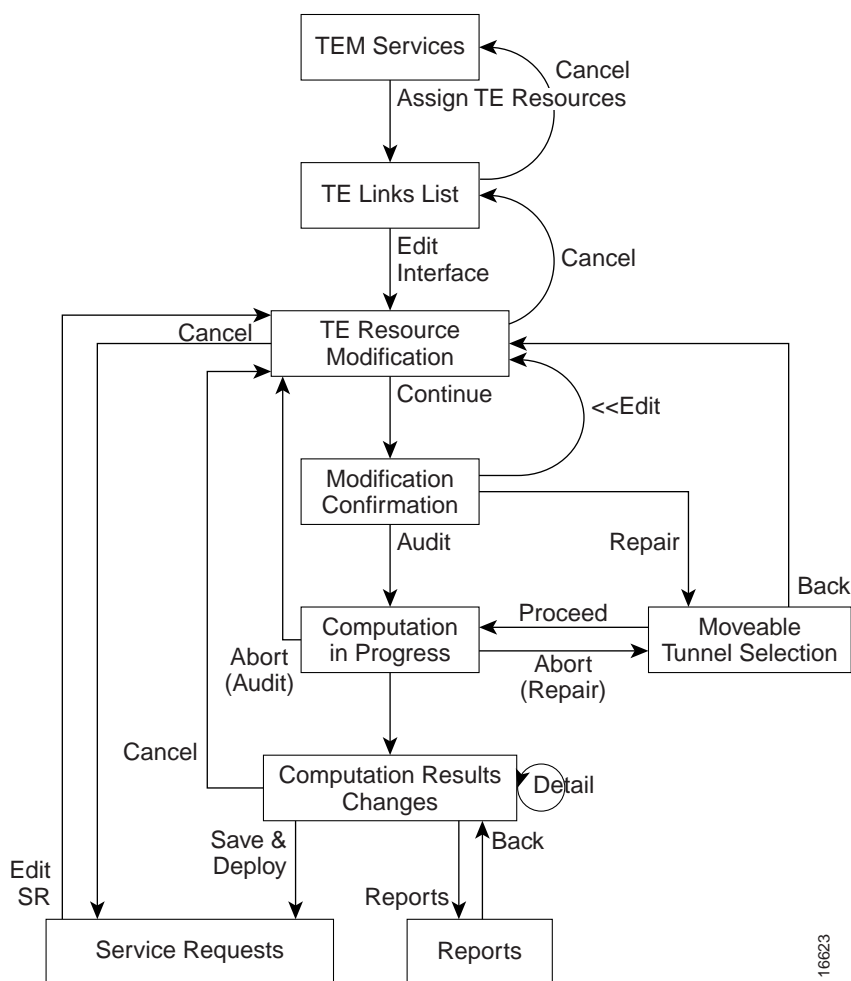
When a tunnel placement is attempted and there is insufficient bandwidth, sometimes the resources on the TE links can be changed and the tunnel placement retried.

Network resources in this context are understood to be routers in the TE network, the interfaces that connect them, and the RSVP bandwidths and other properties configured on the links. Since ISC TEM relies on the discovery process to add the network elements to the repository, the resources must be discovered before resource management can be performed.

TE resource management is a manual process that should be performed on an as needed basis. If the original configuration is already optimal, there is no need for the user to do any resource management tasks. If subsequent discovery unveils any discrepancy, or if you experience difficulty achieving desired results in protection planning or placing primary tunnels, adjustments on the resources may be warranted.

An overview of the resource management process is provided in [Figure 4-1](#).

**Figure 4-1** Resource Management Processes



## Modifying Network Resources

The resource management tasks are first of all carried out from the TE Links List window.



### Note

Certain attributes, such as Description, that do not impact the computation carried out by these tools and updates to these are, therefore, not displayed in the Computation Result Window.

To modify a TE link, use the following steps:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Assign TE Resources**.



The TE Links List window shown in [Figure 4-2](#) appears.

**Figure 4-2** TE Links List

#	End Device A	Type	Interface A	End Device B	Type	Interface B	Label	Admin Status
1.	isctmp11	CISCO_ROUTER	POS0/2/0/0	isctmp12	CISCO_ROUTER	POS0/3/0/0	10.2.4.10<->10.2.4.9	UP
2.	isctmp11	CISCO_ROUTER	POS0/3/0/1	isctmp12	CISCO_ROUTER	POS0/1/0/1	10.2.4.14<->10.2.4.13	UP
3.	isctmp11	CISCO_ROUTER	POS0/0/0/0	isctmp8	CISCO_ROUTER	POS5/0	10.2.4.6<->10.2.4.5	UP
4.	isctmp10	CISCO_ROUTER	POS0/2/0/0	isctmp12	CISCO_ROUTER	POS0/4/0/0	10.2.4.22<->10.2.4.21	UP
5.	isctmp12	CISCO_ROUTER	GigabitEthernet0/2/0/0	isctmp7	CISCO_ROUTER	GigabitEthernet5/0	10.2.4.29<->10.2.4.30	UP

For an explanation of the various window elements, see [TE Links, page A-21](#).

The links list shows the current active links in the TE network. Use the arrows to page forward as needed.

**Step 2** Select the desired link in the links list.

**Step 3** Click **Edit > Interface A** or **Edit > Interface B** to edit one of interfaces on the link.



**Note** If a non-Cisco interface is selected for editing, changes made in the Edit window will be saved in the ISC repository but they will not be deployed.

**Step 4** The TE Resource Modification window appears as shown in [Figure 4-3](#).

Figure 4-3 TE Resource Modification

TE Resource Modification

SR Job ID: New		Provider: Provider2	SR ID: New
SR State: REQUESTED		Creator:	Type: ADD
Device/Interface:	isctmp11 : POS0/2/0/0		
Peer Device/Interface:	isctmp12 : POS0/3/0/0		
Description:	<div></div>		
Link Bandwidth (Kbps):	2488320		
Max Global (BC0) Reservable (Kbps) *:	45000		
Max Sub Pool (BC1) Bandwidth (Kbps) *:	30000		
Attribute Bits (0x0-0xFFFFFFFF) *:	0x0		
TE Metric *:	2000		
Propagation Delay *:	0		
Max Delay Increase *:	0		
Link Speed Factor *:	1.0		
		Continue >>	Cancel

Note: \* - Required Field

138921

For an explanation of the various fields, see [TE Links](#), page A-21.

- Step 5
- Make the desired modifications and click **Continue >>** to proceed to the confirmation page as shown in [Figure 4-4](#) to verify the changes or click **Cancel** to quit without saving.

Figure 4-4 TE Resource Modification (Confirmation Page)

TE Resource Modification	
SR Job ID: New	Provider: Provider2
SR State: REQUESTED	Creator:
SR ID: New	Type: ADD
Device/Interface:	isctmp11 : POS0/2/0/0
Peer Device/Interface:	isctmp12 : POS0/3/0/0
Description	
Link Bandwidth (Kbps):	2488320
Max Global (BC0) Reservable (Kbps) *	45000
Max Sub Pool (BC1) Bandwidth (Kbps) *	30000
Attribute Bits (0x0-0xFFFFFFFF) *	0x0
TE Metric *	2000
Propagation Delay *	0
Max Delay Increase *	0
Link Speed Factor *	1.0
<input data-bbox="867 919 948 947" type="button" value=" &lt;&lt; Edit "/> <input data-bbox="964 919 1208 947" type="button" value=" Proceed with Changes &gt;&gt; "/> <input data-bbox="1224 919 1386 947" type="button" value=" Save &amp; Deploy "/>	
Note: * - Required Field	

**Step 6** Click << Edit to return to the editable window or proceed in one of the following ways:

- **Proceed with Changes >>** (Figure 4-5)—Perform Tunnel Audit or Tunnel Repair.

For a detailed explanation of Tunnel Audit and Tunnel Repair, see [Chapter 6, “Advanced Primary Tunnel Management.”](#)

If a non-Cisco device is edited, **Proceed with Changes >>** will be disabled. Instead, **Save & Deploy** is enabled and the changes can be saved (not deployed).

- **Save & Deploy** (Figure 4-6)—If the changes made do not affect tunnel placement, click **Save & Deploy** to proceed. In this case, there is no need for performing Tunnel Audit or Tunnel Repair.

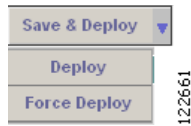


#### Note

When you click Save & Deploy, a background process is started. To avoid a potential conflict with another deployment, wait until the SR has completed the Requested and Pending states before deploying another SR with Save & Deploy. To see the state of deployment, go to the Service Requests window under **Inventory and Connection Manager > Service Requests** or open **Monitoring > Task Manager**.

Figure 4-5 TE Links List - Proceed with Changes

Proceed with Changes >> ▼
Tunnel Audit
Tunnel Repair

**Figure 4-6 Save & Deploy Tunnels**

For an explanation of the options available under **Proceed with Changes >>** and **Save & Deploy**, see [Edit Interface, page A-27](#)



**Note** In ISC TEM, service requests (SRs) are generally deployed from each TE service, not from the **Service Requests** page in **Inventory and Connection Manager** with the exception of the TE Traffic Admission SR.

After deployment, the SR status can be viewed from the SR window at **Service Inventory > Inventory and Connection Manager > Service Requests**.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

If the SR does not go to the **Deployed** state, go to the Task Log to see the deployment log (**Monitoring > Task Manager > Logs**). Task logs are further described in [TE Task Logs, page 10-1](#).

## Change Link Status

From the TE Links List window ([Figure 4-2](#)), you can also find out what effect it will have if a link is taken offline. This approach can be used to move tunnels off a link before actually shutting down the interface.



**Note** Link status in ISC TEM is of local significance. Changing link status as described in this section is not provisioned down to the network.

To change the link status, use the following steps:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Assign TE Resources**.  
The TE Links List window appears.
- Step 2** Select one or more links and click the **Change Status** button as shown in [Figure 4-7](#).

**Figure 4-7** Change Link Status

**TE Links List**

TE Provider Provider2

Show TE Links with  matching

Showing 1 - 5 of 35 records

#	<input type="checkbox"/>	End Device A	Type	Interface A	End Device B	Type	Interface B	Label	Admin Status
1.	<input checked="" type="checkbox"/>	isctmp11	CISCO_ROUTER	POS0/2/0/0	isctmp12	CISCO_ROUTER	POS0/3/0/0	10.2.4.10<->10.2.4.9	UP
2.	<input type="checkbox"/>	isctmp11	CISCO_ROUTER	POS0/3/0/1	isctmp12	CISCO_ROUTER	POS0/1/0/1	10.2.4.14<->10.2.4.13	UP
3.	<input type="checkbox"/>	isctmp11	CISCO_ROUTER	POS0/0/0/0	isctmp8	CISCO_ROUTER	POS5/0	10.2.4.6<->10.2.4.5	UP
4.	<input type="checkbox"/>	isctmp10	CISCO_ROUTER	POS0/2/0/0	isctmp12	CISCO_ROUTER	POS0/4/0/0	10.2.4.22<->10.2.4.21	UP
5.	<input type="checkbox"/>	isctmp12	CISCO_ROUTER	GigabitEthernet0/2/0/0	isctmp7	CISCO_ROUTER	GigabitEthernet5/0	10.2.4.29<->10.2.4.30	UP

Rows per page:   Go to page:  of 7

For an explanation of the various window elements, see [TE Links](#), page A-21.

**Step 3** Select **Enable** or **Disable** to enable or disable the selected link.

**Step 4** As an example, selecting **Disable** will change the link status to **DOWN** as shown in [Figure 4-8](#).

**Figure 4-8** Link Status Down

1.	<input checked="" type="checkbox"/>	isctmp11	CISCO_ROUTER	POS0/2/0/0	isctmp12	CISCO_ROUTER	POS0/3/0/0	10.2.4.10<->10.2.4.9	DOWN
----	-------------------------------------	----------	--------------	------------	----------	--------------	------------	----------------------	------

Similarly, use **Enable** to change the status back to **UP**.

**Step 5** Click **Proceed with Changes >>** to assess any impact on tunnel placement using Tunnel Audit or Tunnel Repair and deploy the changes (see [Figure 4-9](#)).

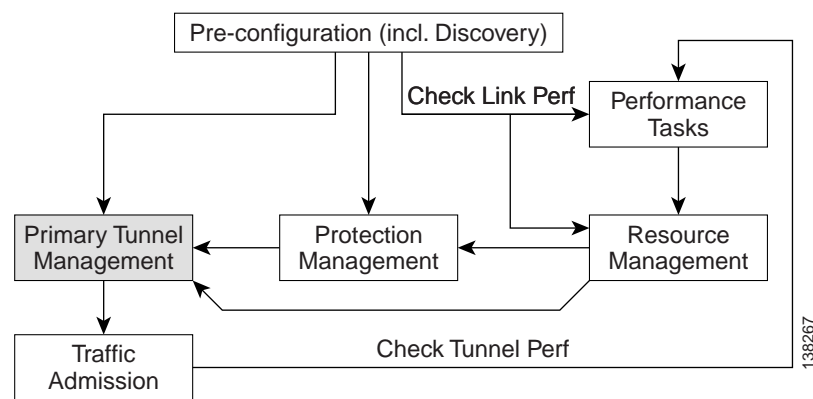
**Figure 4-9** TE Links List - Proceed with Changes

For a detailed explanation of Tunnel Audit and Tunnel Repair, see [Chapter 6, “Advanced Primary Tunnel Management.”](#)





## Basic Tunnel Management



This chapter describes the processes involved in creating primary and backup tunnels with ISC TEM. To create a tunnel, certain steps must first be performed as described in previous chapters.

This chapter includes the following sections:

- [Overview, page 5-2](#)
- [Create TE Policy, page 5-2](#)
- [Create Explicit Path, page 5-4](#)
- [Primary Tunnel Operations, page 5-8](#)
  - [Create Primary Tunnel, page 5-8](#)
  - [Edit Primary Tunnel, page 5-16](#)
  - [Delete Primary Tunnel, page 5-19](#)
- [Backup Tunnel Operations, page 5-20](#)
  - [Create Backup Tunnel, page 5-20](#)
  - [Edit Backup Tunnel, page 5-24](#)
  - [Delete Backup Tunnel, page 5-26](#)

# Overview

Primary tunnels are characterized by carrying traffic during normal operation. They have a prioritized list of possible paths, by which traffic can be routed. At any one time, the highest priority path available will be used to route traffic. If this fails, traffic will normally be re-routed via the next available path until a higher priority path becomes available again.

Prior to setting up the tunnel, a TE policy governing the traffic must be defined. An explicit path is created to establish the route and, in the case of a primary tunnel, it is created as either a managed or an unmanaged tunnel.

The purpose of a backup tunnel is to carry FRR protected traffic around a failed element until the routing in the network has reconverged. It is intended to protect traffic travelling along primary tunnels. There can be many backup tunnels protecting the same traffic through the use of load balancing.

If the network fails to reconverge, the backup tunnel will remain in place.

The difference between managed and unmanaged tunnels is described in [Managed/Unmanaged Primary Tunnels, page 1-3](#).

The concept of bandwidth pools from which tunnels reserve bandwidth is important to understand. This is described in [Bandwidth Pools, page 1-5](#).

## Create TE Policy

To create a primary tunnel, each primary tunnel must be associated with a policy. A policy can be used by multiple tunnels.

For backup tunnels, this step is not necessary. In this case, proceed to [Create Explicit Path, page 5-4](#).

For other TE policy management operations, see [TE Policies, page 9-2](#).

The TE policy is a set of rules governing the TE network and defines the Class-of-Service (for example, gold, silver, bronze) for primary tunnel traffic.

ISC TEM has a notion of **Managed** and **Unmanaged** policies. **Managed** policies have setup/hold priorities of 0/0 and can have additional pathing constraints such as protection level and max delay. Tunnels with **Unmanaged** policies are provisioned by the system, but the system only tracks the deployment, not the operation of the tunnel. **Unmanaged** policies cannot have a setup/hold priority of zero.

Policies are managed under **Policy Manager** in **Service Design**. For a more detailed explanation of the **Policy Manager** GUI, see [TE Policies, page 9-2](#).

To create a TE policy, use the following steps:

---

**Step 1**    Navigate to **Service Design > Policy Manager**.

**Step 2**    Click the **Policy Manager** icon.

The Policies window in [Figure 5-1](#) appears.



Figure 5-1 Policies Window

The screenshot shows the Cisco IP Solution Center interface. The top navigation bar includes links for Home, Shortcuts, Account, Index, Help, About, and Logout. The main menu has tabs for Service Inventory, Service Design, Monitoring, Diagnostics, and Administration. The 'Policies' tab is selected, and the 'Create' button is highlighted. The 'Policies' window displays a table of existing policies.

#	Policy Name	Type	Owner
11.	ISC-P1-iscmp11:tunnel-te2	TE	Provider - Provider2
12.	ISC-P122-iscmp11:tunnel-te1003	TE	Provider - Provider2
13.	ISC-P126-iscmp10:tunnel-te1003	TE	Provider - Provider2
14.	ISC-P2-iscmp11:tunnel-te1000	TE	Provider - Provider2
15.	L2VpnPolicy1	L2VPN	Global
16.	L2VpnPolicy2	L2VPN	Global
17.	MPLSPolicy_PECE	MPLS	Customer - Customer1
18.	MPLSPolicyNO_CE	MPLS	MPLS Policy ner1
19.	VPLSPolicy1	VPLS	L2VPN (P2P) Policy
20.	VPLSPolicy2	VPLS	VPLS Policy

At the bottom of the table, there are buttons for 'Create', 'Edit', 'Copy', and 'Delete'. The 'Create' button is highlighted. The 'Rows per page' is set to 10, and the 'Page' is 2 of 2.

**Step 3** Click **Create** and select **TE Policy** to set up a new TE policy.

To edit an existing policy, select the policy that you want to modify and click **Edit**. The TE Policy Editor window in Figure 5-2 appears.



**Note** A policy that is being used by a tunnel cannot be modified.

**Figure 5-2** *TE Policy Editor*

TE Policy Editor

Policy Name \* :  (1 - 64 characters)

Owner \* :

Managed: ☐

Pool Type: ☐ Sub Pool (BC1) ☒ Global Pool (BC0)

Setup Priority \* :

Hold Priority \* :

Affinity (0x0-0xFFFFFFFF):

Affinity Mask (0x0-0xFFFFFFFF):

FRR Protection Level: ☒ None ☐ Best Effort

Note: \* - Required Field

122718

For an explanation of the various window elements, see [TE Policies, page 9-2](#).

- Step 4** Fill in the required fields marked with an asterisk (\*) and any optional fields.

If you intend to use the TE policy for managed tunnels, make sure to check the **Managed** check box. When setting up a policy for a managed tunnel, the **Setup** and **Hold** priorities are automatically set to zero (highest priority). In the case of a policy for an unmanaged tunnel, you can specify the desired **Setup** and **Hold** priority settings.

- Step 5** Click **Save**.

## Create Explicit Path

This section describes how to create a TE explicit path. For other TE explicit path operations, see [TE Explicit Paths, page A-33](#).

Paths are defined between source and destination routers, possibly with one or more hops in between. Paths are used for primary and backup tunnels in the explicit path option(s).

If you intend to create an explicit path for managed tunnels, the path should not contain any non-TE enabled interfaces. Paths with non-TE enabled interfaces will be filtered out by the tunnel path chooser of the tunnel editor for managed tunnels and backup tunnels (not unmanaged tunnels).

To create or edit an explicit path, use the following steps:

- Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2** Click **TE Explicit Paths**. The TE Explicit Path List window appears. (see [Figure 5-3](#))

Figure 5-3 TE Explicit Path List

**IP Solution Center**

Service Inventory | Service Design | Monitoring | Diagnostics | Administration

User: admin

Inventory and Connection Manager | Discovery | Device Console

You Are Here: Service Inventory > Inventory and Connection Manager > Traffic Engineering Management

Customer: None

**TE Explicit Path List**

Provider: Provider2

Show Paths with All matching \* Find

Showing 11 - 15 of 67 records

#	<input type="checkbox"/>	Path Name	Head	Dest
11.	<input type="checkbox"/>	isctmp1-isctmp5-1	isctmp1	isctmp5
12.	<input type="checkbox"/>	isctmp1-isctmp6-1	isctmp1	isctmp6
13.	<input type="checkbox"/>	isctmp1-isctmp8-1	isctmp1	isctmp8
14.	<input type="checkbox"/>	isctmp10-isctmp1-1	isctmp10	isctmp1
15.	<input type="checkbox"/>	isctmp10-isctmp6-1	isctmp10	isctmp6

Rows per page: 5 Go to page: 3 of 14 Go

Create Edit Delete

For an explanation of the various window elements, see [Create/Edit Explicit Path, page A-34](#).

**Step 3** To create an explicit path in the **TE Explicit Path List**, click **Create**. The New TE Explicit Path window in [Figure 5-4](#) appears.

To edit an explicit path in the explicit path list, select the explicit path that you want to modify and click **Edit**. The TE Explicit Path Editor window in [Figure 5-5](#) appears.



**Note** An explicit path that is being used by a tunnel cannot be modified. However, use Edit to view the path.

Figure 5-4 New TE Explicit Path

**New TE Explicit Path**

Path Name \*:

Head Router \*:

Links:

Showing 0 of 0 records

#	<input type="checkbox"/>	Device	Outgoing Interface	Outgoing IP	Next Hop	Incoming Interface	Incoming IP
Rows per page: 10 <input type="button" value="Go"/> of 1 <input type="button" value="Go"/>							
<input type="button" value="Add Link"/> <input type="button" value="Delete Link"/>							

Provision Preference \*: Outgoing Interface ☒ Incoming Interface ☐

Note: \* - Required Field

122643

Figure 5-5 TE Explicit Path Editor

**TE Explicit Path Editor**

Path Name \*: isctmp1->isctmp3-2

Head Router \*: isctmp1

Links:

Showing 0 of 0 records

#	<input type="checkbox"/>	Device	Outgoing Interface	Outgoing IP	Next Hop	Incoming Interface	Incoming IP
1.	<input type="checkbox"/>	isctmp1	FastEthernet2/1/1	10.2.3.57	isctmp9	FastEthernet2/1	10.2.3.58
2.	<input type="checkbox"/>	isctmp9	POS5/0	10.2.3.69	isctmp3	POS5/0	10.2.3.70
Rows per page: 10 <input type="button" value="Go"/> of 1 <input type="button" value="Go"/>							
<input type="button" value="Add Link"/> <input type="button" value="Delete Link"/>							

Provision Preference \*: Outgoing Interface ☒ Incoming Interface ☐

Note: \* - Required Field

122698

For an explanation of the various window elements, see [Create/Edit Explicit Path](#), page A-34 and [Edit TE SR \(Primary or Backup\)](#), page A-52.

**Note**

If a path is used by any tunnel, no modifications are possible. The **Outgoing Interface** and **Incoming Interface** links are not selectable and the Provision Preference line and the **Add Link**, **Delete Link**, and **Save** buttons disappear.

- Step 4** Specify a path name and select a head router.
- Step 5** Click **Add Link**. A blank line is added to the hop list table.
- Step 6** Now an outgoing or an incoming interface must be selected for the head router. Under **Incoming Interface** or **Outgoing Interface**, click **Add Interface**. The Select Next Hop window in [Figure 5-6](#) appears.

**Figure 5-6** Select Next Hop

#	Outgoing Interface	Outgoing IP	Next Hop	Type	Incoming Interface	Incoming IP
1.	<input type="radio"/> FastEthernet2/0/1	10.2.2.145	isctmp2	CISCO_ROUTER	FastEthernet1/0	10.2.2.158
2.	<input type="radio"/>		isctmp2	CISCO_ROUTER	Loopback0	192.168.118.189
3.	<input type="radio"/> FastEthernet2/1/0	10.2.3.54	isctmp9	CISCO_ROUTER	FastEthernet2/0	10.2.3.53
4.	<input type="radio"/>		isctmp9	CISCO_ROUTER	Loopback0	192.168.118.219
5.	<input type="radio"/> FastEthernet2/1/1	10.2.3.57	isctmp9	CISCO_ROUTER	FastEthernet2/1	10.2.3.58
6.	<input type="radio"/> FastEthernet1/0/0	10.2.2.161	isctmp8	CISCO_ROUTER	FastEthernet3/0	10.2.2.174
7.	<input type="radio"/>		isctmp8	CISCO_ROUTER	Loopback0	192.168.118.183
8.	<input type="radio"/> FastEthernet1/1/0	10.2.2.110	isctmp7	CISCO_ROUTER	FastEthernet0/0	10.2.2.97
9.	<input type="radio"/>		isctmp7	CISCO_ROUTER	Loopback0	192.168.118.214
10.	<input type="radio"/> FastEthernet3/1/0	10.2.3.93	isctmp7	CISCO_ROUTER	FastEthernet4/0	10.2.3.94

Rows per page: 10 Go to page: 1 of 2

Select Cancel

The next hop list contains all the possible next hops of the router, excluding the ones already included in the explicit paths (to avoid path loops).

The next hop list contains TE interfaces and at most one non-TE interface for each router (if the loopback interface is used as the MPLS TE ID of the device). For TE interfaces, the **Outgoing Interface** and **Outgoing IP** columns are populated by the application.

**Note**

If a non-TE interface is selected, **Provision Preference** ([Figure 5-4](#)) is set to **Incoming Interface**. The provision preference cannot be set manually.

- Step 7** Select an interface and click **Select**. The corresponding link information is added to the new explicit path in the **Links** table as shown in [Figure 5-7](#).

The incoming interface field is automatically populated.

**Figure 5-7**      **New Link for TE Explicit Path**

**New TE Explicit Path**

Path Name \*: new\_path

Head Router \*: isctmp3 Select

Links:

Showing 0 of 0 records

#	Device	Outgoing Interface	Outgoing IP	Next Hop	Incoming Interface	Incoming IP
1.	isctmp3	FastEthernet0/1	10.2.2.241	isctmp4	Ethernet5/5	10.2.2.254

Rows per page: 10 Go to page: 1 of 1 Go

Add Link Delete Link

Provision Preference \*: Outgoing Interface Incoming Interface

Save Cancel

Note: \* - Required Field

- Step 8** To add another link, click **Add Link** again.
- Step 9** To modify an existing link, click the link in the **Outgoing Interface** or the **Incoming Interface** columns, make the desired changes, and click **Select**.
- Step 10** Optionally, select **Provision Preference** by clicking either the **Outgoing Interface** or the **Incoming Interface** radio button.



**Note** If you try to select the **Provision Preference** before adding a link when non-TE interfaces are present, the **Add Link** process overrides the **Provision Preference** and sets it to incoming.

- Step 11** Click **Save** to keep the created TE explicit path or click **Cancel** to quit without saving.

## Primary Tunnel Operations

ISC TEM allows you to perform a number of primary tunnel operations, which are described in the following.

### Create Primary Tunnel

After a TE Policy and an explicit path have been set up, a primary tunnel can be created. There are two types of primary tunnels:

- Managed Primary Tunnels
- Unmanaged Primary Tunnels

Below, the GUI flow is described for creating unmanaged primary tunnels. It is very similar for managed primary tunnels and the few differences that exist are described in [Managed/Unmanaged Primary Tunnels, page 1-3](#) and [Create Unmanaged TE Tunnel, page A-59](#).

To create a managed or an unmanaged primary tunnel, use the following steps:

- Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2** Click **Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window in [Figure 5-8](#) appears.
- or
- Click **Create Unmanaged TE Tunnel**. The TE Unmanaged Primary Tunnels SR window in [Figure 5-9](#) appears.

**Figure 5-8** TE Managed Primary Tunnels SR

**TE Managed Primary Tunnels SR**

SR Job ID: 8      Provider: Provider2      SR State: REQUESTED  
 SR ID: New      Creator:      Type: ADD

Description:

Show Existing Tunnels with All matching \* Find

Showing 1 - 5 of 23 records

#	Op	Tunnel ID	T#	Head	Dest	Policy	BW	AutoBW	Deploy Status	Verified	Allow Reroute
1.	<input type="checkbox"/>	ISC-P1	2	isctmp11	isctmp10	ISC-P1-isctmp11:tunnel-te2	2	false	LOST	succeed	false
2.	<input type="checkbox"/>	ISC-P2	1000	isctmp11	isctmp1	ISC-P2-isctmp11:tunnel-te1000	200	false	LOST	succeed	false
3.	<input type="checkbox"/>	ISC-P122	1003	isctmp11	isctmp12	ISC-P122-isctmp11:tunnel-te1003	500	false	DEPLOYED	succeed	false
4.	<input type="checkbox"/>	ISC-P123	1004	isctmp11	isctmp8	ISC-P122-isctmp11:tunnel-te1003	500	false	DEPLOYED	succeed	false
5.	<input type="checkbox"/>	ISC-P3	1	isctmp10	isctmp6	ISC-P2-isctmp11:tunnel-te1000	1000	false	DEPLOYED	succeed	false

Rows per page: 5      Go to page: 1 of 5 Go

Close Display Details Admit Create Edit Delete

Import Placement Tools Proceed with Changes >> Save & Deploy Cancel

138930

Figure 5-9 TE Unmanaged Primary Tunnels SR

**TE Unmanaged Primary Tunnels SR**

SR Job ID: 1      Provider: pad0      SR State: REQUESTED  
 SR ID: Neww      Creator:      Type: ADD

Description:

Show Existing Tunnels with All Matching \* Find

Showing 1 - 2 of 2 records

#	Op	Tunnel ID	T#	Head	Dest	Policy	BW	AutoBW	Deploy Status	Conformance
1.	<input type="checkbox"/>	ISC-P1	3	isctmp1	isctmp6	ISC-P1-isctmp1:Tunnel3	56	false	DEPLOYED	Yes
2.	<input type="checkbox"/>	ISC-P41	1	isctmp1	isctmp2	unman	44	false	DEPLOYED	Yes

Rows per page: 10 Go to page: 1 of 1 Go

Close Display Details Create Edit Delete

Save & Deploy Cancel

122770

For an explanation of the various window elements, see [Create Managed TE Tunnel, page A-41](#).

Note that for the unmanaged tunnels list, the last two columns in the managed tunnels list in [Figure 5-8](#) (Verified and Allow Reroute) are replaced by the Conformance column.

In this example, we will create an unmanaged tunnel.

- Step 3** Click **Create**. The Create TE Unmanaged Primary Tunnel window in [Figure 5-10](#) appears.



**Figure 5-10** Create TE Unmanaged Primary Tunnel

**Create TE Unmanaged Primary Tunnel**

<b>SR Job ID:</b> New	<b>SR ID:</b> New	<b>SR State:</b> REQUESTED
<b>Tunnel ID:</b>	<b>Creator:</b>	<b>Type:</b> ADD
Head Device *:	<input type="text"/>	<input type="button" value="Select"/>
Destination Device *:	<input type="text"/>	<input type="button" value="Select"/>
TE Policy *:	<input type="text"/>	<input type="button" value="Select"/>
Tunnel Bandwidth (kbps):	<input type="text"/>	
Tunnel Number:	Auto Gen <input checked="" type="checkbox"/>	<input type="text"/>
Customer:	<input type="text"/>	
Auto BW:	Enable: <input type="checkbox"/> Freq (sec): <input type="text"/> Min (kbps): <input type="text"/> Max (kbps): <input type="text"/>	
<b>Path Options:</b>		
Showing 0 of 0 records		
<input type="checkbox"/>	Option #	Path Name Path Type Lock Down
Rows per page: 10 Go to page: 1 of 1 <input type="button" value="Go"/>		
		<input type="button" value="Add"/> <input type="button" value="Delete"/>
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Note: \* - Required Field

129259

For an explanation of the various window elements, see [Create Managed TE Tunnel, page A-41](#) and [Create Unmanaged TE Tunnel, page A-59](#).

- Step 4** To select a **Head Device** in the Create TE Unmanaged Primary Tunnel window, click the corresponding **Select** button to open the Select Device for TE Head Router window shown in [Figure 5-11](#).

Figure 5-11 Select Device for TE Head Router

Device for **TE Head Router**

Show Devices with:  matching

Showing 1 - 5 of 14 records

#	Device Name	IGP ID	MPLS TE ID	Admin Status
1.	<input type="radio"/> isctmp1	192.168.118.176	192.168.118.176	UP
2.	<input type="radio"/> isctmp11	192.168.118.166	192.168.118.166	UP
3.	<input type="radio"/> isctmp10	192.168.118.167	192.168.118.167	UP
4.	<input type="radio"/> isctmp12	192.168.118.168	192.168.118.168	UP
5.	<input type="radio"/> isctmp13	192.168.118.171	192.168.118.171	UP

Rows per page:

For an explanation of the various window elements, see [Create Managed TE Tunnel, page A-41](#) and [Create Unmanaged TE Tunnel, page A-59](#).

- Step 5** Select a device name and click **Select**. The Select Device for TE Head Router window closes and the prompt returns to the Create TE Unmanaged Primary Tunnel window.
- Step 6** To select a **Destination Device** in the Create TE Unmanaged Primary Tunnel window, click the corresponding **Select** button to open the Select Device for TE Tail Router window shown in [Figure 5-12](#).

Figure 5-12 Select Device for TE Tail Router

Device for **TE Tail Router**

Show Devices with:  matching

Showing 1 - 5 of 15 records

#	Device Name	IGP ID	MPLS TE ID	Admin Status
1.	<input type="radio"/> 192.168.118.178	192.168.118.178	192.168.118.178	UP
2.	<input type="radio"/> isctmp1	192.168.118.176	192.168.118.176	UP
3.	<input type="radio"/> isctmp11	192.168.118.166	192.168.118.166	UP
4.	<input type="radio"/> isctmp10	192.168.118.167	192.168.118.167	UP
5.	<input type="radio"/> isctmp12	192.168.118.168	192.168.118.168	UP

Rows per page:

For an explanation of the various window elements, see [Create Managed TE Tunnel, page A-41](#) and [Create Unmanaged TE Tunnel, page A-59](#).

- Step 7** Select a device name and click **Select**. The Select Device for TE Tail Router window closes and the prompt returns to the Create TE Unmanaged Primary Tunnel window.

- Step 8** To select a **Tunnel Policy** in the Create TE Unmanaged Primary Tunnel window, click the corresponding **Select** button to open the Select Unmanaged TE Tunnel Policy window shown in [Figure 5-13](#).

**Note**

To create a managed tunnel, make sure that one or more managed tunnel policies are available. If that is not the case, go to **Policy Manager** (see [Create TE Policy, page 5-2](#)) and make sure to check the **Managed** check box.

**Figure 5-13** Select Unmanaged TE Tunnel Policy

#	Policy Name	Pool Type	Setup Priority	Hold Priority	Affinity	Affinity Mask	FRR Protection
1.	um1	GLOBAL	1	1	0x0	0xFFFF	None
2.	um2	GLOBAL	2	2	0x0	0xFFFF	None

Rows per page: 10 Go to page: 1 of 1 **Go**

**Select** **Cancel**

For an explanation of the various window elements, see [Create Managed TE Tunnel, page A-41](#) and [Create Unmanaged TE Tunnel, page A-59](#).

- Step 9** Select a policy and click the **Select** button. This brings you back to the tunnel editor.
- Step 10** Click **Add** to set up path options for the tunnel. The Select TE Explicit Path window in [Figure 5-14](#) appears.

The **Path Options** section provides two path types, **Explicit Path** and **Dynamic Path**.

An **Explicit Path** is a fixed path from a specific head to a specific destination device.

A **Dynamic Path** is provisioned by allowing the head router to find a path. The **dynamic** keyword is provisioned to the routers.

**Figure 5-14** Select TE Explicit Path

#	Path Name	Head	Dest
1.	Dynamic		

Rows per page: 10 Go to page: 1 of 1 **Go**

**Select** **Cancel**

For unmanaged tunnels, paths can be either explicit or dynamic.

- Step 11** Select the desired TE Explicit Path unless you prefer dynamic path only. If none is available, you can set one up first. To do so, see [Create Explicit Path, page 5-4](#).

Click **Select**.

The selected path appears in the **Path Options** section of the create window as shown in [Figure 5-15](#).

**Figure 5-15** Path Options

Path Options:				
Showing 1 - 2 of 2 records				
<input type="checkbox"/>	Option #	Path Name	Path Type	Lock Down
<input checked="" type="checkbox"/>	1	isctmp11-isctmp10-1	Explicit	<input type="checkbox"/>
<input type="checkbox"/>	2	Dynamic Path	Dynamic	<input type="checkbox"/>

Rows per page: 10 Go to page: 1 of 1

For explicit paths (<head\_device>-<destination\_device>), you can click the path name to open the non-editable Explicit Path Viewer as shown in [Figure 5-16](#).

**Figure 5-16** TE Explicit Path Viewer

Path Name \*: isctmp11-isctmp10-1

Head Router \*: isctmp11

Links:

Showing 1 - 2 of 2 records							
#	Device	Outgoing Interface	Outgoing IP	Next Hop	Type	Incoming Interface	Incoming IP
1.	isctmp11	POS0/3/0/1	10.2.4.14	isctmp12	CISCO_ROUTER	POS0/1/0/1	10.2.4.13
2.	isctmp12	POS0/4/0/0	10.2.4.21	isctmp10	CISCO_ROUTER	POS0/2/0/0	10.2.4.22

Rows per page: 10 Go to page: 1 of 1

Provision Preference \*: Outgoing Interface Incoming Interface

Close

Note: \* - Required Field

For an explanation of the various window elements, see [Create/Edit Explicit Path, page A-34](#).

- Step 12** In the Create TE Unmanaged Tunnel window, click **OK** to accept the entered tunnel information or click **Cancel** to quit and return to the TE Unmanaged Primary Tunnels SR window.
- Step 13** The TE Unmanaged Primary Tunnel SR window appears with the newly created SR ([Figure 5-17](#)) with the Op field set to ADD.



**Note**

The added tunnel can be reverted from the ADD state to its original state by selecting it and clicking **Delete**. The tunnel is removed from the tunnel list.

Figure 5-17 Service Requests - Unmanaged Tunnels

**TE Unmanaged Primary Tunnels SR**

SR Job ID: 8      Provider: Provider2      SR State: REQUESTED  
 SR ID: New      Creator:      Type: ADD

Description:

Show  Tunnels with  matching

Showing 1 - 1 of 1 record

#	<input type="checkbox"/>	Op	Tunnel ID	T#	Head	Dest	Policy	BW	AutoBW	Deploy Status	Conformance
1.	<input type="checkbox"/>	ADD	ISC-P151		isctmp11	isctmp10	te_policy1	100000	false	REQUESTED	Yes

Rows per page:       Go to page:  of 1

138935

- Step 14** In the TE Unmanaged Primary Tunnel window, click **Save & Deploy** (see [Note](#) on page 15) to either deploy the new tunnel SR to the network or force deploy all tunnels, or you can create or edit more primary tunnels and then save and deploy all changes.

When you click Save & Deploy, a background process is started. To avoid a potential conflict with another deployment, wait until the SR has completed the Requested and Pending states before deploying another SR with Save & Deploy. To see the state of deployment, go to the Service Requests window at **Inventory and Connection Manager > Service Requests** or open **Monitoring > Task Manager**.

For a further description of save and deploy options, see [Create Managed TE Tunnel, page A-41](#).

**Note**

For managed tunnels, you cannot deploy the service request until you have used the **Proceed with Changes >>** button to perform either Tunnel Placement, Tunnel Audit, or Tunnel Repair (see [Chapter 6, "Advanced Primary Tunnel Management"](#)).

**Note**

With the exception of TE Traffic Admission SRs, TE SRs are always deployed immediately from the specific TE SR window, not from **Inventory and Connection Manager > Service Requests**.

- Step 15** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears (see [Figure 5-18](#)) and displays the state of the deployed SR (first REQUESTED, then PENDING, then DEPLOYED, if successful).

**Figure 5-18** Service Requests - Unmanaged Tunnels

**Service Requests**

Show Services with Job ID  matching \*  of Type All

Showing 6 - 10 of 15 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
6.	6	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy1	10/19/05 3:29 PM	
7.	7	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy2	10/19/05 3:29 PM	
8.	8	REQUESTED	TE Tunnel	MODIFY	admin			11/6/05 4:15 PM	
9.	9	DEPLOYED	TE Protection	MODIFY	admin			11/2/05 3:54 PM	
10.	10	DEPLOYED	TE Admission	ADD	admin			10/20/05 6:01 PM	tunnel-te1 : CISCO ISC-P55

Rows per page: 5

Auto Refresh: ☒

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

If the SR does not go to the **Deployed** state, go to the Task Logs window to see the deployment log (**Monitoring > Task Manager > Logs**) as described in [SR Deployment Logs, page 10-1](#).

To edit the service request from the **Service Requests** window, go back to the TE Managed Primary Tunnels SR or the TE Unmanaged Primary Tunnels SR window as described in [Edit Primary Tunnel, page 5-16](#).

## Edit Primary Tunnel

Primary tunnel attributes can be modified in the primary tunnel editor

There are two ways to access the primary tunnel editor:

- from the managed or unmanaged primary tunnels SR window or
- from the Service Requests window.

### Access from Primary Tunnel SR Window

To access the primary tunnel editor from the primary tunnel SR window (TE Managed Primary Tunnels SR or TE Unmanaged Primary Tunnels SR window) and edit a managed or an unmanaged primary tunnel, use the following steps:

- Step 1 Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2 Click **Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window appears .  
or  
Click **Create Unmanaged TE Tunnel**. The TE Unmanaged Primary Tunnels SR window in [Figure 5-9](#) appears.

- Step 3** To edit a tunnel SR, select the desired SR and click **Edit**. The Edit TE Managed Primary Tunnel or the Edit TE Unmanaged Primary Tunnel window in [Figure 5-19](#) appears.

**Figure 5-19** Edit TE Unmanaged Primary Tunnel

**Edit TE Unmanaged Primary Tunnel**

SR Job ID: 3      SR ID: 11      SR State: DEPLOYED  
Tunnel ID: ISC-P140      Creator: admin      Type: ADD

Head Device \*: isctmp5  
Destination Device \*: isctmp9  
TE Policy \*: te\_policy1 Select  
Tunnel Bandwidth (kbps): 150  
Tunnel Number: 3  
Customer:   
Auto BW:   
Enable: ☐   
Freq (sec):   
Min (kbps):   
Max (kbps):   
Path Options:   
Showing 1 - 1 of 1 record  

<input type="checkbox"/>	Option #	Path Name	Path Type	Lock Down
<input type="checkbox"/>	1	isctmp5->isctmp9-3	Explicit	<input type="checkbox"/>

Rows per page: 10      Go to page: 1 of 1 Go  
Add Delete  
OK Cancel  
Note: \* - Required Field

The primary tunnel editor is identical to that of the create primary tunnel GUI. For an explanation of the various window elements, see [Create Managed TE Tunnel, page A-41](#) and [Create Unmanaged TE Tunnel, page A-59](#).

- Step 4** Make the desired changes and click **OK** or **Cancel** to discard the changes.
- Step 5** In the TE Unmanaged Primary Tunnel SR window, the Op field changes to **MODIFY**.



**Note** The modified tunnel can be reverted to its original state by selecting it and clicking **Delete**. The **MODIFY** flag in the Op column disappears.

Click **Save & Deploy** (see [Note](#) on page 15) to either deploy the new tunnel SR to the network or force deploy all tunnels, or you can create or edit more primary tunnels and then save and deploy all changes.

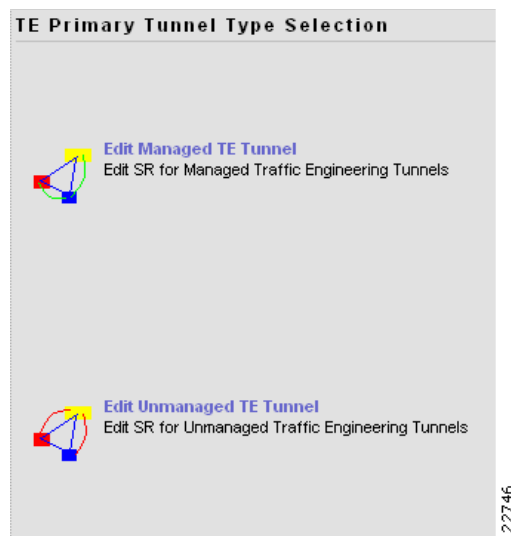
- Step 6** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears (see [Figure 5-18](#)) and displays the state of the deployed SR.
- For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)
- 

## Access from Service Requests Window

To access the primary tunnel editor from the Service Requests window, assuming that the SR has been created, use the following steps:

- Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Service Requests**.
- Step 2** To edit the desired tunnel SR, select the SR in question and click **Edit**. The TE Primary Tunnel Type Selection window in [Figure 5-20](#) appears.

**Figure 5-20** TE Primary Tunnel Type Selection



- Step 3** Specify the type of tunnel, managed or unmanaged. The TE Managed Primary Tunnel SR or the TE Unmanaged Primary Tunnel SR window appears displaying the SR selected in the Service Requests window. An example of the TE Unmanaged Primary Tunnel SR window is shown in [Figure 5-9](#).
- Step 4** Select the tunnel SR and click **Edit**. The Edit TE Unmanaged Primary Tunnel window in [Figure 5-19](#) appears.

Go to [Access from Primary Tunnel SR Window, page 5-16](#) and continue the process from [Step 4](#).

---



## Delete Primary Tunnel

To delete a managed or an unmanaged primary tunnel from the primary tunnel SR window (TE Managed Primary Tunnels SR or TE Unmanaged Primary Tunnels SR window), use the following steps:

- Step 1 Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2 Click **Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window appears .  
or  
Click **Create Unmanaged TE Tunnel**. The TE Unmanaged Primary Tunnels SR window in [Figure 5-9](#) appears.
- Step 3 To delete a tunnel, select the desired tunnel(s) and click **Delete**. The **Op** field status changes to **DELETE** as shown in [Figure 5-21](#).

**Figure 5-21** TE Unmanaged Primary Tunnels SR - Delete Requested

The screenshot shows the 'TE Unmanaged Primary Tunnels SR' window. At the top, it displays 'SR Job ID: 1', 'SR ID: New', 'Provider: pad0', 'Creator:', 'SR State: REQUESTED', and 'Type: ADD'. Below this is a 'Description:' field. A search bar shows 'Show Existing Tunnels with All Matching \*'. The table below shows two records. The first record is 'ISC-P1' with 'Op' as a checkbox. The second record is 'ISC-P41' with 'Op' as 'DELETE'. The table has columns: #, Op, Tunnel ID, T#, Head, Dest, Policy, BW, AutoBW, Deploy Status, and Conformance. At the bottom, there are buttons for 'Close', 'Display', 'Details', 'Create', 'Edit', 'Delete', 'Save & Deploy', and 'Cancel'.

#	Op	Tunnel ID	T#	Head	Dest	Policy	BW	AutoBW	Deploy Status	Conformance
1.	<input type="checkbox"/>	ISC-P1	3	isctmp1	isctmp6	ISC-P1-isctmp1:Tunnel3	56	false	DEPLOYED	Yes
2.	DELETE	ISC-P41	1	isctmp1	isctmp2	unman	44	false	REQUESTED	Yes

For an explanation of the various window elements, see [Create Managed TE Tunnel, page A-41](#) and [Create Unmanaged TE Tunnel, page A-59](#).



**Note** The deleted tunnel can be reverted to its original state by selecting it and clicking **Delete**. The DELETE flag in the Op column disappears.

Click **Save & Deploy** to either deploy the new tunnel SR to the network or force deploy all tunnels, or you can create or edit more primary tunnels and then save and deploy all changes.

- Step 4** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears (see [Figure 5-18](#)) and displays the state of the deployed SR.
- For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)
- 

## Backup Tunnel Operations

ISC TEM allows you to perform a number of backup tunnel operations, which are described in this section.

**Note**

Non-POS interfaces cannot be FRR protected on IOS-XR devices.

## Create Backup Tunnel

Backup tunnels are created in much the same way as primary tunnels. In both cases, building an explicit path is not required when an existing path already traverses the desired routers. A path can be used for any number of tunnels within its bandwidth capacity.

A precondition for creating a backup tunnel is the presence of an explicit path. To create an explicit path, see [Create Explicit Path, page 5-4](#).

To create a backup tunnel, use the following steps:

- 
- Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2** Click **Create TE Backup Tunnel**. The TE Protection SR window in [Figure 5-22](#) appears.

Figure 5-22 TE Protection SR

**Cisco Systems** IP Solution Center

Home | Shortcuts | Account | Index | Help | About | Logout

User: admin

Service Inventory Service Design Monitoring Diagnostics Administration

Inventory and Connection Manager Discovery Device Console

You Are Here: Service Inventory > Inventory and Connection Manager > Traffic Engineering Management Customer: None

**TE Protection SR**

SR Job ID: 9 Provider: Provider2 SR State: REQUESTED  
 SR ID: New Creator: Type: ADD

Description:

Show: Existing Tunnels with: All matching: Find

Showing 1 - 5 of 47 records

#	Op	Tunnel ID	T#	Head	Dest	BW Quota	Deploy Status	Conformance
1.	<input type="checkbox"/>	ISC-B30	3	isctmp11	isctmp12	2	LOST	Yes
2.	<input type="checkbox"/>	ISC-B31	1001	isctmp11	isctmp8	30000	LOST	Yes
3.	<input type="checkbox"/>	ISC-B141	1002	isctmp11	isctmp8	30000	DEPLOYED	Yes
4.	<input type="checkbox"/>	ISC-B142	1005	isctmp11	isctmp12	1000	DEPLOYED	No
5.	<input type="checkbox"/>	ISC-B143	1000	isctmp12	isctmp5	1000	DEPLOYED	No

Rows per page: 5 Go to page: 1 of 10 Go

Close Display Details Create Edit Delete

Audit SR Save & Deploy Cancel

For an explanation of the various window elements, see [Create TE Backup Tunnel](#), page A-59.

**Step 3** Click **Create**. The Create TE Backup Tunnel window in [Figure 5-23](#) appears.

Figure 5-23 Create TE Backup Tunnel

**Create TE Backup Tunnel**

<b>SR Job ID:</b> New	<b>SR ID:</b> New	<b>SR State:</b> REQUESTED
<b>Tunnel ID:</b>	<b>Creator:</b>	<b>Type:</b> ADD

Head Device \* :

Destination Device \* :

Protected Interface(s) \* :

Backup Bandwidth Limit (kbps) \* :   
☒ Any Pool BW    
☐ Sub Pool (BC1) BW  Global Pool (BC0) BW

Tunnel Number: ☐ Auto Gen ☒

Tunnel Bandwidth (kbps):

Tunnel Pool Type:   
☐ Global Pool (BC0)   
☐ Sub Pool (BC1)

Setup Priority (0-7):

Hold Priority (0-7):

Affinity (0x0-0xFFFFFFFF):

Affinity Mask (0x0-0xFFFFFFFF):

**Path Options:**

Showing 0 of 0 records

<input type="checkbox"/>	Option #	Path Name	Path Type	Lock Down
Rows per page: 10 <input type="button" value="Go"/> 1 of 1				
				<input type="button" value="Add"/> <input type="button" value="Delete"/>
				<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Note: \* - Required Field

129257

For an explanation of the various window elements, see [Create TE Backup Tunnel, page A-59](#).

- Step 4** Select, at a minimum, a **Head Device**, a **Destination Device**, and a **Protected Interface**. Also, specify a **Backup Bandwidth Limit** greater than zero. Add other tunnel information as desired.

**Figure 5-24**      *Select TE Protected Interface*

#	Interface Name	IP Address	Next Hop
1.	ATM5/0.1	10.2.2.49	isctmp2
2.	FastEthernet3/0	10.2.2.81	isctmp4
3.	FastEthernet0/1	10.2.2.17	isctmpe1

Rows per page: 10    Go to page: 1 of 1    Go    Cancel

For an explanation of the various window elements, see [Select TE Protected Interface, page A-63](#).

- Step 5** Click **Add** to add just one path. The Select TE Explicit Path window in [Figure 5-25](#) appears.

**Figure 5-25**      *Select TE Explicit Path*

#	Path Name	Head	Dest
1.	isctmp3->isctmp4-2	isctmp3	isctmp9

Rows per page: 10    Go to page: 1 of 1    Go    Cancel

- Step 6** Select an explicit path. It must match the head and destination of an existing path. If none is available, you first must set one up. To do so, see [Create Explicit Path, page 5-4](#).
- Step 7** Click **Select**. The selected path appears in the **Path Options** section of the page as shown in the Select TE Explicit Path window in [Figure 5-26](#).

**Figure 5-26**      *Path Options*

Option #	Path Name	Path Type	Lock Down
1	backup_path	Explicit	<input type="checkbox"/>

Rows per page: 10    Go to page: 1 of 1    Go    Cancel

For explicit paths, you can click the path name to open the Explicit Path Viewer as shown in [Figure 5-16](#).

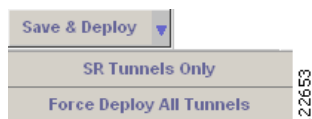
- Step 8** In the Create TE Backup Tunnel window, click **OK** to accept the entered tunnel information or click **Cancel** to quit the window without saving it. The window closes.
- Step 9** In the TE Protection SR window, a new backup tunnel is added in the tunnel list with the Op field set to ADD.



**Note** The added tunnel can be reverted to its original state by selecting it and clicking **Delete**. The tunnel is removed from the tunnel list.

- Step 10** Click **Save & Deploy** to either deploy the new tunnel SR to the network or force deploy all tunnels, or you can create or edit more backup tunnels and then save and deploy all changes.

**Figure 5-27 Save & Deploy Tunnels**



The **Save & Deploy** button provides two options:

- **SR Tunnels Only**—Deploy all tunnel changes that does not impact tunnel placement, or if no changes were made to the SR, use this to re-deploy the SR that was in **Requested** or **Invalid** state.
- **Force Deploy All Tunnels**—Force deployment of all tunnels in this SR. This could be useful when previous provisioning of the SR has failed, so that it is necessary to force through the deployment of all tunnels in the SR.

When you click **Save & Deploy**, a background process is started. To avoid a potential conflict with another deployment, wait until the SR has completed the **Requested** and **Pending** states before deploying another SR with **Save & Deploy**. To see the state of deployment, go to the **Service Request** window under **Inventory and Connection Manager** or open the **Task Manager** under **Monitoring**.



**Note** With the exception of TE Traffic Admission SRs, TE SRs are always deployed immediately from the specific TE SR window, not from the **Service Requests** page in **Inventory and Connection Manager**.

- Step 11** The **Service Requests** window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

If the SR does not go to the **Deployed** state, go to the **Task Logs** window to see the deployment log (**Monitoring > Task Manager > Logs**) as described in [SR Deployment Logs, page 10-1](#).

## Edit Backup Tunnel

Backup tunnel attributes can be modified in the backup tunnel editor.

There are two ways to access the backup tunnel editor:

- from the **Protection SR** window or
- from the **Service Requests** window.

## From the Protection SR Window

To access the Protection SR window to edit a backup tunnel, use the following steps:

- Step 1 Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Create TE Backup Tunnel**. The TE Protection SR window appears.
- Step 2 To edit a tunnel SR, select the desired SR and click **Edit**. The Edit TE Backup Tunnel window in [Figure 5-28](#) appears.

**Figure 5-28** Edit TE Backup Tunnel

**Edit TE Backup Tunnel**

SR Job ID: 2      SR ID: 4      SR State: DEPLOYED  
Tunnel ID: ISC-B41      Creator: admin      Type: ADD

Head Device \*: isctmp4

Destination Device \*: isctmp2

Protected Interface(s) \*: FastEthernet2/0 Select

Backup Bandwidth Limit (kbps) \*:   
☐ Any Pool BW    
☒ Sub Pool (BC1) BW 40  Global Pool (BC0) BW

Tunnel Number: 9

Tunnel Bandwidth (kbps): 0

Tunnel Pool Type:   
☒ Global Pool (BC0)   
☐ Sub Pool (BC1)

Setup Priority (0-7): 0

Hold Priority (0-7): 0

Affinity (0x0-0xFFFFFFFF): 0x0

Affinity Mask (0x0-0xFFFFFFFF): 0x0

**Path Options:**

Showing 1 - 1 of 1 record

<input type="checkbox"/>	Option #	Path Name	Path Type	Lock Down
<input type="checkbox"/>	1	isctmp4->isctmp2-1	Explicit	<input type="checkbox"/>

Rows per page: 10 Go to page: 1 of 1 Go Next Previous

Add Delete

OK Cancel

Note: \* - Required Field

The backup tunnel editor is identical to that of the create backup tunnel GUI. For an explanation of the various window elements, see [Create TE Backup Tunnel](#), page A-59.

- Step 3 Make the desired changes and click **OK**.
- Step 4 In the TE Protection window, the Op field changes to MODIFY.

**Note**

The modified tunnel can be reverted to its original state by selecting it and clicking **Delete**. The **MODIFY** flag in the **Op** column disappears.

- Step 5** In the TE Protection SR window, click **Save & Deploy** to either deploy the new tunnel SR to the network or force deploy all tunnels, or you can create or edit more backup tunnels and then save and deploy all changes.

The **Save & Deploy** button options are discussed in [Create Managed TE Tunnel, page A-41](#).

- Step 6** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears (see [Figure 5-18](#)) and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

## From the Service Requests Window

To edit a backup tunnel from the **Service Requests** window, assuming that the SR has been created use the following steps:

- Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Service Requests**.
- Step 2** To edit the desired tunnel SR, select the SR in question and click **Edit**. The TE Protection SR window appears displaying the SR selected in the Service Requests window. An example of the TE Protection SR window is shown in [Figure 5-22](#).
- Step 3** Select the tunnel SR and click **Edit**. The Edit TE Backup Tunnel window in [Figure 5-28](#) appears.
- Go to [From the Protection SR Window, page 5-25](#) and continue the process from [Step 3](#).

## Delete Backup Tunnel

To delete a backup tunnel from the TE Protection SR window, use the following steps:

- Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Create TE Backup Tunnel**.
- The TE Protection SR window in [Figure 5-22](#) appears.
- Step 2** To delete a tunnel SR, select the desired SR and click **Delete**. The **Op** field status changes to **DELETE** as shown in [Figure 5-29](#).



Figure 5-29 TE Protection SR - Delete Requested

**TE Protection SR**

SR Job ID: 2      Provider: pad0      SR State: REQUESTED  
 SR ID: Neww      Creator:      Type: ADD

Description:

Show Existing Tunnels with All Matching \* Find

Showing 1 - 5 of 5 records

#	<input type="checkbox"/>	Op	Tunnel ID	T#	Head	Dest	BW Quota	Deploy Status	Conformance
1.	<input type="checkbox"/>		ISC-B31	1	isctmp1	isctmp3	10	DEPLOYED	No
2.	<input type="checkbox"/>	DELETE	ISC-B46	4	isctmp1	isctmp8	120	REQUESTED	Yes
3.	<input type="checkbox"/>		ISC-B32	2	isctmp5	isctmp4	10	DEPLOYED	Yes
4.	<input type="checkbox"/>		ISC-B34	1	isctmp3	isctmp1	2000	DEPLOYED	Yes
5.	<input type="checkbox"/>		ISC-B35	1	isctmp9	isctmp8	300	DEPLOYED	Yes

Rows per page: 10 Go to page: 1 of 1 Go

Close Display Details Create Edit Delete

Audit SR Save & Deploy Cancel

122625

For an explanation of the various window elements, see [Create TE Backup Tunnel, page A-59](#).



**Note** The deleted tunnel can be reverted to its original state by selecting it and clicking **Delete**. The DELETE flag in the Op column disappears.

Click **Save & Deploy** to either deploy the new tunnel SR to the network or force deploy all tunnels, or you can create or edit more primary tunnels and then save and deploy all changes.

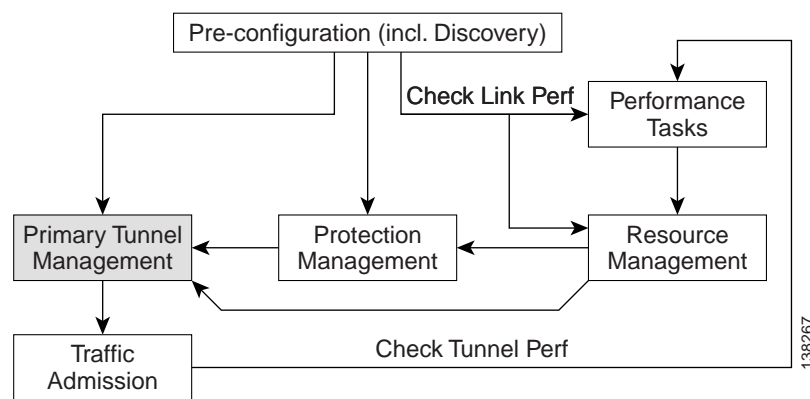
**Step 3** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears (see [Figure 5-18](#)) and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)





## Advanced Primary Tunnel Management



In addition to the basic tunnel management tools described in [Chapter 5, “Basic Tunnel Management”](#), ISC TEM gives access to a set of advanced tunnel planning tools that provide optimal placement of tunnels to ensure efficient use of network resources.

The advanced tools are available for managed tunnels only. The difference between managed and unmanaged tunnels is described in [Managed/Unmanaged Primary Tunnels, page 1-3](#).

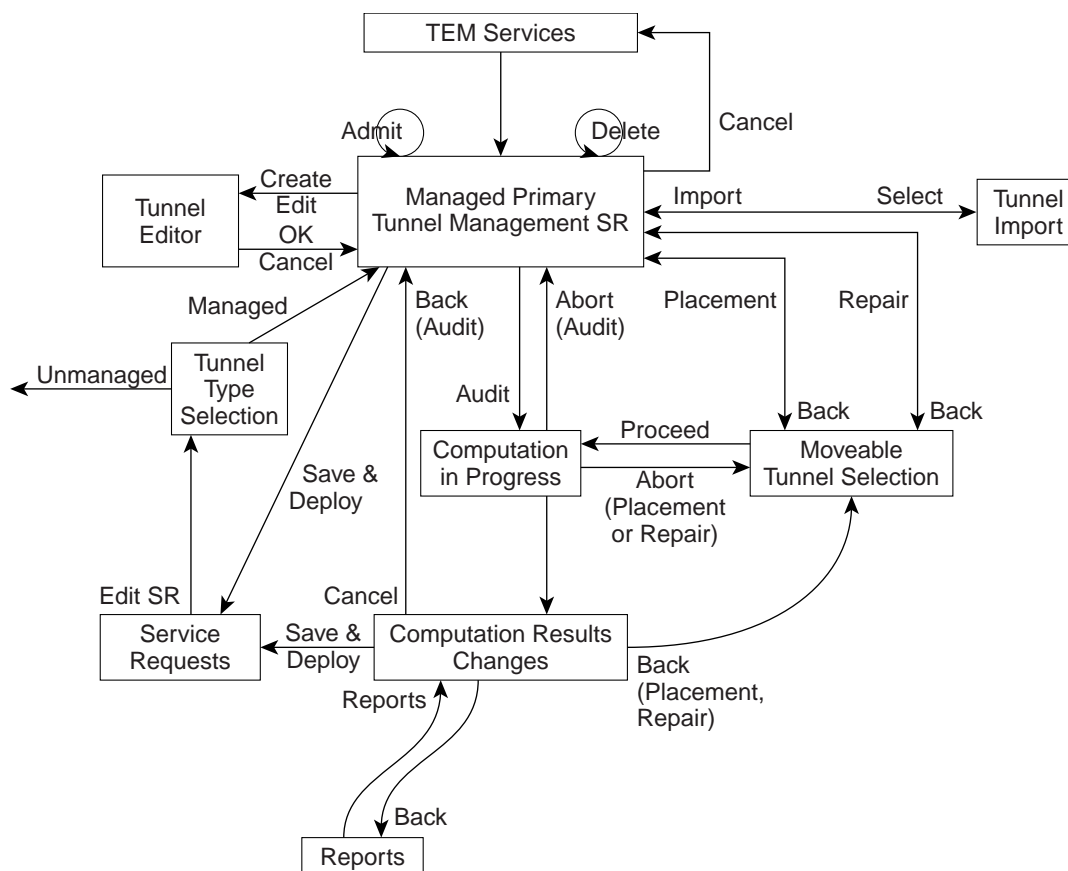
This chapter includes the following sections:

- [Tunnel Operations, page 6-2](#)
  - [Create Primary Tunnel, page 6-2](#)
  - [Edit Primary Tunnel, page 6-8](#)
  - [Delete Primary Tunnel, page 6-8](#)
  - [Admit Primary Tunnel, page 6-8](#)
  - [Import Primary Tunnel, page 6-8](#)
- [Planning Strategy, page 6-11](#)
- [Placement Tools, page 6-11](#)
  - [Tunnel Audit, page 6-12](#)
  - [Tunnel Placement, page 6-17](#)
  - [Tunnel Repair, page 6-22](#)
  - [Grooming, page 6-26](#)

# Tunnel Operations

This section explains the advanced tunnel operations in ISC TEM that incorporate the planning tools. An overview of the primary tunnel management process is provided in [Figure 6-1](#).

**Figure 6-1 Primary Tunnel Management Processes**



116622

For **Tunnel Type Selection**, when you select **Unmanaged** the TE Unmanaged Primary Tunnel SR window appears (see [Chapter 5, “Basic Tunnel Management”](#)).

All other elements in [Figure 6-1](#) are described in this chapter.

## Create Primary Tunnel

To create a TE managed primary tunnel with the RG license installed, use the following steps:

- Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2 Click **Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window appears as shown in [Figure 6-2](#).

Figure 6-2 TE Managed Primary Tunnels SR

The screenshot displays the Cisco IP Solution Center interface for managing TE Managed Primary Tunnels. The top navigation bar includes links for Home, Shortcuts, Account, Index, Help, About, and Logout. The user is logged in as 'admin'. The main content area is titled 'TE Managed Primary Tunnels SR' and shows details for SR Job ID: 8, SR ID: New, Provider: Provider2, and SR State: REQUESTED. A description field is present but empty. Below this is a table of tunnels with columns for #, Op, Tunnel ID, T#, Head, Dest, Policy, BW, AutoBW, Deploy Status, Verified, and Allow Reroute. The table shows 5 records. At the bottom, there are buttons for Close, Display, Details, Admit, Create, Edit, and Delete. A footer bar contains buttons for Import, Placement Tools, Proceed with Changes, Save & Deploy, and Cancel.

**TE Managed Primary Tunnels SR**

SR Job ID: 8      Provider: Provider2      SR State: REQUESTED  
 SR ID: New      Creator:      Type: ADD

Description:

Show Existing Tunnels with All matching Find

Showing 1 - 5 of 23 records

#	Op	Tunnel ID	T#	Head	Dest	Policy	BW	AutoBW	Deploy Status	Verified	Allow Reroute
1.	<input type="checkbox"/>	ISC-P1	2	isctmp11	isctmp10	ISC-P1-isctmp11:tunnel-te2	2	false	DEPLOYED	succeed	false
2.	<input type="checkbox"/>	ISC-P2	1000	isctmp11	isctmp1	ISC-P2-isctmp11:tunnel-te1000	200	false	DEPLOYED	succeed	false
3.	<input type="checkbox"/>	ISC-P122	1003	isctmp11	isctmp12	ISC-P122-isctmp11:tunnel-te1003	500	false	DEPLOYED	succeed	false
4.	<input type="checkbox"/>	ISC-P123	1004	isctmp11	isctmp8	ISC-P122-isctmp11:tunnel-te1003	500	false	DEPLOYED	succeed	false
5.	<input type="checkbox"/>	ISC-P3	1	isctmp10	isctmp6	ISC-P2-isctmp11:tunnel-te1000	1000	false	DEPLOYED	succeed	false

Rows per page: 5      Go to page: 1 of 5

Close Display Details Admit Create Edit Delete

Import Placement Tools Proceed with Changes Save & Deploy Cancel

For an explanation of the various window elements, see [Create Managed TE Tunnel](#), page A-41.

**Step 3** Click **Create**. The Create TE Managed Primary Tunnel window appears as shown in [Figure 6-3](#).

Figure 6-3 Create TE Managed Primary Tunnel

**Create TE Managed Primary Tunnel**

SR Job ID: New		SR ID: New		SR State: REQUESTED	
Tunnel ID: *		Creator:		Type: ADD	
Head Device *:	<input type="text"/>	<input type="button" value="Select"/>			
Destination Device *:	<input type="text"/>	<input type="button" value="Select"/>			
Tunnel Policy *:	<input type="text"/>	<input type="button" value="Select"/>			
Tunnel Bandwidth (Kbps):	<input type="text"/>				
Tunnel Number:	Auto Gen <input checked="" type="checkbox"/>				
Customer:	<input type="text"/>				
Auto BW:	Enable: <input type="checkbox"/> Freq (sec): <input type="text"/> Min (Kbps): <input type="text"/> Max (Kbps): <input type="text"/>				
<b>Path Options:</b>					
Showing 1 - 2 of 2 records					
<input type="checkbox"/>	Option #	Path Name	Path Type	Lock Down	
<input type="checkbox"/>	1	System Path	Explicit	<input type="checkbox"/>	
<input type="checkbox"/>	2	Dynamic Path	Dynamic	<input type="checkbox"/>	
Rows per page: 5		Go to page: 1 of 1 <input type="button" value="Go"/>			
			<input type="button" value="Add"/> <input type="button" value="Delete"/>		
			<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

Note: \* - Required Field

138939

For an explanation of the various window elements, see [Create Managed TE Tunnel, page A-41](#).

The **Path Options** section provides three path types, **System Path**, **Explicit Path**, and **Dynamic Path**.

A **System Path** is an ISC system generated explicit path (immovable). The first path has to be an explicit path.

An **Explicit Path** is a fixed path from a specific head to a specific destination device.

A **Dynamic Path** is provisioned by allowing the head router to find a path. The **dynamic** keyword is provisioned to the routers.

**Step 4** To select a **Head Device**, click the corresponding **Select** button to open the window shown in [Figure 6-4](#).

**Figure 6-4** Select Device for TE Head Router

Device for **TE Head Router**

Show Devices with:  matching

Showing 1 - 5 of 14 records

#	Device Name	IGP ID	MPLS TE ID	Admin Status
1.	<input type="radio"/> isctmp1	192.168.118.176	192.168.118.176	UP
2.	<input type="radio"/> isctmp11	192.168.118.166	192.168.118.166	UP
3.	<input type="radio"/> isctmp10	192.168.118.167	192.168.118.167	UP
4.	<input type="radio"/> isctmp12	192.168.118.168	192.168.118.168	UP
5.	<input type="radio"/> isctmp13	192.168.118.171	192.168.118.171	UP

Rows per page:  Go to page:  of 3

For an explanation of the various window elements, see [Create TE Managed Primary Tunnel, page A-44](#).  
 Select a head device and click **Select**.

- Step 5** To select a **Destination Device**, click the corresponding **Select** button to open the window shown in [Figure 6-5](#).

**Figure 6-5** Select Device for TE Tail Router

Device for **TE Tail Router**

Show Devices with:  matching

Showing 1 - 5 of 15 records

#	Device Name	IGP ID	MPLS TE ID	Admin Status
1.	<input type="radio"/> 192.168.118.178	192.168.118.178	192.168.118.178	UP
2.	<input type="radio"/> isctmp1	192.168.118.176	192.168.118.176	UP
3.	<input type="radio"/> isctmp11	192.168.118.166	192.168.118.166	UP
4.	<input type="radio"/> isctmp10	192.168.118.167	192.168.118.167	UP
5.	<input type="radio"/> isctmp12	192.168.118.168	192.168.118.168	UP

Rows per page:  Go to page:  of 3

For an explanation of the various window elements, see [Create TE Managed Primary Tunnel, page A-44](#).  
 Select a tail device and click **Select**.

- Step 6** To select a **Tunnel Policy**, click the corresponding **Select** button to open the window shown in [Figure 6-6](#).



**Note**

If no tunnel policies are available, the reason could be that they are all unmanaged. To create a managed tunnel, use the **Policy Manager** (see [Create Primary Tunnel, page 6-2](#)) and make sure to check the **Managed** check box.

**Figure 6-6** Select Managed TE Tunnel Policy

#	Policy Name	Pool Type	Setup Priority	Hold Priority	Affinity	Affinity Mask	Delayed Constraint	FRR Protection
1.	man1	GLOBAL	0	0	0x0	0xFFFF		None
2.	pm-none	GLOBAL	0	0	0x0	0xFFFF		None

For an explanation of the various window elements, see [Create TE Managed Primary Tunnel, page A-44](#).

- Step 7** Specify a tunnel bandwidth greater than zero. Add other tunnel information as desired.
- Step 8** Optionally, if you want to specify an explicit path rather than using the system path provided by ISC TEM, delete the system path and subsequently add the explicit path. For a more detailed explanation of this step, see [Create Primary Tunnel, page 5-8](#).
- Step 9** In the Create TE Managed Tunnel window, click **OK** to accept the entered tunnel information or **Cancel** to quit and return to the TE Managed Primary Tunnels SR window.

The TE Managed Primary Tunnel SR window in [Figure 6-7](#) appears displaying the new tunnel with the Op field set to ADD to signify that an SR has been added.



**Note**

The added tunnel can be reverted to its original state by selecting it and clicking **Delete**. The tunnel is removed from the tunnel list.



Figure 6-7 TE Managed Primary Tunnel SR - Added Tunnel

**TE Managed Primary Tunnels SR**

SR Job ID: 8      Provider: Provider2      SR State: REQUESTED  
 SR ID: New      Creator:      Type: ADD

Description:

Show SR      Tunnels with All matching      Find

Showing 1 - 1 of 1 record

#	Op	Tunnel ID	T#	Head	Dest	Policy	BW	AutoBW	Deploy Status	Verified	Allow Reroute
1.	<input type="checkbox"/> ADD	ISC-P153		isctmp11	isctmp10	ISC-P122-isctmp11:tunnel-te1003	100	false	REQUESTED	unknown	true

Rows per page: 5

Tunnel Audit      Go to page: 1 of 1      Go

Close      Display      Tunnel Placement      Create      Edit      Delete

Tunnel Repair

Import      Placement Tools      Proceed with Changes >>      Save & Deploy      Cancel

**Step 10** In the TE Managed Primary Tunnel SR window, you can create or edit more tunnels, or if you are done with all the changes, proceed in one of the following two ways depending on which of the following buttons are active (**Save & Deploy** is not available after the **Create** operation):

- **Proceed with Changes:** The changes you entered impacts tunnel placement. Click on this to continue with one of the planning flows described in the Placement Tools (see [Placement Tools, page 6-11](#)) until the SR can be saved and deployed.
- **Save & Deploy:** The changes you entered do not impact tunnel placement. Click on this to save and deploy the SR. This function is further described in [Create Managed TE Tunnel, page A-41](#).

**Note**

When you click **Save & Deploy**, a background process is started. To avoid a potential conflict with another deployment, wait until the SR has completed the Requested and Pending states before deploying another SR with **Save & Deploy**. To see the state of deployment, go to the Service Request window under Inventory and Connection Manager or open the Task Manager under Monitoring.

**Note**

With the exception of TE Traffic Admission SRs, TE SRs are always deployed immediately from the specific TE SR screen, not from the Service Requests page in **Inventory and Connection Manager**.

**Step 11** If **Save & Deploy** was selected in [Step 10](#), the Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) opens and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

If the SR does not go to the **Deployed** state, go to the Task Logs window to see the deployment log (**Monitoring > Task Manager > Logs**) as described in [Task Monitoring, page 10-1](#).

## Edit Primary Tunnel

The only difference between creating and editing tunnels is that in the tunnel editor, the head and destination devices and tunnel number fields are not editable. Otherwise, you create and edit the same attributes.

Only **Proceed with Changes** or **Save & Deploy**, not both, are available depending on whether the changes you entered impacts tunnel placement.

To edit a primary tunnel, see [Chapter 5, “Basic Tunnel Management.”](#)

## Delete Primary Tunnel

To delete one or more tunnels, see [Chapter 5, “Basic Tunnel Management.”](#)

## Admit Primary Tunnel

The Admit function is used to admit selected tunnels not previously verified into the managed topology. This feature is used only for discovered tunnels that failed verification. During the discovery process, verification is performed with the Tunnel Placement algorithm, as if the tunnels were admitted for the first time.

Verification means that the discovered managed tunnel is verified against the network topology and ISC TEM checks if there is enough bandwidth along the tunnel path (both are specified in the tunnel).

In general, verification will fail if there is not enough bandwidth due to the existence of other tunnels or a limitation on link capacity/bandwidth.

More specifically, this can happen when a priority 0 tunnel is created independently of ISC TEM and a TE Discovery task is run. If the tunnel does not satisfy all the managed tunnel constraints (that is, if it is reserving more bandwidth than is available in a link that it passes through) TE discovery will mark it as ‘verified = false’. It will not be managed by ISC TEM until you use the Admit button to make it verified. Typically this would have to be accompanied with some other tunnel or resource change to ensure that the constraint is now satisfied.

To admit a primary tunnel, use the following steps:

- 
- |        |  |
|--------|--|
| Step 1 | In the <b>TE Managed Primary Tunnel SR</b> , select one or more unverified tunnels to migrate.   |
| Step 2 | Click <b>Admit</b> . The unverified tunnel(s) are verified and, if successful, an <b>ADMIT</b> flag will appear in the <b>Op</b> column.             |
| Step 3 | Select <b>Proceed with Changes &gt;&gt; &gt; Tunnel Placement</b> to determine if the tunnels can be placed. If not, edit the tunnels and try again. |
- 

## Import Primary Tunnel

This feature allows you to update tunnels in bulk through a file-based import mechanism. The data is migrated into the managed primary tunnel service request.

## Construct XML Import File

To import tunnels from a file, first construct an XML import file conforming to the structure defined in the system supplied Document Type Definition (DTD) file (see [Appendix D, “Document Type Definition \(DTD\) File”](#)), and save the XML file together with the DTD file on the ISC server under the same directory. To create a valid import file, use the provided command line validation tool (see [Command Line Validation Tool, page 6-9](#)).

The following files are necessary for importing data into the ISC TEM application and are included in the installation:

- DTD file for the import file in  
`< installedDir >/ resources/java/xml/com/cisco/vpnsc/ui/te`
  - **TeImport.dtd**  
(a sample file, ‘**sample.xml**’, is also included)
- Shell script for executing the command line validator in the `<installedDir>/bin` directory.
  - **ImportTeTunnels**  
Usage: **importTeTunnels** *<importfile>*

*importfile* is a XML file and must specify **TeImport.dtd** as its DTD. **TeImport.dtd** must be in the same directory as *importfile*.

## Command Line Validation Tool

The purpose of a command line validator is to help construct a valid import file off-line that corresponds to **TeImport.dtd**. The tool helps screen out errors associated with files that are not well-formed and files that do not conform to the rules set by the DTD.

For instructions on how to use the DTD file, see the DTD file documentation.

The tool reads the import file line-by-line, echoes each line in on the output as it parses, and reports any parsing error it encounters. The parsing and validation continues even when parsing errors are encountered for as long as the file structure makes sense.



### Note

This tool does not check for cross field validation or data integrity errors with respect to the ISC TEM application.

## Import Procedure

The file-based import feature is only enabled when there are no uncommitted new, changed, or deleted tunnels in the service request.

It provides a way of adding, editing, deleting, or migrating many tunnels at a time.

To start the import procedure, use the following steps:

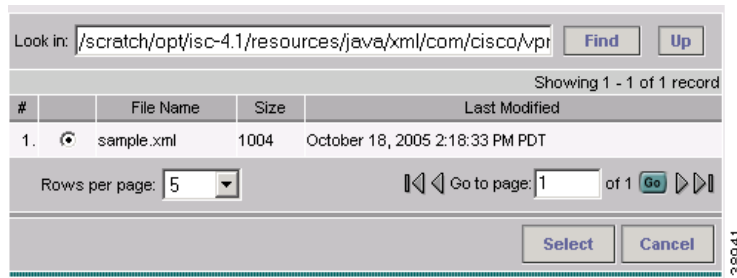
- 
- Step 1** Prepare the XML import file in accordance with the DTD file.
  - Step 2** Go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
  - Step 3** Select provider if this has not been done earlier in the session.
  - Step 4** Click **Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window appears as shown in [Figure 6-2](#).

**Step 5** Click **Import** to start the import process. The Select Import File window in [Figure 6-8](#) appears.



**Note** The Import button is only enabled when there are no uncommitted new, changed, or deleted tunnels in the service request.

**Figure 6-8** *Select Import File*



For an explanation of the various window elements, see [Import Tunnel](#), page A-50.

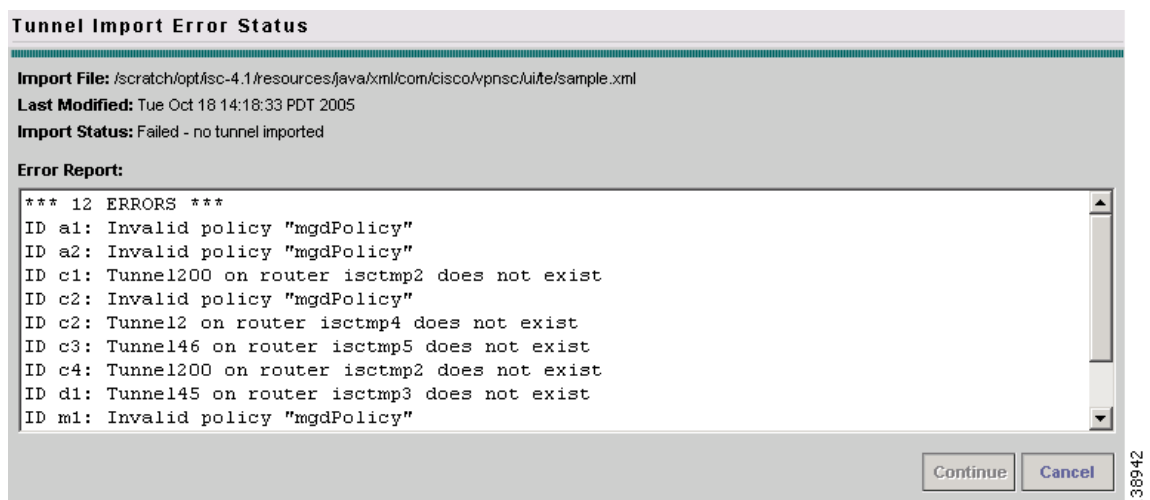
The Select Import File window lists all the XML files and any directories under the directory name shown in the **Look in** field.

The default directory shown in the **Look in** field in [Figure 6-8](#) corresponds to the installation directory in which the DTD and sample XML files reside.

**Step 6** Select the desired XML file to be used for the import operation.

The system then parses the file. If any error is detected, it will be reported in the Tunnel Import Error Status window shown in [Figure 6-9](#).

**Figure 6-9** *Tunnel Import Error Status*



For an explanation of the various window elements, see [Import Tunnel](#), page A-50.

The Tunnel Import Error Status window shows the URL of the file, its last modified timestamp, the import status, and any error/warning messages.

- Step 7** If the import operation failed, **Cancel** to return to the previous screen. If it is partially successful, the **Continue** button is enabled, thereby providing an additional option to accept system treatment for errors/warnings and continue with the import operation.
- Step 8** If the file is parsed successfully or you click **Continue**, all valid tunnels in the file are added to the service request and the TE Managed Primary Tunnels SR window is re-displayed in the SR view. The imported tunnels are displayed with the appropriate tunnel **Op** type.
- 

## Planning Strategy

The main objective of using the planning tools is to achieve optimal overall network utilization while causing minimal impact on any existing traffic on the network.

In most cases, the following strategy can be applied:

- Attempt to admit the new traffic optimising on utilisation (Placement feature) without allowing existing traffic to be moved. This offers the possibility of accommodating the new traffic without any changes to the existing traffic, while still optimising reserved bandwidth utilisation under the constraint that existing tunnels do not move.
- If this fails, attempt to admit the same new traffic minimising change to existing traffic (Repair feature) to see if the new traffic can be accommodated without affecting any more existing tunnels than necessary.
- If this succeeds in placing the new traffic, but you feel that the overall reserved bandwidth utilisation is higher than would be preferred, consider grooming the network.
- If the Repair fails, review the parameters that control how many changes can be considered. Alternatively the specification to the desired traffic could be changed, or resource modifications could be made.

This strategy reflects the different approaches taken by the different algorithms in searching for solutions. However, other combinations are possible.

## Placement Tools

Planning tools for primary tunnels are available in two buttons on the TE Primary Tunnel SR screen as shown in [Figure 6-10](#) and [Figure 6-11](#) depending on whether a change has been made to the managed primary tunnels.

- **Proceed with Changes:** Used when you have made changes (add/change/delete/admit) to the tunnels. Tunnel operations are described in [Tunnel Operations, page 6-2](#). Then choose one of the placement tools to verify primary placement with the system and continue with deployment. This button is also available in Resource Management.
- **Placement Tools:** Used to perform planning function on the existing network.
  - The Tunnel Audit option should be used to verify the constraint-based placement of existing managed primary tunnels with the existing network topology. You can use this option to find out the optimality of your primary placement. If you are requiring protection levels above "Best Effort" on your primary tunnels, it is also important to perform an audit after any changes have been made in the protection network. If the audit results in warnings/violations, you can use the Tunnel Repair option help you find a solution.

- The **Groom** option is used for optimizing your primary placement. In all primary computation, a quality report is produced which displays the optimality and utilization of the bandwidth pools. You can perform a Tunnel Audit first to determine if grooming is needed on your network.

They are accessed from two buttons in the TE Managed Primary Tunnels SR window as shown in [Figure 6-10](#) and [Figure 6-11](#).

**Figure 6-10** Proceed with Changes Button



**Figure 6-11** Placement Tools Button



The planning tools are described in detail in the following sections.



#### Note

If tunnel attributes that are not supported by the placement tools (such as auto-bw frequency) are changed in conjunction with attributes that are supported, the attributes appear correctly in the TE Computation Results window. But if only unsupported attributes are changed, the TE Computation Results window still shows no achieved changes and the Save & Deploy button is grayed out so the change cannot be deployed.

## Tunnel Audit

When any type of change is required, whether tunnel modifications or TE resource modifications, a Tunnel Audit is run to determine what inconsistencies the change might cause, if any. Tunnel Audit can also be used anytime to check the for optimality of network utilization.

The audit can be performed from the primary tunnel window or from the **TE Resource Modifications** window.

Tunnel Audit can also be invoked from the Resource Management window (see [Chapter 4, “TE Resource Management”](#)).

To perform an audit on the created tunnel, use the following steps:

- Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2 Click **Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window appears as shown in [Figure 6-2](#).

Tunnel Audit can be used in two ways:

- When one or more tunnels have been created or their attributes altered (see [Create Primary Tunnel, page 6-2](#)), Tunnel Audit can be activated by selecting **Proceed with Changes >>**.
- When no changes have taken place, Tunnel Audit can be accessed by selecting **Placement Tools**.

**Step 3** As an example, assume that a new primary tunnel SR has been created. The TE Managed Primary Tunnel SR window shown in [Figure 6-12](#) appears.

**Figure 6-12** TE Managed Primary Tunnel SR (Audit)

**TE Managed Primary Tunnels SR**

SR Job ID: 8      Provider: Provider2      SR State: REQUESTED  
 SR ID: New      Creator:      Type: ADD

Description:

Show **SR** Tunnels with **All** matching **Find**

Showing 1 - 1 of 1 record

#	Op	Tunnel ID	T#	Head	Dest	Policy	BW	AutoBW	Deploy Status	Verified	Allow Reroute
1.	<input type="checkbox"/> ADD	ISC-P153		isctmp11	isctmp10	ISC-P122-isctmp11:tunnel-te1003	100	false	REQUESTED	unknown	true

Rows per page: **5**

**Tunnel Audit**    Go to page: **1** of 1 **Go**

**Tunnel Placement**

**Tunnel Repair**

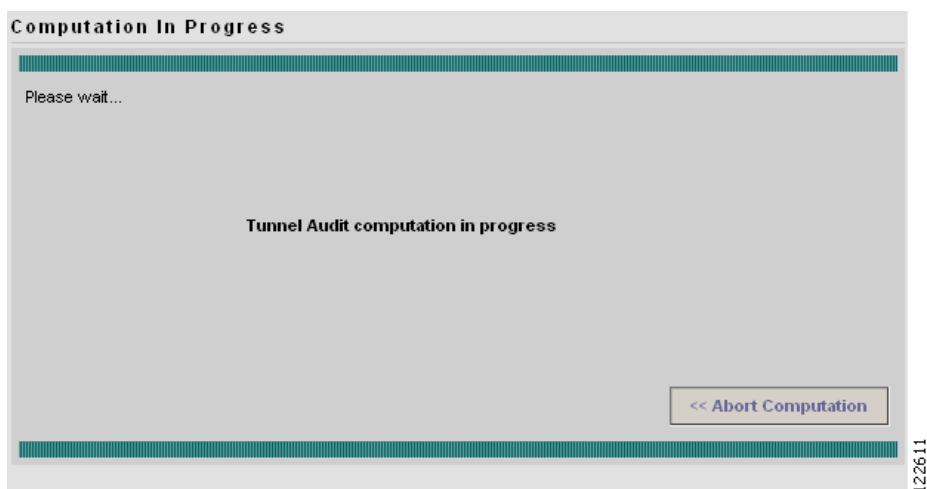
**Create**    **Edit**    **Delete**

**Import**    **Placement Tools**    **Proceed with Changes >>**    **Save & Deploy**    **Cancel**

For an explanation of the various window elements, see [Create Managed TE Tunnel, page A-41](#).

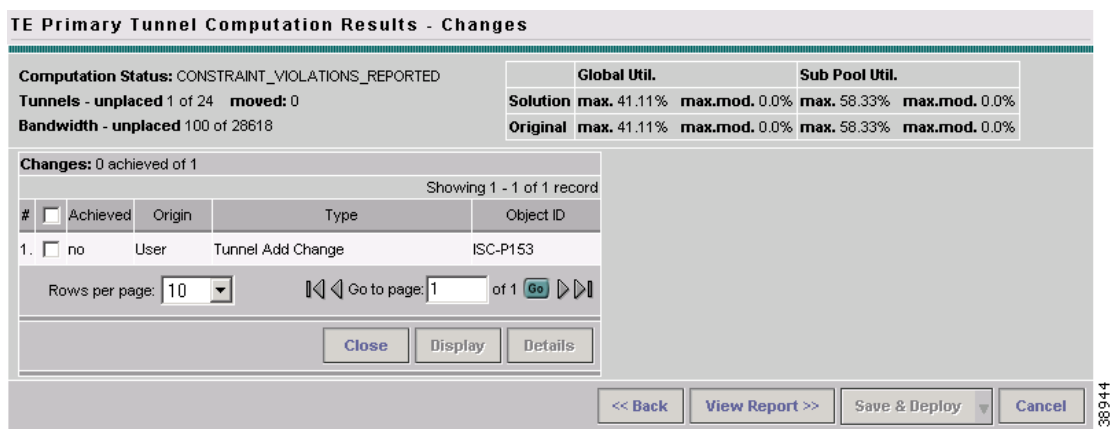
**Step 4** Select **Proceed with Changes >>** > **Tunnel Audit**.

The Computation In Progress window shown in [Figure 6-13](#) appears.

**Figure 6-13** Computation In Progress - Audit

To abort the computation and return to the previous window, click << **Abort Computation**.

**Step 5** The TE Primary Tunnel Computation Results - Changes window in [Figure 6-14](#) appears.

**Figure 6-14** TE Primary Tunnel Computation Results - Changes

For an explanation of the various window elements, see [Planning Tools, page A-52](#).

**Note**

Certain attributes, such as Description, that do not impact the computation carried out by the placement tools and updates to these are not displayed in the Computation Result Window.

**Step 6** To obtain detailed information about the tunnel and whether the change request was achieved, select the specific tunnel and click **Detail**. The detail section in the right side of the window appears as shown in [Figure 6-15](#).



Figure 6-15 TE Primary Tunnel Computation Results - Audit Changes (Details)

**TE Primary Tunnel Computation Results - Changes**

Computation Status: CONSTRAINT\_VIOLATIONS\_REPORTED  
Tunnels - unplaced 1 of 24 moved: 0  
Bandwidth - unplaced 100 of 28618

Global Util.		Sub Pool Util.	
Solution	max. 41.11% max.mod. 0.0%	max. 58.33%	max.mod. 0.0%
Original	max. 41.11% max.mod. 0.0%	max. 58.33%	max.mod. 0.0%

Changes: 0 achieved of 1

Showing 1 - 1 of 1 record

#	Achieved	Origin	Type	Object ID
1.	<input checked="" type="checkbox"/>	no	User	Tunnel Add Change

Rows per page: 10 Go to page: 1 of 1

Change Type: Tunnel Add Change  
Achieved: no  
Description: A new tunnel has been requested, for which a path must be calculated by the system

Requested Tunnel  
ID: ISC-P153  
Head: isctmp11  
Tail: isctmp10  
Policy: ISC-P122-isctmp11:tunnel-te1003  
Bandwidth: 100  
Computed Path:

Close Display Details

<< Back View Report >> Save & Deploy Cancel

For an explanation of the various window elements, see [Planning Tools, page A-52](#).

A **qualityReport** is always generated. If the computation was successful, this will be the only report. If a warning or a violation was encountered, one or more warning or violation reports will also be generated.

- Step 7** To view an audit report, click **View Report >>**. The TE Primary Tunnel Computation Results - Report window in [Figure 6-16](#) appears.

Figure 6-16 TE Primary Tunnel Computation Results - Audit Report

**TE Primary Tunnel Computation Results - Report**

Computation Status: CONSTRAINT\_VIOLATIONS\_REPORTED  
Tunnels - unplaced 1 of 24 moved: 0  
Bandwidth - unplaced 100 of 28618

Global Util.		Sub Pool Util.	
Solution	max. 41.11% max.mod. 0.0%	max. 58.33%	max.mod. 0.0%
Original	max. 41.11% max.mod. 0.0%	max. 58.33%	max.mod. 0.0%

Report:

Showing 1 - 2 of 2 records

#	Report Type	Summary Info
1.	<input checked="" type="checkbox"/> qualityReport	
2.	<input type="checkbox"/> violationNoTunnelForDemand	ISC-P153

Rows per page: 10 Go to page: 1 of 1

Details

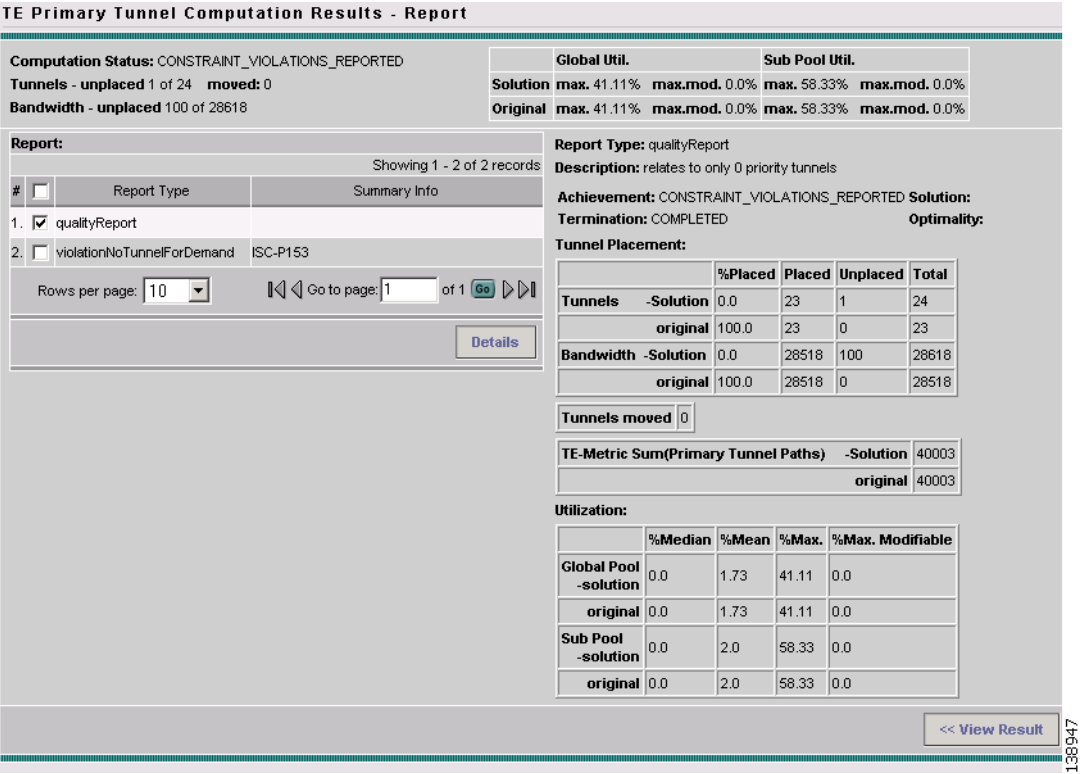
<< View Result

For an explanation of the various window elements, see [Planning Tools, page A-52](#).

In this case, as shown in [Figure 6-16](#), both a **qualityReport** and a violation report have been generated.

- Step 8** To view the contents of the **qualityReport**, select the **qualityReport** and click the **Detail** button. The TE Primary Tunnel Computation Results - Report (details) window in [Figure 6-17](#) appears.

Figure 6-17 TE Managed Primary Tunnels SR - Audit qualityReport (Details)



For an explanation of the various window elements, see [Planning Tools](#), page A-52.

The qualityReport fields in the right window pane are described in [TE Primary Tunnel Computation Results - Report](#), page A-57.

- Step 9 To view the contents of the violation report, select the violation report and click the **Detail** button. The TE Primary Tunnel Computation Results - Report (details) window in [Figure 6-18](#) appears.

**Figure 6-18** TE Managed Primary Tunnels SR - Audit Violation Report (Details)

**TE Primary Tunnel Computation Results - Report**

<b>Computation Status:</b> CONSTRAINT_VIOLATIONS_REPORTED		<b>Global Util.</b>		<b>Sub Pool Util.</b>	
<b>Tunnels - unplaced</b> 1 of 24 <b>moved:</b> 0		<b>Solution</b>	max. 41.11%	max.mod. 0.0%	max. 58.33%
<b>Bandwidth - unplaced</b> 100 of 28618		<b>Original</b>	max. 41.11%	max.mod. 0.0%	max. 58.33%

**Report:**

Showing 1 - 2 of 2 records

#	Report Type	Summary Info
1.	<input type="checkbox"/> qualityReport	
2.	<input checked="" type="checkbox"/> violationNoTunnelForDemand	ISC-P153

Rows per page: 10    Go to page: 1 of 1 **Go**

**Details**

**Report Type:** violationNoTunnelForDemand

**Description:** No path implements a requested PrimaryTunnel, even though there exists a valid path in the network that this tunnel could take

**Requested Primary Tunnel**

<b>Name:</b> ISC-P153	<b>Pool:</b> GLOBAL
<b>Head:</b> isctmp11	<b>FRR Protection:</b> None
<b>Tail:</b> isctmp10	<b>Propagation Delay:</b> Not Constrained
<b>Bandwidth:</b> 100	<b>Affinity Bits/Mask:</b> 0x0/0xFFFF

**Requested Path:**

**<< View Result**

For an explanation of the various window elements, see [Planning Tools, page A-52](#).

The report fields in the right window pane are described for each report in [Appendix C, “Warnings and Violations.”](#)

- Step 10** Click **<< View Result** to return to the Changes window ([Figure 6-14](#) or [Figure 6-15](#)). If the proposed changes were achieved, you can click on **Save & Deploy** to save the achievable changes to the repository and implement the tunnel modifications on the network.

**Note**

**Save & Deploy** will discard any changes that were not achievable.

- Step 11** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

## Tunnel Placement

The Placement feature supports the admission of new tunnels into the network and the modification of tunnels already admitted into the network. ISC TEM will attempt to implement the changes in such a way that network utilization is optimized.

To place a created tunnel, use the following steps:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2** Click **Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window appears as shown in [Figure 6-2](#).

- Step 3** When one or more tunnels have been created or their attributes altered (see [Create Primary Tunnel](#), page 6-2), select **Proceed with Changes >> > Tunnel Placement**. The Movable Tunnel Selection (Placement) window shown in [Figure 6-19](#) appears.

**Figure 6-19** Movable Tunnel Selection - Placement

**Movable Tunnel Selection**

**Computation Type** Tunnel Placement

**Maximum computation duration (Timeout in sec) \*** 100

Number of reroutable tunnels selected as movable: 0 of 0 Non-reroutable tunnels 23

Show Tunnels with All matching \* Find

Showing 1 - 5 of 23 records

#	Movable	Allow Reroute	Tunnel ID	T#	Head	Dest	Policy	BW
1.	<input type="checkbox"/> NA	false	ISC-P1	2	isctmp11	isctmp10	ISC-P1-isctmp11:tunnel-te2	2
2.	<input type="checkbox"/> NA	false	ISC-P2	1000	isctmp11	isctmp1	ISC-P2-isctmp11:tunnel-te1000	200
3.	<input type="checkbox"/> NA	false	ISC-P122	1003	isctmp11	isctmp12	ISC-P122-isctmp11:tunnel-te1003	700
4.	<input type="checkbox"/> NA	false	ISC-P123	1004	isctmp11	isctmp8	ISC-P122-isctmp11:tunnel-te1003	500
5.	<input type="checkbox"/> NA	false	ISC-P3	1	isctmp10	isctmp6	ISC-P2-isctmp11:tunnel-te1000	1000

Rows per page: 5 Go to page: 1 of 5 Go

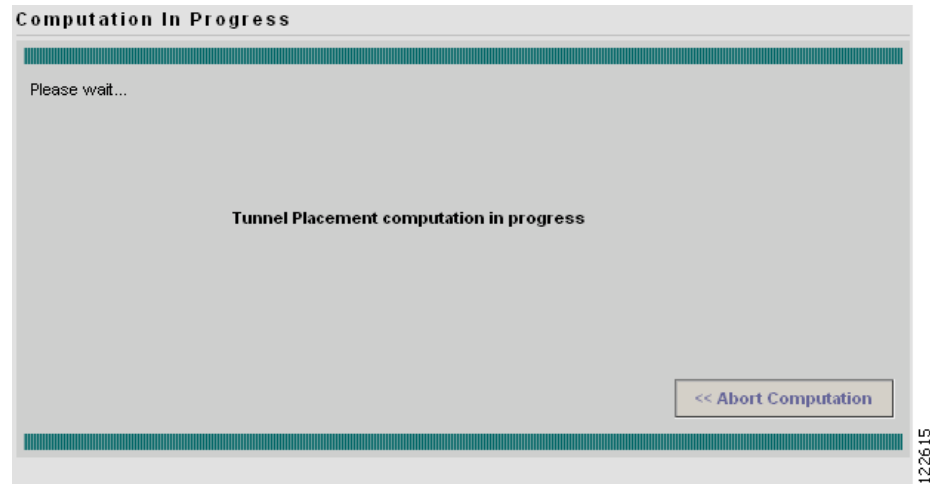
Set Movable Set Unmovable

<< Back Proceed >> Cancel

For an explanation of the various window elements, see [Planning Tools](#), page A-52.

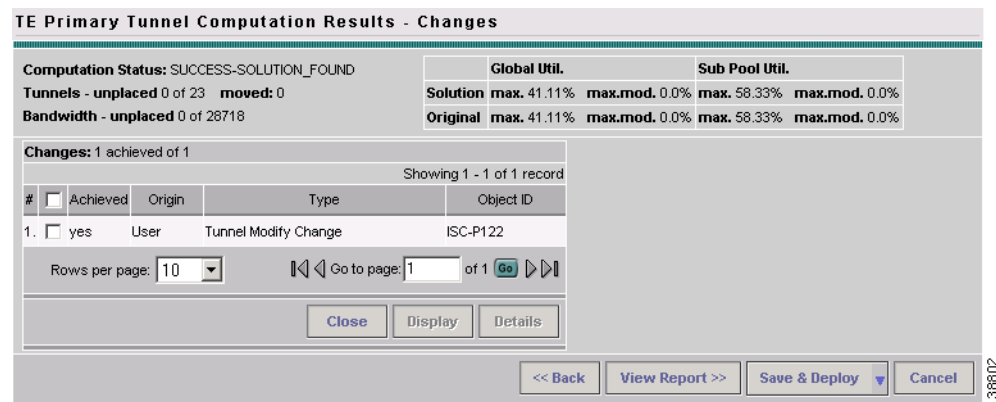
- Step 4** Set the movable and unmovable managed tunnels.
- You can specify whether, when admitting a new tunnel, existing tunnels can be moved (re-routed). This is configurable by the user. The default is that managed tunnels are not movable.
- Step 5** Click **Proceed >>**. The Computation In Progress window shown in [Figure 6-20](#) appears.

Figure 6-20 Computation In Progress - Placement



To abort the computation and return to the previous window, click **<< Abort Computation**. The TE Primary Tunnel Computation Results - Changes window shown in Figure 6-21 appears.

Figure 6-21 TE Primary Tunnel Computation Results - Placement Changes



For an explanation of the various window elements, see [Planning Tools, page A-52](#).



#### Note

Certain attributes, such as Description, that do not impact the computation carried out by the placement tools and updates to these are not displayed in the Computation Result Window.

#### Step 6

To obtain detailed information about the tunnel and whether the placement request was achieved, select the specific tunnel and click **Detail**. The detail section in the right side of the window appears as shown in Figure 6-14.

Figure 6-22 TE Primary Tunnel Computation Results - Placement Changes (Details)

**TE Primary Tunnel Computation Results - Changes**

**Computation Status:** SUCCESS-SOLUTION\_FOUND  
**Tunnels -** unplaced 0 of 23    moved: 0  
**Bandwidth -** unplaced 0 of 28718

		Global Util.		Sub Pool Util.	
<b>Solution</b>	max. 41.11%	max.mod. 0.0%	max. 58.33%	max.mod. 0.0%	
<b>Original</b>	max. 41.11%	max.mod. 0.0%	max. 58.33%	max.mod. 0.0%	

**Changes:** 1 achieved of 1  
 Showing 1 - 1 of 1 record

#	Achieved	Origin	Type	Object ID
1.	<input checked="" type="checkbox"/> yes	User	Tunnel Modify Change	ISC-P122

Rows per page: 10    Go to page: 1 of 1    Go

[Close](#)   [Display](#)   [Details](#)

**Change Type:** Tunnel Modify Change  
**Achieved:** yes  
**Description:** Request to modify one or more attributes of an existing tunnel

**Requested Tunnel**  
**ID:** isctmp11:tunnel-te1003  
**Head:** isctmp11  
**Tail:** isctmp12  
**Policy:** ISC-P122-isctmp11:tunnel-te1003  
**Bandwidth:** 700  
**Path:** [isctmp11-isctmp12-1](#)

Changed Attributes	New Value	Achieved
B/W	700	yes

<< Back   View Report >>   Save & Deploy   Cancel

For an explanation of the various window elements, see [Planning Tools](#), page A-52.

If the placement request succeeded (**Achieved: yes**), the Detail pane will contain a computed **Path** that is selectable as shown in [Figure 6-22](#).

To view the path information, click the blue link in the computed **Path** field. The TE Explicit Path window shown in [Figure 6-23](#) appears.

Figure 6-23 TE Explicit Path for Placement Request

**Path Name \***: isctmp11-isctmp12-1

**Head Router \***: isctmp11

**Links:**

Showing 1 - 1 of 1 record

#	Device	Outgoing Interface	Outgoing IP	Next Hop	Type	Incoming Interface	Incoming IP
1.	isctmp11	POS0/2/0/0	10.2.4.10	isctmp12	CISCO_ROUTER	POS0/3/0/0	10.2.4.9

Rows per page: 10    Go to page: 1 of 1    Go

**Provision Preference \***:    Outgoing Interface ☒    Incoming Interface ☐

[Close](#)

- Step 7** To view the placement report(s), click **View Report >>** in the Changes window ([Figure 6-22](#)). The TE Primary Tunnel Computation Results - Report window in [Figure 6-24](#) appears.

Figure 6-24 TE Primary Tunnel Computation Results - Placement Report Window

**TE Primary Tunnel Computation Results - Report**

Computation Status: SUCCESS-SOLUTION\_FOUND  
 Tunnels - unplaced 0 of 23 moved: 0  
 Bandwidth - unplaced 0 of 28718

	Global Util.		Sub Pool Util.	
Solution	max. 41.11%	max.mod. 0.0%	max. 58.33%	max.mod. 0.0%
Original	max. 41.11%	max.mod. 0.0%	max. 58.33%	max.mod. 0.0%

**Report:**

Showing 1 - 1 of 1 record

#	Report Type	Summary Info
1.	<input checked="" type="checkbox"/> qualityReport	

Rows per page: 10 Go to page: 1 of 1

[Details](#)

[View Result](#)

138805

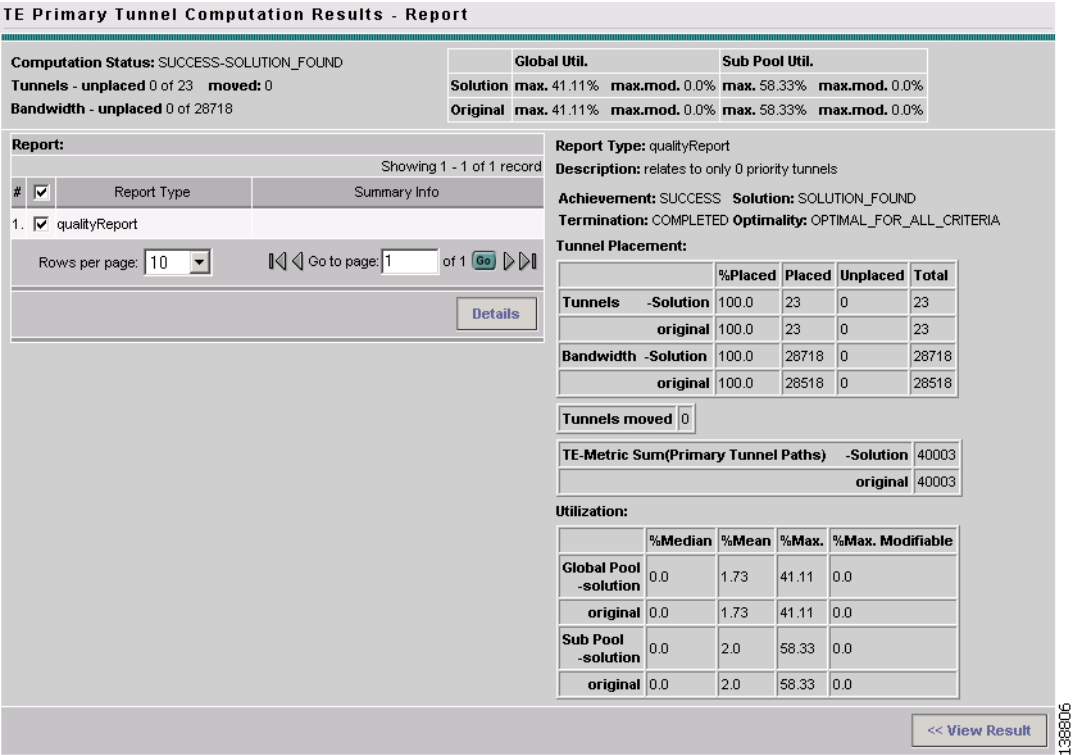
For an explanation of the various window elements, see [Planning Tools, page A-52](#).

A **qualityReport** is always generated. If the computation was successful, this will be the only report. If a warning or a violation was encountered, one or more warning or violation reports will be generated as well.

- Step 8** To view the contents of a placement report, select one of the reports and click the **Detail** button. In the case of a **qualityReport**, the TE Primary Tunnel Computation Results - Report (details) window in [Figure 6-25](#) appears in the report pane on the right.

For an example of a violation report, see [Figure 6-18](#).

Figure 6-25 TE Managed Primary Tunnels SR - Placement Report (Details)



For an explanation of the various window elements, see [Planning Tools](#), page A-52.

The qualityReport fields in the right window pane are described in [TE Primary Tunnel Computation Results - Report](#), page A-57.

- Step 9 Click << **View Result** to return to the Changes window and click **Save & Deploy** to save the change to the repository and implement the tunnel modifications on network.
- Step 10 The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

# Tunnel Repair

As changes are made to the bandwidth requirements or delay parameters of existing tunnels, inconsistencies can arise with the Tunnel Placement. You can run a Tunnel Repair to address such inconsistencies. The objective of Tunnel Repair is to try to move as few existing tunnels as possible to accommodate the changes.

Tunnel Repair can also be invoked from the Resource Management window (see [Chapter 4, “TE Resource Management”](#)).



In the following, the case of an edited tunnel has been used:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Create Managed TE Tunnel**.
- Step 2** Click **Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window appears as shown in [Figure 6-2](#).
- Tunnel Repair can be used in two ways:
- When one or more tunnels have been created or their attributes altered (see [Create Primary Tunnel, page 6-2](#)), Tunnel Repair can be activated by selecting **Proceed with Changes >> > Tunnel Repair**.
  - When no changes have taken place, Tunnel Repair can be accessed by selecting **Placement Tools > Tunnel Repair**.
- Step 3** As an example, let us say that a new primary tunnel SR has been created. Run Tunnel Repair on the modified tunnels from the TE Managed Primary Tunnels SR window ([Figure 6-12](#)) by navigating **Proceed with Changes -> Tunnel Repair**
- The Movable Tunnel Selection window shown in [Figure 6-26](#) appears.

**Figure 6-26 Movable Tunnel Selection - Repair**

#	<input type="checkbox"/> Movable	Allow Reroute	Tunnel ID	T#	Head	Dest	Policy	BW
1.	<input type="checkbox"/> NA	false	ISC-P1	2	isctmp11	isctmp10	ISC-P1-isctmp11:tunnel-te2	2
2.	<input type="checkbox"/> NA	false	ISC-P2	1000	isctmp11	isctmp1	ISC-P2-isctmp11:tunnel-te1000	200
3.	<input type="checkbox"/> NA	false	ISC-P122	1003	isctmp11	isctmp12	ISC-P122-isctmp11:tunnel-te1003	500000
4.	<input type="checkbox"/> NA	false	ISC-P123	1004	isctmp11	isctmp8	ISC-P122-isctmp11:tunnel-te1003	500
5.	<input type="checkbox"/> NA	false	ISC-P3	1	isctmp10	isctmp6	ISC-P2-isctmp11:tunnel-te1000	1000

For an explanation of the various window elements, see [Planning Tools, page A-52](#).

- Step 4** Set the tunnels that should be movable.

Tunnel Repair will only move existing tunnels if it has to. If you do not want certain tunnels to be moved during Tunnel Repair, these tunnels should be explicitly excluded from the selected list of movable tunnels.

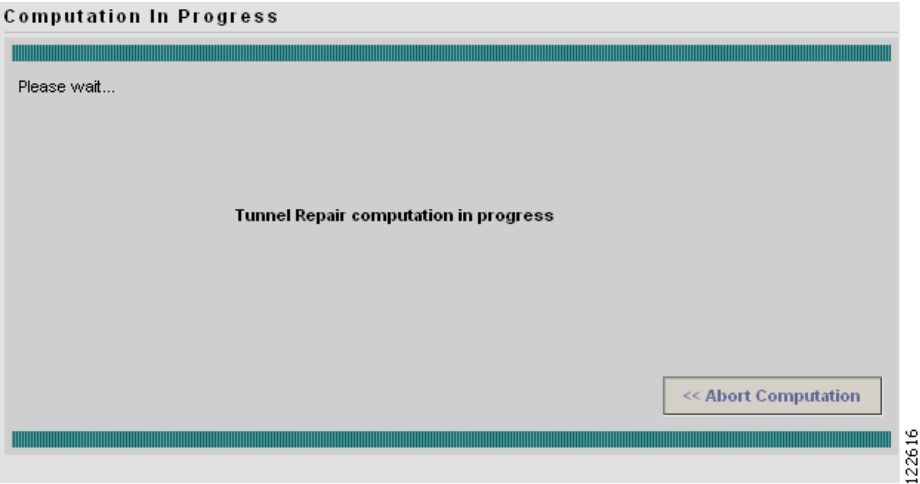
You can also specify a limit on the maximum number of tunnel moves that are acceptable using the **Maximum number of tunnel moves** field.



**Note** It is not necessary to set modified tunnels to be movable as these are movable by default.

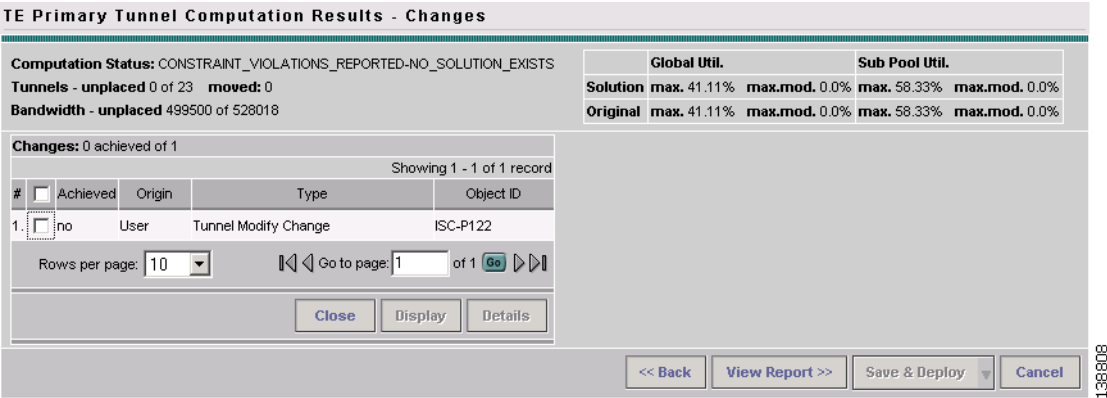
**Step 5** Click **Proceed >>**. The Computation In Progress window shown in [Figure 6-27](#) appears.

**Figure 6-27** Computation In Progress - Repair



To abort the computation and return to the previous window, click **<< Abort Computation**. The TE Primary Tunnel Computation Results - Changes window shown in [Figure 6-28](#) appears.

**Figure 6-28** TE Primary Tunnel Computation Results - Repair Changes



For an explanation of the various window elements, see [Planning Tools, page A-52](#).



**Note** Certain attributes, such as Description, that do not impact the computation carried out by the placement tools and updates to these are not displayed in the Computation Result Window.

- Step 6** To obtain detailed information about the tunnel and whether the change request was achieved, select the specific tunnel and click **Detail**. The detail section in the right side of the window appears as shown in [Figure 6-29](#).

**Figure 6-29** TE Primary Tunnel Computation Results - Repair Changes (Details)

**TE Primary Tunnel Computation Results - Changes**

**Computation Status:** CONSTRAINT\_VIOLATIONS\_REPORTED-NO\_SOLUTION\_EXISTS  
**Tunnels -** unplaced 0 of 23 **moved:** 0  
**Bandwidth -** unplaced 499500 of 528018

**Changes:** 0 achieved of 1  
 Showing 1 - 1 of 1 record

#	Achieved	Origin	Type	Object ID
1.	<input checked="" type="checkbox"/> no	User	Tunnel Modify Change	ISC-P122

Rows per page: 10 Go to page: 1 of 1

Buttons: Close Display Details

**Change Type:** Tunnel Modify Change  
**Achieved:** no  
**Description:** Request to modify one or more attributes of an existing tunnel

**Requested Tunnel**  
**ID:** isctmp11:tunnel-te1003  
**Head:** isctmp11  
**Tail:** isctmp12  
**Policy:** ISC-P122-isctmp11:tunnel-te1003  
**Bandwidth:** 500000  
**Path:** isctmp11-isctmp12-1

Changed Attributes	New Value	Achieved
BMV	500000	no

Buttons: << Back View Report >> Save & Deploy Cancel

For an explanation of the various window elements, see [Planning Tools, page A-52](#).

- Step 7** To view a repair report, click **View Report >>**. The TE Primary Tunnel Computation Results - Report window in [Figure 6-30](#) appears.

**Figure 6-30** TE Primary Tunnel Computation Results - Repair Report

**TE Primary Tunnel Computation Results - Report**

**Computation Status:** CONSTRAINT\_VIOLATIONS\_REPORTED-NO\_SOLUTION\_EXISTS  
**Tunnels -** unplaced 0 of 23 **moved:** 0  
**Bandwidth -** unplaced 499500 of 528018

**Report:**  
 Showing 1 - 2 of 2 records

#	Report Type	Summary Info
1.	<input checked="" type="checkbox"/> qualityReport	
2.	<input type="checkbox"/> violationLinkPoolOversubscribed	isctmp11/POS0/2/0/0,GLOBAL_POOL

Rows per page: 10 Go to page: 1 of 1

Buttons: Details

Button: << View Result

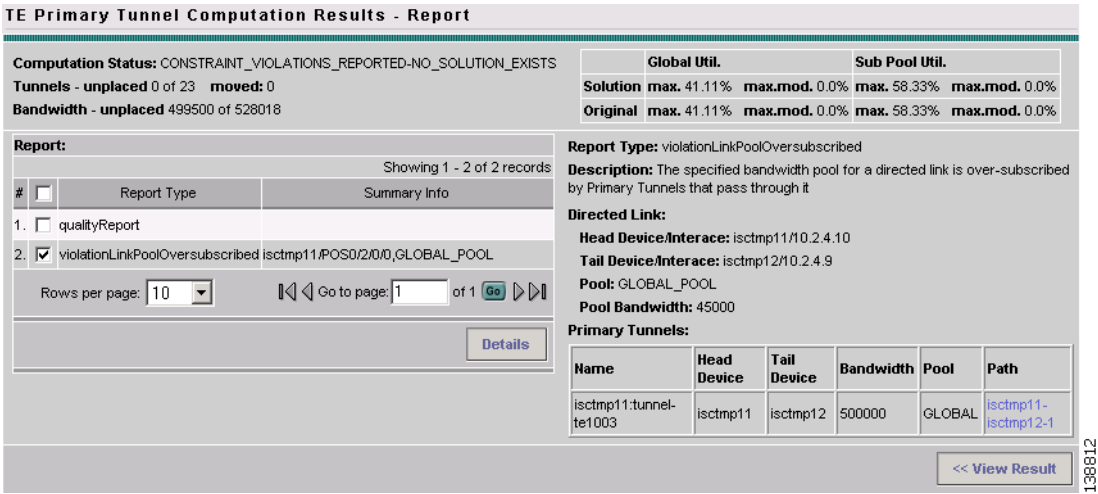
For an explanation of the various window elements, see [Planning Tools, page A-52](#).

A **qualityReport** is always generated. If the computation was successful, this will be the only report. If a warning or a violation was encountered, one or more warning or violation reports will also be generated.

- Step 8** To view the contents of the repair report, click the **Detail** button. In the case of a **qualityReport**, the TE Primary Tunnel Computation Results - Report (details) window in [Figure 6-31](#) appears.

For an example of a violation report, see [Figure 6-18](#).

**Figure 6-31** TE Managed Primary Tunnels SR - Repair Report (Details)



For an explanation of the various window elements, see [Planning Tools](#), page A-52.

The report fields in the right window pane are described for each report in [Appendix C, “Warnings and Violations.”](#)

- Step 9** Click << **View Result** to return to the Changes window and click **Save & Deploy** to save the change to the repository and implement the tunnel modifications on network.
- Step 10** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

# Grooming

The purpose of grooming is to analyze the tunnel pathing with respect to the network elements and optimize resource allocation.

Grooming is not available when change requests have been created. In that case, only the placement tools under **Proceed with Changes >>** will be available.

To perform grooming on the network, use the following steps:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Create Managed TE Tunnel**.
- Step 2** Click **Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window appears as shown in [Figure 6-2](#).
- Step 3** Run Grooming by navigating **Placement Tools -> Groom**
- The Movable Tunnel Selection window shown in [Figure 6-32](#) appears.

Figure 6-32 Movable Tunnel Selection

**Movable Tunnel Selection**

Computation Type: Grooming

Maximum computation duration (Timeout in sec) \*: 100

Number of reroutable tunnels selected as movable: 0 of 0    Non-reroutable tunnels 23

Show Tunnels with: All matching \* Find

Showing 1 - 5 of 23 records

#	<input type="checkbox"/> Movable	Allow Reroute	Tunnel ID	T#	Head	Dest	Policy	BW
1.	<input type="checkbox"/> NA	false	ISC-P1	2	isctmp11	isctmp10	ISC-P1-isctmp11:tunnel-te2	2
2.	<input type="checkbox"/> NA	false	ISC-P2	1000	isctmp11	isctmp1	ISC-P2-isctmp11:tunnel-te1000	200
3.	<input type="checkbox"/> NA	false	ISC-P122	1003	isctmp11	isctmp12	ISC-P122-isctmp11:tunnel-te1003	500
4.	<input type="checkbox"/> NA	false	ISC-P123	1004	isctmp11	isctmp8	ISC-P122-isctmp11:tunnel-te1003	500
5.	<input type="checkbox"/> NA	false	ISC-P3	1	isctmp10	isctmp6	ISC-P2-isctmp11:tunnel-te1000	1000

Rows per page: 5    Go to page: 1 of 5 Go

Set Movable    Set Unmovable

<< Back    Proceed >>    Cancel

Note: \* - Required Field

138813

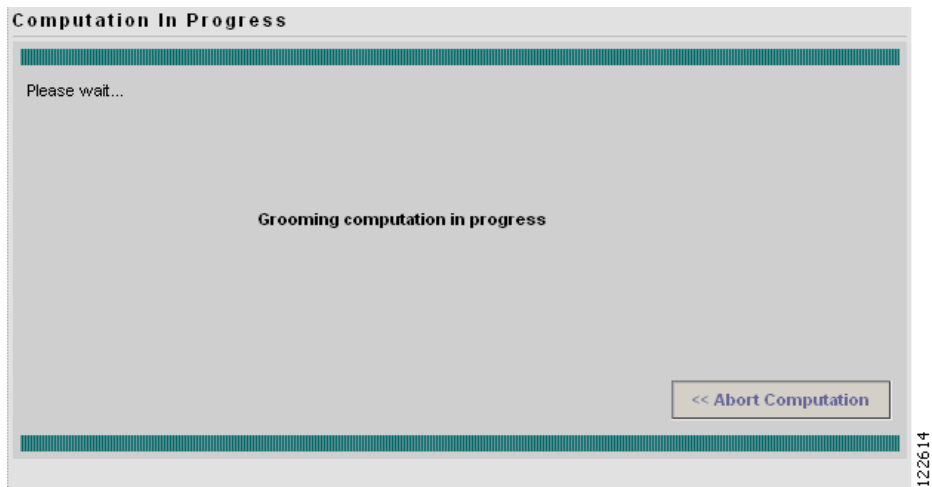
For an explanation of the various window elements, see [Planning Tools, page A-52](#).

**Step 4** Set the tunnels that should be movable.

As with Tunnel Repair, Grooming will only move existing tunnels if it has to. If you do not want certain tunnels to be moved during the Grooming process, these tunnels should be explicitly excluded from the selected list of movable tunnels.

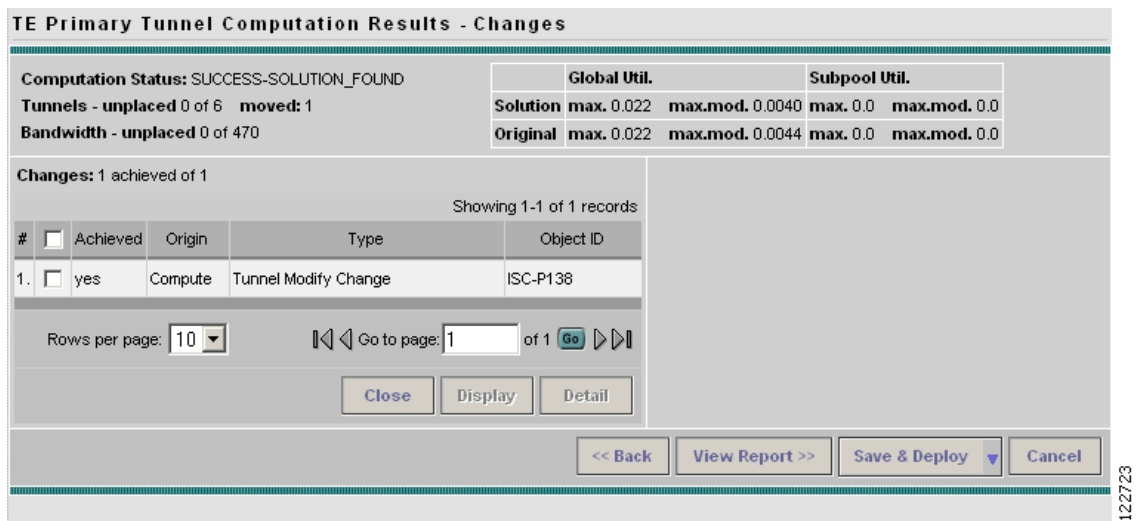
**Step 5** Click **Proceed >>**. The Computation In Progress window shown in [Figure 6-33](#) appears.

**Figure 6-33** Computation In Progress - Grooming



To abort the computation and return to the previous window, click << **Abort Computation**. The TE Primary Tunnel Computation Results - Changes window shown in [Figure 6-34](#) appears.

**Figure 6-34** TE Primary Tunnel Computation Results - Grooming Changes



For an explanation of the various window elements, see [Planning Tools, page A-52](#).



**Note**

Certain attributes, such as Description, that do not impact the computation carried out by the placement tools and updates to these are not displayed in the Computation Result Window.

**Step 6**

To obtain detailed information about the Grooming and whether it succeeded, select the specific tunnel and click **Detail**. The detail section in the right side of the window appears as shown in [Figure 6-35](#).

Figure 6-35 TE Primary Tunnel Computation Results - Grooming Changes (Details)

**TE Primary Tunnel Computation Results - Changes**

Computation Status: SUCCESS-SOLUTION\_FOUND  
Tunnels - unplaced 0 of 6 moved: 1  
Bandwidth - unplaced 0 of 470

		Global Util.		Subpool Util.	
Solution	max. 0.022	max.mod. 0.0040	max. 0.0	max.mod. 0.0	
Original	max. 0.022	max.mod. 0.0044	max. 0.0	max.mod. 0.0	

Changes: 1 achieved of 1  
Showing 1-1 of 1 records

#	✓	Achieved	Origin	Type	Object ID
1.	✓	yes	Compute	Tunnel Modify Change	ISC-P138

Rows per page: 10 Go to page: 1 of 1

Change Type: Tunnel Modify Change  
Achieved: yes  
Description: Request to modify one or more attributes of an existing tunnel

**Requested Tunnel**  
ID: isctmp6:Tunnel2  
Head: isctmp6  
Tail: isctmp7  
Policy: ISC-P2-isctmp2:Tunnel44  
Bandwidth: 100  
Path: Computed Path

Changed Attributes	New Value	Achieved
TE_EXPLICIT_PATH_ID	Computed Path	yes

Close Display Detail << Back View Report >> Save & Deploy Cancel

For an explanation of the various window elements, see [Planning Tools, page A-52](#).

- Step 7** To view a Grooming report, click **View Report >>**. The TE Primary Tunnel Computation Results - Report window in [Figure 6-30](#) appears.

Figure 6-36 TE Primary Tunnel Computation Results - Grooming Report

**TE Primary Tunnel Computation Results - Report**

Computation Status: SUCCESS-SOLUTION\_FOUND  
Tunnels - unplaced 0 of 6 moved: 1  
Bandwidth - unplaced 0 of 470

		Global Util.		Subpool Util.	
Solution	max. 0.022	max.mod. 0.0040	max. 0.0	max.mod. 0.0	
Original	max. 0.022	max.mod. 0.0044	max. 0.0	max.mod. 0.0	

**Report:**  
Showing 1-1 of 1 records

#	Report Type	Summary Info
1.	qualityReport	

Rows per page: 10 Go to page: 1 of 1

Detail << View Result

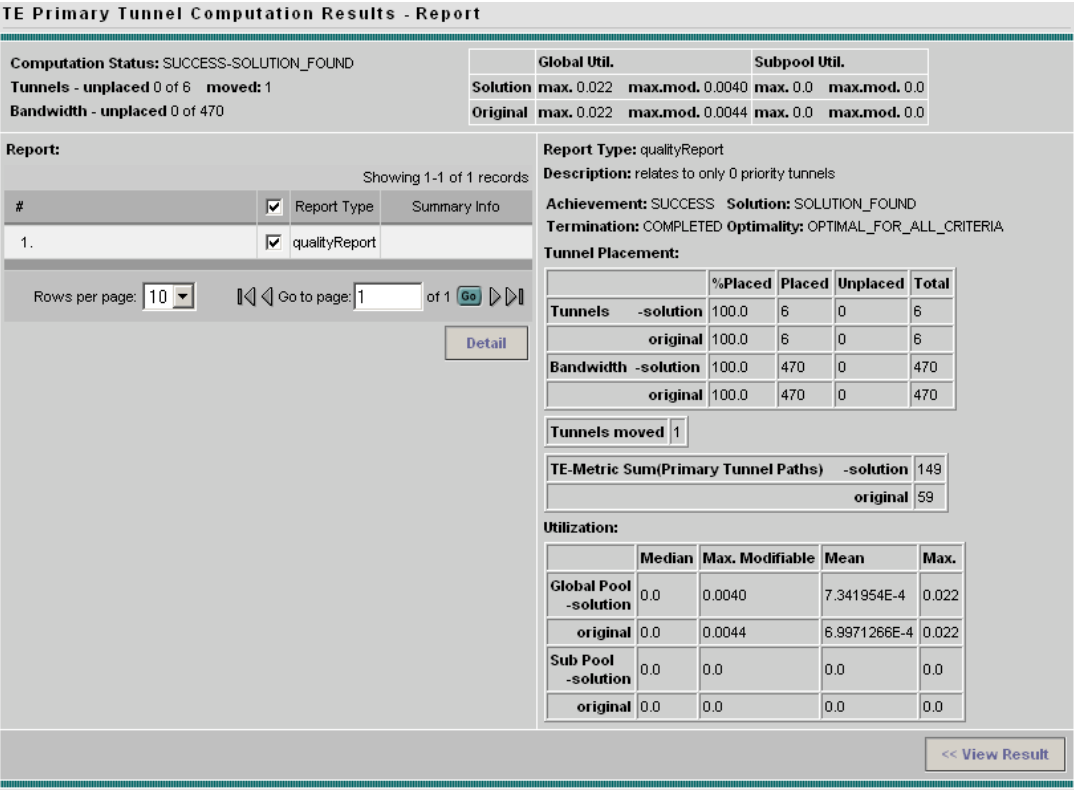
For an explanation of the various window elements, see [Planning Tools, page A-52](#).

A **qualityReport** is always generated. If the computation was successful, this will be the only report. If a warning or a violation was encountered, one or more warning or violation reports will also be generated.

- Step 8** To view the contents of the Grooming report, click the **Detail** button. In the case of a **qualityReport**, the TE Primary Tunnel Computation Results - Report (details) window in [Figure 6-37](#) appears.

For an example of a violation report, see [Figure 6-18](#).

Figure 6-37 TE Managed Primary Tunnels SR - Grooming Report (Details)



For an explanation of the various window elements, see [Planning Tools](#), page A-52.

The report fields in the right window pane are described for each report in [Appendix C](#), “Warnings and Violations.”

**Step 9** Click << **View Result** to return to the Changes window and click **Save & Deploy** to save the change to the repository and implement the tunnel modifications on the network.

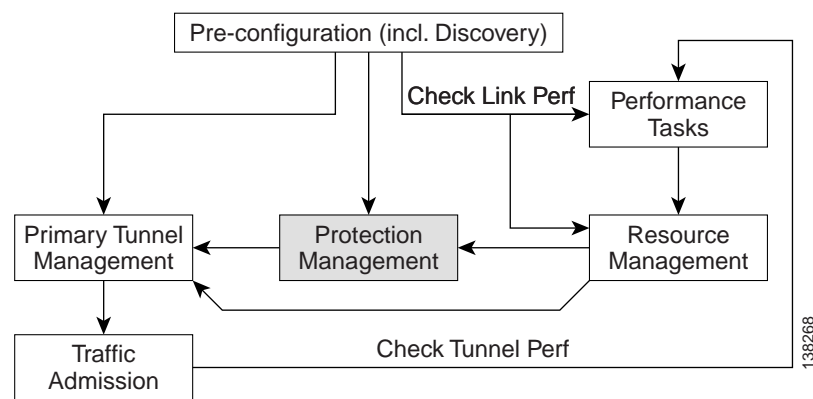
**Step 10** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B](#), “Managing Service Requests.”





## Protection Planning



This chapter describes the process of creating and managing the protection of network elements using automated protection tools. See [Chapter 5, “Basic Tunnel Management”](#) for a description of the process using the basic tools.

This chapter includes the following sections:

- [Overview, page 7-2](#)
- [SRLG Operations, page 7-3](#)
  - [Create SRLG, page 7-3](#)
  - [Edit SRLG, page 7-5](#)
  - [Delete SRLG, page 7-5](#)
- [Configure Element Protection, page 7-5](#)
- [Protection Tools, page 7-7](#)
  - [Compute Backup, page 7-7](#)
  - [Audit Protection, page 7-12](#)
  - [Audit SR, page 7-14](#)

# Overview

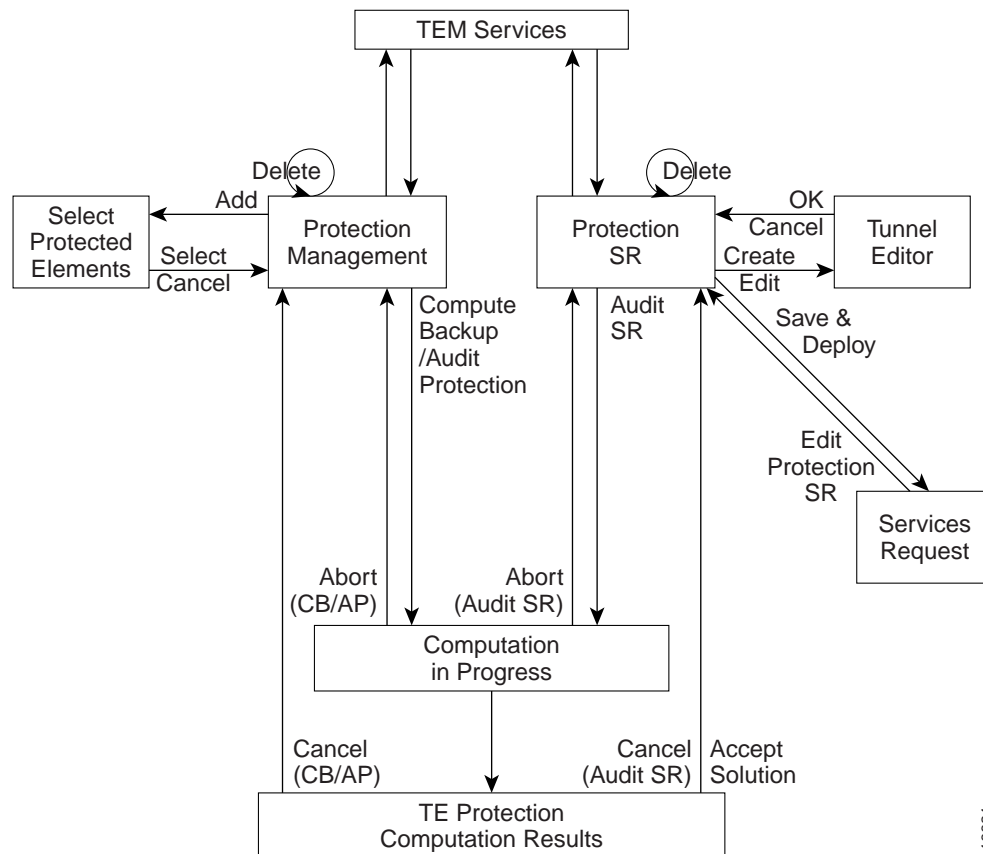
The purpose of protection planning is to protect selected elements in the network (links, routers, or SRLGs) against failure.

The first step is to identify the elements that must be protected and then invoke the protection tools to compute the protected tunnels. From the computation, the system responds for each element with either a set of tunnels that protect the element or a set of violations and warnings that help the user to determine why it could not be protected.

For successfully protected elements the tunnels can be deployed on the network. For elements that could not be protected, the protection is either ignored or the constraints are altered on the protection case. More specifically, this can involve changing the TE bandwidth settings of the links associated to the element and then rerunning the protection computation on the altered network.

An overview of the protection management processes is provided in [Figure 7-1](#).

**Figure 7-1** Protection Management Processes



116621

# SRLG Operations

It is not uncommon for links to have identical physical characteristics, such as being physically located in the same conduit, or being connected to the same hardware. As a result, they could fail as a group during a single failure event. A Shared-Risk Link Group (SRLG) addresses this problem by identifying links that could fail together.

After SRLG modifications (create, edit, delete), use the protection planning functions in the **TE Protection Management** window to ensure that adequate protection is available on the network.



**Note**

If you include a non-POS interface of an IOS-XR device in an SRLG, the SRLG cannot be protected.

## Create SRLG

Creating an SRLG is only necessary if a shared risk link group has been identified and it must be protected.

To create an SRLG, use the following steps:

- Step 1 Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2 Click **TE SRLGs**. The TE SRLG List window in [Figure 7-2](#) appears.

**Figure 7-2** TE SRLG List

**TE SRLG List**

Provider: Provider2

Show SRLG with  matching

Showing 1 - 2 of 2 records

#	<input type="checkbox"/>	SRLG Name
1.	<input type="checkbox"/>	srlg1
2.	<input type="checkbox"/>	srlg2

Rows per page:

Go to page:  of 1

For an explanation of the various window elements, see [Create/Edit TE SRLG, page A-31](#).

- Step 3 To create an SRLG in the **TE SRLG List**, click **Create**. The TE SRLG Editor window in [Figure 7-3](#) appears.

Figure 7-3 TE SRLG Editor

TE SRLG Editor

Provider Name \*: Provider2

SRLG Name \*: srlg1

Links :

Showing 1 - 5 of 9 records

#	<input type="checkbox"/>	Device From	Label	Device To
1.	<input type="checkbox"/>	isctmp8	10.2.2.126<->10.2.2.113	isctmp7
2.	<input type="checkbox"/>	isctmp1	10.2.3.85<->10.2.3.86	isctmp2
3.	<input type="checkbox"/>	isctmp1	10.2.3.89<->10.2.3.90	isctmp3
4.	<input type="checkbox"/>	isctmp1	10.2.2.129<->10.2.2.142	isctmp3
5.	<input type="checkbox"/>	isctmp1	10.2.3.93<->10.2.3.94	isctmp7

Rows per page: 5

Go to page: 1 of 2 Go

Add Link Remove Link

Save Cancel

138815

For an explanation of the various window elements , see [Create/Edit TE SRLG, page A-31](#).

**Step 4** Specify an **SRLG Name**.

**Step 5** Click **Add Link**. The Links associated with SRLG window in [Figure 7-4](#) appears.

Figure 7-4 Links associated with SRLG

Links associated with SRLG

Show Links with: Device Name Matching \* Find

Showing 1 - 10 of 32 records

#	<input type="checkbox"/>	From Device	Link	To Device
1.	<input type="checkbox"/>	isctmp4	10.2.3.117<->10.2.3.118	isctmp9
2.	<input type="checkbox"/>	isctmp7	10.2.2.33<->10.2.2.46	isctmpe3
3.	<input type="checkbox"/>	isctmp4	10.2.3.82<->10.2.3.81	isctmp9
4.	<input type="checkbox"/>	isctmp4	10.2.3.106<->10.2.3.105	isctmp3
5.	<input type="checkbox"/>	isctmp4	10.2.2.254<->10.2.2.241	isctmp3
6.	<input type="checkbox"/>	isctmp4	10.2.3.78<->10.2.3.77	isctmp9
7.	<input type="checkbox"/>	isctmp5	10.2.2.81<->10.2.2.94	isctmp4
8.	<input type="checkbox"/>	isctmp6	10.2.2.78<->10.2.2.65	isctmp5
9.	<input type="checkbox"/>	isctmp6	10.2.2.222<->10.2.2.209	isctmp4
10.	<input type="checkbox"/>	isctmp2	10.2.2.62<->10.2.2.49	isctmp5

Rows per page: 10

Go to page: 1 of 4 Go

Select Cancel

122637

For an explanation of the various window elements , see [Create/Edit TE SRLG, page A-31](#).

- Step 6** Select one or more links and click **Select**. The corresponding link information is added to the link list and the Select window closes and returns to the SRLG editor.
  - Step 7** Click **Save** to save the SRLG. This closes the SRLG editor and brings back the TE SRLG List as the active window, where the newly created SRLG is listed.
- 

## Edit SRLG

To edit an SRLG, use the following steps:

- Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
  - Step 2** Click **TE SRLGs**. The TE SRLG List window in [Figure 7-2](#) appears.
  - Step 3** To edit an SRLG in the TE SRLG List, from the TE SRLG List window select the SRLG that you want to modify and click **Edit**. The TE SRLG Editor window in [Figure 7-3](#) appears.
  - Step 4** Use **Add Link** and **Remove Link** to adjust to the desired set of links for the selected SRLG.
  - Step 5** Click **Save** to save the changes.
- 

## Delete SRLG

To delete an SRLG, use the following steps:

- Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
  - Step 2** Click **TE SRLGs**. The TE SRLG List window in [Figure 7-2](#) appears.
  - Step 3** To delete an SRLG in the TE SRLG List, from the TE SRLG List window select the SRLG(s) that you want to delete and click **Delete**. The Delete Confirm window appears.
  - Step 4** Click **Delete** to confirm. The Delete Confirm window closes. After the TE SRLG List window has been updated, the deleted SRLG no longer appears in the SRLG list.
- 

## Configure Element Protection

Before a protection computation can be performed, it is necessary to configure the network element protection.

To do so, use the following steps:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Protected Elements**.

The TE Protection Management window in [Figure 7-5](#) appears.

**Figure 7-5** *TE Protection Management*

TE Protection Management

Provider: Provider1

Show: All Elements Matching: \* Find

Showing 0 of 0 records

#	<input type="checkbox"/>	Element Name	Type	Protection Status
---	--------------------------	--------------	------	-------------------

Rows per page: 10 Go to page: 1 of 1 Go

Close Display Compute Backup Audit Protection Add Delete Cancel

For an explanation of the various window elements, see [Protection Management, page A-35](#).

**Step 2** First, decide which network elements must be protected.

In the TE Protection Management window, click **Add** to add a protection element (link, node, or SRLG). The Select Protection Elements window in [Figure 7-6](#) appears.



**Note**

If a link, node or SRLG contains a non-POS interface on an IOS-XR device, the element is selectable as a protected element and backup tunnels will be generated, but the deployment will fail due to a restriction is IOS-XR 3.2. For nodes, all nodes connected to an IOS-XR device must have POS interfaces. If even one node in an SRLG has a non-POS interface, that SRLG cannot be protected.

Links that are connected to non-Cisco devices cannot be protected and will, therefore, not show in the Select protection elements window. Likewise, non-Cisco devices and SRLGs that contain links to non-Cisco devices cannot be protected and are excluded from the selection.

**Figure 7-6**      **Select Protection Elements**

Protection Elements for **Provider1**

Show:  Matching:

Showing 1 - 10 of 45 records

#	<input type="checkbox"/>	Element Name	Type
1.	<input type="checkbox"/>	10.2.3.117<->10.2.3.118	Link
2.	<input type="checkbox"/>	10.2.2.81<->10.2.2.94	Link
3.	<input type="checkbox"/>	10.2.3.78<->10.2.3.77	Link
4.	<input type="checkbox"/>	10.2.2.254<->10.2.2.241	Link
5.	<input type="checkbox"/>	10.2.3.106<->10.2.3.105	Link
6.	<input type="checkbox"/>	10.2.3.82<->10.2.3.81	Link
7.	<input type="checkbox"/>	10.2.2.33<->10.2.2.46	Link
8.	<input type="checkbox"/>	10.2.3.70<->10.2.3.69	Link
9.	<input type="checkbox"/>	10.2.3.74<->10.2.3.73	Link
10.	<input type="checkbox"/>	isctmp1	Node

Rows per page:  Go to page:  of 5

For an explanation of the various window elements, see [Protection Management, page A-35](#).

- Step 3**      Select one or more elements to be protected and click **Select**. The Select Protection Element window closes and the TE Protection Management window reappears.

Next, decide which protection tools should be applied.

## Protection Tools

Relying on manual creation of backup tunnels as described in [Chapter 5, “Basic Tunnel Management”](#) has its limitations, not just for larger and more complicated networks.

The protection tools available in ISC TEM provide a number of tools that automatically compute and verify protection of specified network elements.



### Note

Certain attributes, such as Description, that do not impact the computation carried out by these tools and updates to these are, therefore, not displayed in the Computation Result Window.

## Compute Backup

Compute Backup is used to let ISC TEM automatically compute the necessary backup tunnels to protect specified network elements. The manual process is described in [Chapter 5, “Basic Tunnel Management.”](#)

To run Compute Backup, use the following steps:

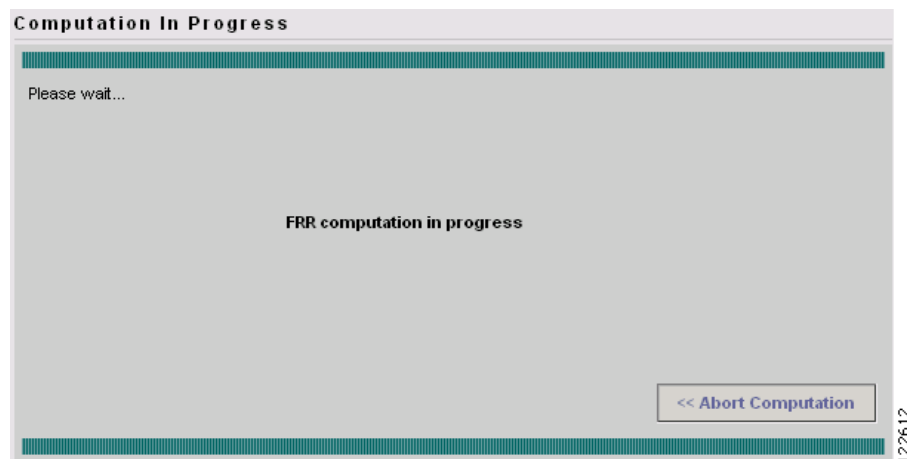
- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Protected Elements**.
- Step 2** Configure the necessary protection elements as described in [Configure Element Protection, page 7-5](#).
- Step 3** If you only want to perform Compute Backup on selected elements, select one or more elements on which to calculate a backup path.

Click **Compute Backup** and select one of the following:

- All Elements
- Selected Elements

The Computation In Progress window shown in [Figure 7-7](#) appears.

**Figure 7-7** *FRR Computation In Progress - Compute Backup*



To abort the computation and return to the previous window, click << **Abort Computation**.

- Step 4** The TE Protection Computation window in [Figure 7-8](#) appears.



**Figure 7-8** TE Protection Computation Results

**TE Protection Computation Results**

**Element:**

Show  with name matching

Showing 1 - 4 of 4 records

#	Element Name	Type	Report	Status
1.	10.2.2.33<->10.2.2.46	Link		NoSolutionExists
2.	10.2.2.33<->10.2.2.46	Link	violationNoBackupTunnels	NoSolutionExists
3.	10.2.2.33<->10.2.2.46	Link	violationNoBackupTunnels	NoSolutionExists
4.	isctmpe4	Node		ValidTunnels

Rows per page:  Go to page:  of 1

**Backup Tunnels:**

Op	Tunnel ID	Head	Dest	T#	BVV	Path	Protection Type	Report
<input type="button" value="Accept Solution"/> <input type="button" value="Cancel"/>								

122749

For an explanation of the various window elements, see [Compute Backup, page A-37](#).

**Note**

Certain attributes, such as Description, that do not impact the computation carried out by the protection tools and updates to these are not displayed in the Computation Result Window.

**Step 5**

Select a row corresponding to a specific warning or violation and click **Detail** to display a detailed description in the right pane and backup tunnels associated with the selected item in the bottom pane as shown in [Figure 7-9](#).

For a description of warnings and violations, see [Appendix C, “Warnings and Violations.”](#)

Figure 7-9 TE Protection Computation Results with Backup Tunnels

**TE Protection Computation Results**

**Element:**

Show  with name matching

Showing 1 - 10 of 19 records

#	<input type="checkbox"/>	Element Name	Type	Report	Status
1.	<input type="checkbox"/>	isctmp7	Node		NoSolutionExists
2.	<input checked="" type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	NoSolutionExists
3.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	NoSolutionExists
4.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	NoSolutionExists
5.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	NoSolutionExists
6.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	NoSolutionExists
7.	<input type="checkbox"/>	isctmp6	Node		NoSolutionExists
8.	<input type="checkbox"/>	isctmp6	Node	violationNoBackupTunnels	NoSolutionExists
9.	<input type="checkbox"/>	isctmp6	Node	violationNoBackupTunnels	NoSolutionExists
10.	<input type="checkbox"/>	isctmp6	Node	violationNoBackupTunnels	NoSolutionExists

Rows per page:  Go to page:  of 2

**Violation and Warning:**

**Report Type:** violationNoBackupTunnels

**Description:** There are no backup tunnels protecting this flow through the element

**Flow:**

Maximum Bandwidth	Head Links	Through Router	Tail Router	Type
550	isctmp8/1 0.2.3.50	isctmp7	isctmpe3	NNHOP

**Backup Tunnels:**

Op	Tunnel ID	Head	Dest	T#	BW	Path	Protection Type	Report
ADD	ISC-B330	isctmp1	isctmp8		200	Computed Path	Protection	
ADD	ISC-B328	isctmp8	isctmp1		550	Computed Path	Protection	
ADD	ISC-B329	isctmp8	isctmp1		1000	Computed Path	Protection	
DELETE	ISC-B42	isctmp1	isctmp6	4	200	Bug-test2	Activating	
DELETE	ISC-B48	isctmp8	isctmpe4	3	1550	isctmp8->isctmpe4-1	Activating	

For an explanation of the various window elements, see [Compute Backup](#), page A-37.

The **Backup Tunnel** table displays which new protection tunnels are required and any existing tunnels that should be kept or deleted for each element.

- Step 6** In the TE Protection Computation Results window, check whether the proposed protection solution is acceptable. If so, click **Accept Solution**. The TE Protection SR window in [Figure 7-10](#) appears with all tunnel additions and deletions computed by the system.

Figure 7-10 TE Protection SR - Computed Path

**TE Protection SR**

SR Job ID: 2      Provider: p0      SR State: REQUESTED  
 SR ID: New      Creator:      Type: ADD

Description:

Show  Tunnels with  Matching

Showing 1 - 10 of 20 records

#	<input type="checkbox"/>	Op	Tunnel ID	T#	Head	Dest	Protects	BW Quota	Deploy Status	Conformance
1.	<input type="checkbox"/>	ADD	ISC-B316		isctmp6	isctmp5		2000	REQUESTED	Yes
2.	<input type="checkbox"/>	ADD	ISC-B317		isctmp4	isctmp2	isctmp5	2000	REQUESTED	Yes
3.	<input type="checkbox"/>	ADD	ISC-B318		isctmp6	isctmp2	isctmp5	2000	REQUESTED	Yes
4.	<input type="checkbox"/>	ADD	ISC-B319		isctmp6	isctmp4	isctmp5	1000	REQUESTED	Yes
5.	<input type="checkbox"/>	ADD	ISC-B320		isctmp2	isctmp4	isctmp5	1000	REQUESTED	Yes
6.	<input type="checkbox"/>	ADD	ISC-B321		isctmp4	isctmp8	isctmp6	100	REQUESTED	Yes
7.	<input type="checkbox"/>	ADD	ISC-B322		isctmp4	isctmp2	isctmp6	500	REQUESTED	Yes
8.	<input type="checkbox"/>	ADD	ISC-B323		isctmp4	isctmp5	isctmp6	500	REQUESTED	Yes
9.	<input type="checkbox"/>	ADD	ISC-B324		isctmp2	isctmp8	isctmp6	50	REQUESTED	Yes
10.	<input type="checkbox"/>	ADD	ISC-B325		isctmp2	isctmp5	isctmp6	50	REQUESTED	Yes

Rows per page:       Go to page:  of 2

For an explanation of the various window elements, see [Create TE Backup Tunnel, page A-59](#).

Optionally, you can make tunnel changes here and then run **Audit SR** to ensure that you have the desired level of protection before you deploy (see [Audit SR, page 7-14](#)).

**Step 7** Click **Save & Deploy** to deploy the new tunnel SR to the network.



**Note**

When you click **Save & Deploy**, a background process is started. To avoid a potential conflict with another deployment, wait until the SR has completed the Requested and Pending states before deploying another SR with **Save & Deploy**. To see the state of deployment, go to the Service Request window under Inventory and Connection Manager or open the Task Manager under Monitoring.



**Note**

With the exception of TE Traffic Admission SRs, TE SRs are always deployed immediately from the specific TE SR screen, not from the **Service Requests** page in **Inventory and Connection Manager**.

**Step 8** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) opens and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

If the SR does not go to the **Deployed** state, go to the Task Logs screen to see the deployment log (**Monitoring > Task Manager > Logs**) as described in [SR Deployment Logs, page 10-1](#).

## Audit Protection

As opposed to the Compute Backup tool described on page 7, Audit Protection does not attempt to create a backup solution. It seeks to verify protection of specified network elements with the current set of backup tunnels and reports any warnings or violations that are discovered. It is recommended that any time a change has been committed on the TE topology such as resources on TE links or SRLG membership, a protection audit be run to verify the protection status on all elements.

The computation will display the same computation result page as for Compute Backup. When you return from computation result page, the Protection Status column in the TE Protection Management window is updated to show the level of protection for each element.

This section describes the necessary steps to perform Audit Protection on one or more network elements.

To run Audit Protection, use the following steps:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Protected Elements**.

The TE Protection Management window in [Figure 7-5](#) appears.

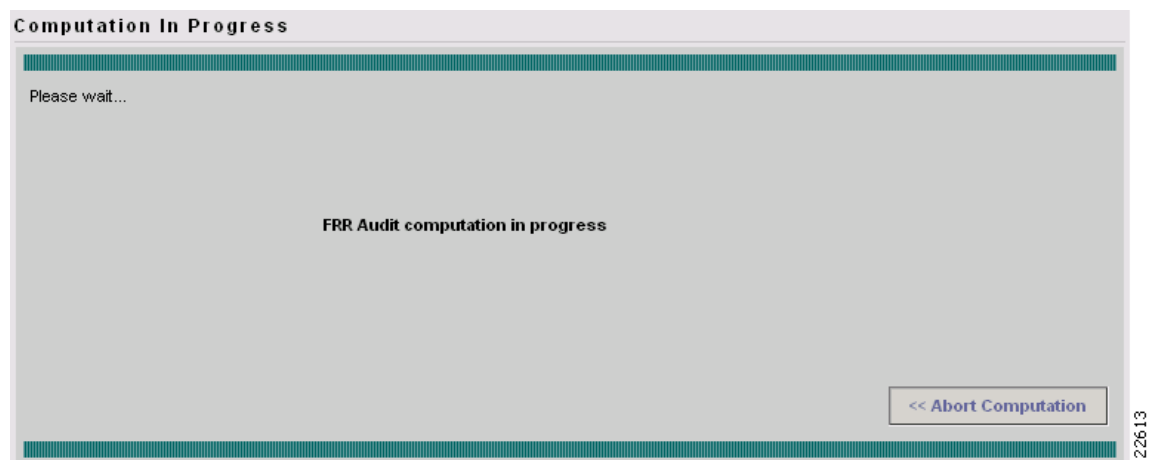
- Step 2** If you only want to perform Audit Protection on selected elements, select one or more tunnels on which to calculate a backup path.

Click **Audit Protection** and select one of the following:

- All Elements
- Selected Elements

The Computation In Progress window shown in [Figure 7-7](#) appears.

**Figure 7-11** *FRR Audit Computation in Progress - Audit Protection*



To abort the computation and return to the previous window, click **<< Abort Computation**.

The TE Protection Computation Results window in [Figure 7-12](#) appears.

**Figure 7-12** TE Protection Computation Results

**TE Protection Computation Results**

**Element:**

Show  with name matching

Showing 1 - 10 of 37 records

#	<input type="checkbox"/>	Element Name	Type	Report	Status
1.	<input type="checkbox"/>	isctmp7	Node		InvalidTunnels
2.	<input checked="" type="checkbox"/>	isctmp7	Node	violationBadBackupTunnel	InvalidTunnels
3.	<input type="checkbox"/>	isctmp7	Node	violationBadBackupTunnel	InvalidTunnels
4.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
5.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
6.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
7.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
8.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
9.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
10.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels

Rows per page:  Go to page:  of 4

**Violation and Warning:**

**Backup Tunnels:**

Op	Tunnel ID	Head	Dest	T#	BW	Path	Protection Type	Report

For an explanation of the various window elements, see [Compute Backup, page A-37](#).

**Note**

Certain attributes, such as Description, that do not impact the computation carried out by the protection tools and updates to these are not displayed in the Computation Result Window.

- Step 3** To view the backup tunnels for a particular element, select the element and click **Details**. The TE Protection Computation Results window in [Figure 7-13](#) appears.

122747

**Figure 7-13** TE Protection Computation Results with Backup Tunnels

**TE Protection Computation Results**

**Element:**

Show:  with name matching:

Showing 1 - 10 of 10 records

#	<input type="checkbox"/>	Element Name	Type	Report	Status
1.	<input type="checkbox"/>	isctmp7	Node		InvalidTunnels
2.	<input checked="" type="checkbox"/>	isctmp7	Node	violationBadBackupTunnel	InvalidTunnels
3.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
4.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
5.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
6.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
7.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
8.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
9.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
10.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels

Rows per page:

**Violation and Warning:**

**Report Type:** violationBadBackupTunnel  
**Description:** The tunnel does not protect a flow over this element

**Backup Tunnels:**

Op	Tunnel ID	Head	Dest	T#	BW	Path	Protection Type	Report
	ISC-B42	isctmp8	isctmp9	4	30000	isctmp8-isctmp9-3	Activating	yes

For an explanation of the various window elements, see [Compute Backup, page A-37](#).

- Step 4** Select a row corresponding to a specific warning or violation and click **Details** to display a detailed description in the right pane and backup tunnels associated with the selected item in the bottom pane as shown in [Figure 7-9](#).

Tunnels associated with a warning or violation are flagged in the **Report** column in the **Backup Tunnels** table in the bottom pane.

The **Accept Solution** button is greyed out because the audit does not provide a solution but rather an evaluation.

For a description of warnings and violations, see [Appendix C, “Warnings and Violations.”](#)

- Step 5** Click **Cancel** to return to the TE Protection Management window. The protection status is updated in the Protection Status column.

## Audit SR

Audit SR audits protection of all elements in the **TE Protection Management** window against backup tunnels in the TE Protection SR window.

This feature can be used to audit the protection for manually added, modified, and deleted tunnels in the TE Protection SR window before deploying them.

To audit a TE backup tunnel SR, use the following steps:

- Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2** Click **Create TE Backup Tunnel**. The **TE Protection SR** window in [Figure 7-14](#) appears.

Figure 7-14 TE Protection SR

**TE Protection SR**

SR Job ID: 9      Provider: Provider2      SR State: REQUESTED  
 SR ID: New      Creator:      Type: ADD

Description:

Show Existing Tunnels with All matching \* Find

Showing 1 - 5 of 47 records

#	Op	Tunnel ID	T#	Head	Dest	BW Quota	Deploy Status	Conformance
1.	<input type="checkbox"/>	ISC-B30	3	isctmp11	isctmp12	2	LOST	Yes
2.	<input type="checkbox"/>	ISC-B31	1001	isctmp11	isctmp8	30000	LOST	Yes
3.	<input type="checkbox"/>	ISC-B141	1002	isctmp11	isctmp8	30000	DEPLOYED	Yes
4.	<input type="checkbox"/>	ISC-B142	1005	isctmp11	isctmp12	1000	DEPLOYED	No
5.	<input type="checkbox"/>	ISC-B143	1000	isctmp12	isctmp5	1000	DEPLOYED	No

Rows per page: 5      Go to page: 1 of 10 Go

Close Display Details Create Edit Delete

Audit SR Save & Deploy Cancel

For an explanation of the various window elements, see [Create TE Backup Tunnel, page A-59](#).

**Step 3** To audit the protection SR, click **Audit SR**.



**Note** Audit SR will only be enabled if there are elements in the TE Protection Management window. If this is not the case, the **Audit SR** button will be disabled (grayed out).

The FRR Audit process begins and the TE Protection Computation Results window in [Figure 7-12](#) appears.

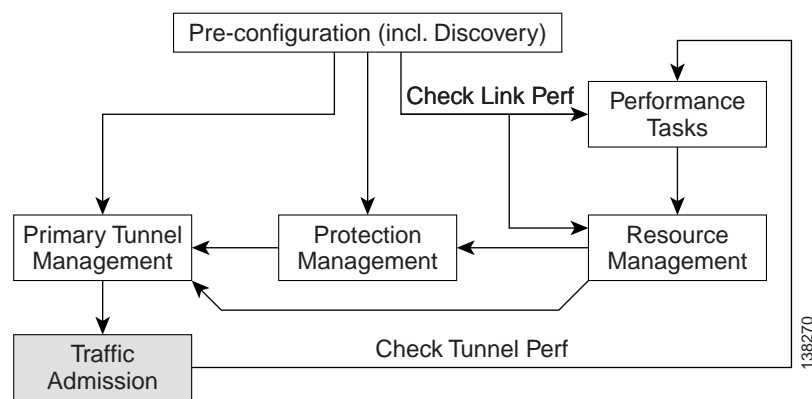
See [Audit Protection, page 7-12](#) for a description of the rest of the process. Detail and report windows are identical in these two processes.







# Traffic Admission



Traffic admission is the first step towards enabling services on TE tunnels. There are a number of mechanisms that can be used for forwarding traffic into a tunnel to provide basic IP connectivity. The current implementation of Cisco IP Solution Center Traffic Engineering Management (ISC TEM) uses static routing.

The TE Traffic Admission tool is used to assign traffic to traffic-engineered tunnels.

This chapter includes the following sections:

- [Overview, page 8-1](#)
- [Creating a TE Traffic Admission SR, page 8-2](#)
- [Deploying a TE Traffic Admission SR, page 8-4](#)
- [Other Traffic Admission SR Operations, page 8-5](#)
- [Viewing the SR State, page 8-5](#)

## Overview

Static routing is perhaps the simplest way of forwarding traffic into a tunnel. Traffic that matches a target destination prefix is routed into a particular tunnel.

While this achieves the basic goal of directing traffic into a given tunnel, this approach has limitations. First, the offering of differentiated Class-of-Service (CoS) treatment is limited to destination-based CoS. As each source PE serves as an aggregation point for a number of traffic flows, there is no way to restrict

which traffic receives preferential treatment to a destination since access to a tunnel is through general routing. Second, it does not generally provide a scalable solution because the static routing mechanism must capture both the large number of subnets that can be served by each PE router, and it must be able to further capture CoS treatment for each of these subnets.

Static routing works best if there is no need to provide differentiated CoS treatment by destination. That is, all packets destined for one or more particular prefixes all receive the same CoS.

## Creating a TE Traffic Admission SR

To create a TE Traffic Admission SR, use the following steps:

- Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**.
- Step 2 Click **TE Traffic Admission**.

The TE Traffic Admission Tunnel Selection window in [Figure 8-1](#) appears.

**Figure 8-1** TE Traffic Admission Tunnel Selection

The screenshot shows the Cisco IP Solution Center interface. The main title is "IP Solution Center". Below it are tabs for "Service Inventory", "Service Design", "Monitoring", "Diagnostics", and "Administration". The "Service Inventory" tab is selected. Under "Service Inventory", there are sub-tabs for "Inventory and Connection Manager", "Discovery", and "Device Console". The "Inventory and Connection Manager" sub-tab is selected. The main content area is titled "TE Traffic Admission Tunnel Selection". It shows a list of tunnels for "TE Provider Provider2". The list has columns for "#", "Tunnel ID", "T#", "Head", "Dest", "Op", "Type", "Policy", and "Deploy Status". The list contains 5 records, all with "DEPLOYED" status. The "Deploy Status" column is highlighted. At the bottom of the window, there are buttons for "Select" and "Cancel".

#	Tunnel ID	T#	Head	Dest	Op	Type	Policy	Deploy Status
1.	ISC-P1	2	isctmp11	isctmp10	ADD	Managed	ISC-P1-isctmp11:tunnel-te2	DEPLOYED
2.	ISC-P122	1003	isctmp11	isctmp12	ADD	Managed	ISC-P122-isctmp11:tunnel-te1003	DEPLOYED
3.	ISC-P149	1006	isctmp11	isctmp10	ADD	UnManaged	te_policy1	DEPLOYED
4.	ISC-P151	1007	isctmp11	isctmp10	ADD	UnManaged	te_policy1	DEPLOYED
5.	ISC-P4	2	isctmp10	isctmp1	ADD	Managed	ISC-P1-isctmp11:tunnel-te2	DEPLOYED

For an explanation of the various window elements, see [Select TE Tunnel for Admission, page A-64](#).

The TE Traffic Admission Tunnel Selection window lists all primary tunnels, both managed and unmanaged, that are not already associated with an admission SR.

The **Deploy Status** can be **Pending**, **Deployed**, or **Functional**.



### Note

Backup tunnels are not displayed in the TE Traffic Admission Tunnel Selection window.

- Step 3** Select a TE tunnel by clicking the corresponding radio button and clicking **Select**. The TE Traffic Admission SR window in [Figure 8-2](#) appears.

**Figure 8-2** TE Traffic Admission SR

For an explanation of the various fields and buttons, see [TE Traffic Admission SR, page A-65](#).

- Step 4** When filling out the form, if **Autoroute Announce** is set to **On**, indicate whether **Autoroute Metric** should be **Absolute** or **Relative**. You can also set an optional autoroute metric. For the relative metric, the range is -10 to 10, for the absolute metric, the range is 1 to 2147483647.

When clicking the **Add** button, the Add TE Static Route window in [Figure 8-3](#) appears.

**Figure 8-3** Add TE Static Route

- Step 5** In the Add TE Static Route window, specify at a minimum a **Destination** IP address (w.x.y.z/n). Optionally specify an administrative **Distance**.

It is recommended that you either define one or more static routes or, alternatively, that you define an autoroute.

Click **OK** to accept the entries or **Cancel** to exit the screen.

- Step 6** Back in the main TE Traffic Admission SR window, you can add another TE Static Route or edit existing routes.

- Step 7** Click **Save** to save the service request. The Service Requests window in [Figure 8-4](#) appears with the TE Traffic Admission SR in **REQUESTED** state and the Operation Type set to **ADD**.

The service request states and the interaction between them are described in [Service Request States, page B-9](#).

- Step 8** To deploy the service request from the Service Requests window, see [Deploying a TE Traffic Admission SR, page 8-4](#).

## Deploying a TE Traffic Admission SR

As opposed to the TE Primary Tunnel SR, Backup Tunnel SR, and TE Resource Modification windows, a TE Admission SR must be deployed from the general Service Requests window.

To deploy a TE Admission SR, use the following steps:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Service Requests**.
- Step 2** Click **TE Traffic Admission**. The Service Requests window in [Figure 8-4](#) appears.

**Figure 8-4** Service Requests

Service Requests									
Show Services with <input type="text" value="Job ID"/> matching <input type="text" value=""/> of Type <input type="text" value="All"/> <input type="button" value="Find"/>									
Showing 11 - 16 of 16 records									
#	<input type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified
11.	<input type="checkbox"/>	11	DEPLOYED	TE Admission	ADD	admin			10/20/05 6:01 PM Tunnel2 : CISCO ISC-P64
12.	<input type="checkbox"/>	12	DEPLOYED	TE Admission	ADD	admin			10/20/05 6:01 PM Tunnel1000 : CISCO ISC-P70
13.	<input type="checkbox"/>	16	DEPLOYED	TE Admission	ADD	admin			11/2/05 3:54 PM tunnel-te1000 : tunnel-te1000
14.	<input type="checkbox"/>	17	DEPLOYED	TE Admission	ADD	admin			11/2/05 3:54 PM tunnel-te1004 : CISCO ISC-P136
15.	<input type="checkbox"/>	18	DEPLOYED	TE Admission	ADD	admin			11/2/05 3:55 PM tunnel-te1006 : tunnel-te1006
16.	<input type="checkbox"/>	22	REQUESTED	TE Admission	ADD	admin			11/7/05 4:03 PM Test
Rows per page: <input type="text" value="10"/> Go to page: <input type="text" value="2"/> of 2 <input type="button" value="Go"/>									
Auto Refresh: <input checked="" type="checkbox"/> <input type="button" value="Create"/> <input type="button" value="Details"/> <input type="button" value="Status"/> <input type="button" value="Edit"/> <input type="button" value="Deploy"/> <input type="button" value="Decommission"/> <input type="button" value="Purge"/>									

138820

The Service Requests window contains the following elements:

- **Job ID**—Job ID for the SR.
- **State**—Indicates whether the tunnel state is **DEPLOYED** or **NOT DEPLOYED** and whether it is **Conformed** or **Not Conformed**.
- **Type**—The type of service request, indicating which service issued the request. For a detailed description of the possible service types, see Cisco IP Solution Center Infrastructure Reference, 4.1.
- **Operation Type**—SR operation on the tunnel, can be either **ADD**, **MODIFY**, **DELETE**, or **ADMIT**. Applicable only to tunnels in the current SR.
- **Creator**—ID for the user who created the SR.

- **Customer Name**—Name of the customer to which the SR applies.
- **Policy Name**—Name of the policy associated with the SR.
- **Last Modified**—Date and time when the SR was last modified.
- **Description**—SR description provided by the user.

**Step 3** Select the desired service request and click **Deploy**. A drop-down menu appears under the **Deploy** button.

In the drop-down menu, select **Deploy** or **Force Deploy**. After having been successfully deployed, the **State** of the SR changes to **Deployed**.

**Step 4** The Service Requests window (**Service Inventory > Inventory and Connection Manager > Service Requests**) appears and displays the state of the deployed SR.

For more information on working with service requests, see [Appendix B, “Managing Service Requests.”](#)

---

## Other Traffic Admission SR Operations

As opposed to other service requests, TE Traffic Admission SRs can be decommissioned in the Service Requests window.

Edit and decommission operations for TE Traffic Admission service requests are described in [Appendix B, “Managing Service Requests.”](#)

## Viewing the SR State

To view a service request state, go to the Service Requests window under **Inventory and Connection Manager**.

If the SR does not enter the **Deployed** state, go to the **Task Logs** screen to see the deployment log (**Monitoring > Task Manager > Logs**) as described in [SR Deployment Logs, page 10-1](#).





# Administration

---

A number of administrative features in Cisco IP Solution Center Traffic Engineering Management (ISC TEM) are common to ISC. Instructions on how to use these features are described in detail in *Cisco IP Solution Center Infrastructure Reference*, 4.1.

In this chapter, only TE-specific administrative features are described.

This chapter includes the following sections:

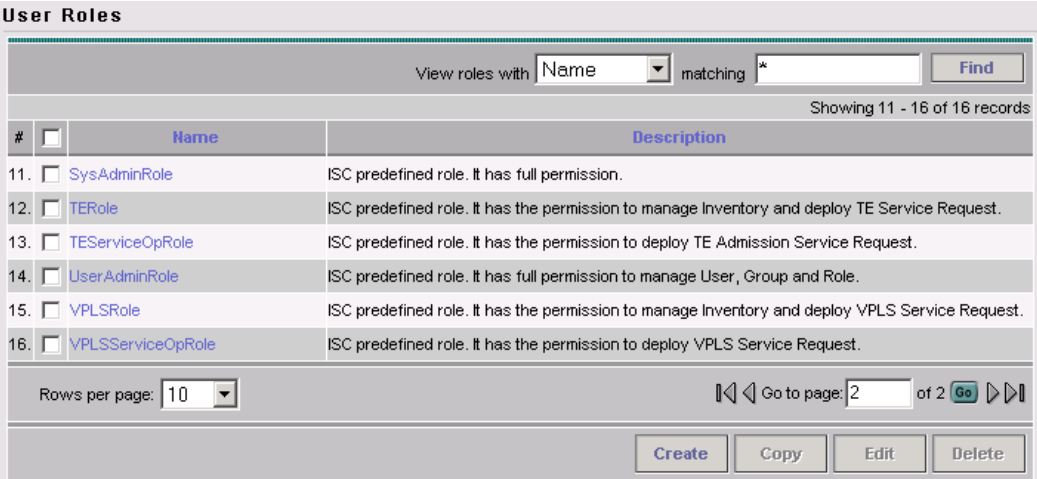
- [TE User Roles, page 9-1](#)
- [TE Policies, page 9-2](#)
  - [Create Policy, page 9-2](#)
  - [Edit Policy, page 9-4](#)
  - [Delete Policy, page 9-5](#)
- [TE Tasks, page 9-5](#)
  - [Creating a TE Task, page 9-6](#)
    - [Creating a TE Functional Audit Task, page 9-6](#)
    - [Creating a TE Interface Performance Task, page 9-11](#)
- [SR History and Configlets, page 9-17](#)
- [Manage Lock, page 9-17.](#)

## TE User Roles

A TE user role can be a predefined or a user-specified role defining a set of permissions. For a detailed description of user roles in ISC and how to use them, see the *Cisco IP Solution Center Infrastructure Reference*, 4.1.

To access the User Roles window and locate the TE user roles, navigate **Administration > Security > User Roles**. The User Roles window in [Figure 9-1](#) appears.

Figure 9-1 User Roles



**User Roles**

View roles with  matching

Showing 11 - 16 of 16 records

#	<input type="checkbox"/>	Name	Description
11.	<input type="checkbox"/>	SysAdminRole	ISC predefined role. It has full permission.
12.	<input type="checkbox"/>	TERole	ISC predefined role. It has the permission to manage Inventory and deploy TE Service Request.
13.	<input type="checkbox"/>	TESServiceOpRole	ISC predefined role. It has the permission to deploy TE Admission Service Request.
14.	<input type="checkbox"/>	UserAdminRole	ISC predefined role. It has full permission to manage User, Group and Role.
15.	<input type="checkbox"/>	VPLSRole	ISC predefined role. It has the permission to manage Inventory and deploy VPLS Service Request.
16.	<input type="checkbox"/>	VPLSServiceOpRole	ISC predefined role. It has the permission to deploy VPLS Service Request.

Rows per page:

For a description of the various window elements, see *Cisco IP Solution Center Infrastructure Reference*, 4.1.

There are two pre-defined TEM user roles:

- **TERole**—Grants full permission to TEM operations.
- **TESServiceOpRole**—Grants permission only to manage the TE Admission SR.

## TE Policies

Policies are used to define common tunnel attributes. Attributes such as bandwidth pools, hold and setup priority, and affinity bits, are set manually during policy creation as described below.

This section describes the following policy operations:

- [Create Policy, page 9-2](#)
- [Edit Policy, page 9-4](#)
- [Delete Policy, page 9-5](#)

## Create Policy

ISC TEM allows you to create TE-specific policies in a manner similar to other ISC policies.

To create a TE policy, you must access the Policy Manager. Use the following steps:

**Step 1** Navigate **Service Design > Policy Manager**.

**Step 2** Click the **Policy Manager** icon.

The Policies window in [Figure 9-2](#) appears.



Figure 9-2 Policies Window

The screenshot shows the IP Solution Center interface. The top navigation bar includes links for Home, Shortcuts, Account, Index, Help, About, and Logout. The main menu has tabs for Service Inventory, Service Design, Monitoring, Diagnostics, and Administration. The left sidebar shows a breadcrumb trail: You Are Here: Service Design > Policies. The main content area is titled 'Policies' and displays a table of policy records. The table has columns for #, Policy Name, Type, and Owner. The records are numbered 11 through 20. The table also includes search filters for Policy Name, matching criteria, and Type. The bottom of the table shows pagination controls: Rows per page: 10, Showing 11 - 20 of 20 records, and buttons for Create, Edit, Copy, and Delete.

#	Policy Name	Type	Owner
11.	ISC-P1-iscmp11:tunnel-te2	TE	Provider - Provider2
12.	ISC-P122-iscmp11:tunnel-te1003	TE	Provider - Provider2
13.	ISC-P126-iscmp10:tunnel-te1003	TE	Provider - Provider2
14.	ISC-P2-iscmp11:tunnel-te1000	TE	Provider - Provider2
15.	L2VpnPolicy1	L2VPN	Global
16.	L2VpnPolicy2	L2VPN	Global
17.	MPLSPolicy_PCE	MPLS	Customer - Customer1
18.	MPLSPolicyNO_CE	MPLS	MPLS Policy ner1
19.	VPLSPolicy1	VPLS	L2VPN (P2P) Policy
20.	VPLSPolicy2	VPLS	VPLS Policy

- Step 3** Click **Create** and select **TE Policy** to set up a new TE policy. The TE Policy Editor window in Figure 9-3 appears.

Figure 9-3 TE Policy Editor

The screenshot shows the TE Policy Editor window. It contains the following fields and controls:

- Policy Name \***: Text input field with a character limit of (1 - 64 characters).
- Owner \***: Dropdown menu set to Global.
- Managed**: Checkbox, currently unchecked.
- Pool Type**: Radio buttons for Sub Pool (BC1) and Global Pool (BC0). Global Pool (BC0) is selected.
- Setup Priority \***: Text input field with value 1.
- Hold Priority \***: Text input field with value 1.
- Affinity (0x0-0xFFFFFFFF)**: Text input field.
- Affinity Mask (0x0-0xFFFFFFFF)**: Text input field.
- FRR Protection Level**: Radio buttons for None and Best Effort. None is selected.
- Buttons**: Save and Cancel buttons.

Note: \* - Required Field

The TE Policy Editor window contains the following fields:

- **Policy Name**—Name of the TE policy chosen by the user.

- **Owner**—The owner of the TE policy:
  - **Global**—A global policy.
  - **Provider**—A provider policy.
  - **Customer**—A customer policy.
- **Managed**—Check this box to make the policy to be used by managed tunnels. When clicked, both the setup and hold priorities are set to zero and these are not editable. If the box is unchecked, the setup/hold priorities can be set to a value between 1 and 7.  
Clicking the **Managed** check box will add some extra fields in the TE Policy Editor corresponding to two additional protection levels for **FRR Protection Level** (Fast Re-Route) and a new field, **Delay Constraint**.
- **Pool Type**—Tunnel bandwidth pool type for this policy. For a definition of pool types, see [Bandwidth Pools, page 1-5](#).
  - **Sub Pool (BC1)**—Bandwidth will be reserved from Sub Pool.
  - **Global Pool (BC0)**—Bandwidth will be reserved from Global Pool.
- **Setup Priority**—Priority used when signaling an LSP for the tunnel to determine, which of the existing tunnels can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 hold priority.
- **Hold Priority**—Priority associated with an LSP for the tunnel to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.
- **Affinity**—Attribute values required for links carrying the tunnel (bit values are either 0 or 1).
- **Affinity Mask**—Which attribute values should be checked. If a bit in the mask is 0, a link's attribute value of that bit is irrelevant. If a bit in the mask is 1, the link's attribute value and the tunnel's required affinity for that bit must match.
- **FRR Protection Level**—Level of Fast Reroute protection required on the primary tunnel.
  - **None**—No backup tunnel needed.
  - **Best Effort**—Use backup tunnel if available.

Two actions are available:

- **Save**—Save the TE policy with the current data.
- **Cancel**—Quit the TE Policy Editor and discard any changes.

## Edit Policy

A policy can be edited only if it is not associated with a tunnel.

To edit a TE policy, use the following steps:

**Step 1** Navigate **Service Design > Policy Manager**.

**Step 2** Click the **Policy Manager** icon.

The Policies window in [Figure 9-2](#) appears.

**Step 3** Select the desired policy and click **Edit**.

The TE Policy Editor window in [Figure 9-3](#) appears. The TE Policy Editor window in [Figure 9-3](#) appears. The policy editor is described in [Create Policy, page 9-2](#). The only difference between the create and edit processes is that the policy name and owner are not editable when editing a policy.

**Step 4** Make the desired changes to the policy attributes and click **Save**. If the save operation succeeds, the new TE policy now appears in the Policies window. If not, the **Status** box will indicate the type of error that occurred and, when possible, the corrective action required.

## Delete Policy

A policy can be deleted only if it is not associated with a tunnel.

To delete a TE policy, use the following steps:

**Step 1** Navigate **Service Design > Policy Manager**.

**Step 2** Click the **Policy Manager** icon.

The Policies window in [Figure 9-2](#) appears.

**Step 3** Select the desired policy and click **Delete**. The Confirm Delete window in [Figure 9-4](#) appears

**Figure 9-4** Policies - Confirm Delete

Confirm Delete			
Showing 1 - 1 of 1 record			
#	Policy Name	Service	Owner
1.	test1	TE	Global

Rows per page: 10

Go to page: 1 of 1

Buttons: Delete, Cancel

**Step 4** Check the policy marked for deletion and click **OK**.

**Step 5** The Policies window refreshes and the selected policy disappears.

## TE Tasks

ISC TEM currently offers three TE-specific tasks that are used in a manner similar to other ISC tasks:

- **TE Discovery**—Populates the repository with data from the TE network. Discrepancies are reconciled and/or reported.
- **TE Functional Audit**—Performs functional audit on TE Primary or Backup SRs in certain states.
- **TE Interface Performance**—Calculates the interface/tunnel bandwidth utilization.

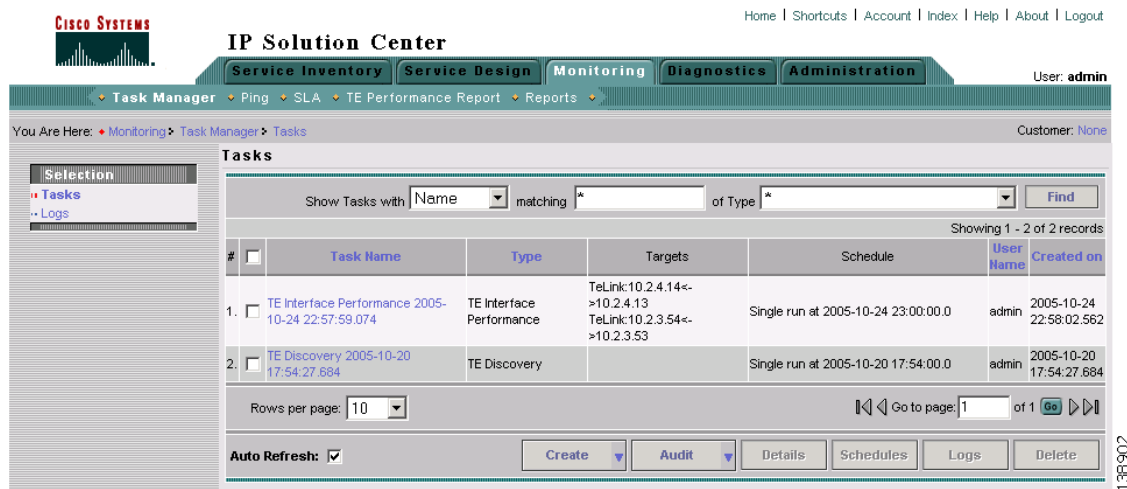
This section focuses on describing how to create TE Functional Audit and TE Interface Performance tasks. Instructions on how to create a TE Discovery task are included in [Chapter 3, “TE Network Discovery”](#).

## Creating a TE Task

TE tasks are managed in the ISC **Task Manager**, which is accessed as follows:

- Step 1** Navigate **Monitoring > Task Manager**.  
The Tasks window in [Figure 9-5](#) appears.

**Figure 9-5** Tasks Window



For a detailed description of the window elements in the Tasks window, see *Cisco IP Solution Center Infrastructure Reference*, 4.1.

This page shows all collection and deployment tasks that have been executed. Note that a task could be scheduled to happen once or there could be several scheduled runs of a task. The schedule can be viewed by selecting a task and clicking **Schedules**.

## Creating a TE Functional Audit Task

For each tunnel in the SR, the TE Functional Audit task checks the LSP currently used on a router against the LSP stored in the repository:

- tunnel down—Ignore (do not check)
- tunnel up—Check the LSP used on the router against the one stored in the repository:
  - If they are the same, the tunnel and the SR are both set to **Functional**.
  - If they are different, both the tunnel and the SR are set to **Broken**.
- tunnel missing from router—SR left untouched. The tunnel state is set to **Lost**.

This task only performs functional audit on TE Primary or Backup SRs, which are not in one of the following states:

- **Closed**
- **Requested**
- **Invalid**
- **Failed Deploy**

For a detailed explanation of the various states, see *Cisco IP Solution Center Infrastructure Reference*, 4.1.

To create a TE Functional Audit task, use the following steps:

- 
- Step 1** Navigate **Monitoring > Task Manager**.
- Step 2** Click **Audit > TE Functional Audit** to open the Create Task window in [Figure 9-6](#).

**Figure 9-6** Create a TE Functional Audit Task

**Create Task**

<b>Name*:</b>	TE Functional Audit 2005-11-08 23:03:20.012
<b>Type:</b>	TE Functional Audit
<b>Description:</b>	Created on 2005-11-08 23:03:20.012

Note: \* - Required Field

- Step 1 of 2 -

< Back   Next >   Finish   Cancel

For a detailed description of the window elements in the Create Task window, see *Cisco IP Solution Center Infrastructure Reference*, 4.1.

- Step 3** Modify the **Name** or **Description** fields as desired and click **Next**.  
The Task Service Requests window in [Figure 9-7](#) appears.

**Figure 9-7** Task Service Requests

**Task Service Requests**

Show Services with Job ID matching \* of Type All Find

Showing 0 of 0 records

#	Job ID	State	Type	Customer Name	VPN Name
Rows per page: 10 Go to page: 1 of 1 Go					
Add Delete					

- Step 1 of 3 -

< Back Next > Finish Cancel

- Step 4** Click **Add** to add a task service request. The Select Service Request(s) window in [Figure 9-8](#) appears.

**Figure 9-8** Select Service Request(s)

Show Services with Job ID matching \* of Type All Find

Showing 1 - 10 of 16 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name
1.	<input type="checkbox"/> 1	REQUESTED	MPLS	ADD	admin	Customer1	MPLSPolicy_PCE
2.	<input type="checkbox"/> 2	REQUESTED	MPLS	ADD	admin	Customer1	MPLSPolicyNO_CE
3.	<input type="checkbox"/> 3	REQUESTED	L2VPN	ADD	admin	Customer1	L2VpnPolicy1
4.	<input type="checkbox"/> 4	REQUESTED	QoS	ADD	admin	Customer1	3550-DSCP
5.	<input type="checkbox"/> 5	REQUESTED	L2VPN	ADD	admin	Customer1	L2VpnPolicy2
6.	<input type="checkbox"/> 6	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy1
7.	<input type="checkbox"/> 7	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy2
8.	<input type="checkbox"/> 8	DEPLOYED	TE Tunnel	MODIFY	admin		
9.	<input type="checkbox"/> 9	DEPLOYED	TE Protection	MODIFY	admin		
10.	<input type="checkbox"/> 10	DEPLOYED	TE Admission	ADD	admin		

Rows per page: 10 Go to page: 1 of 2 Go

Select Cancel

- Step 5** Select an SR using the **Select** button. Only SRs of type TE Tunnel or TE Protection will be accepted. The Selected Service Request(s) window closes and the selected task(s) now appears in the Task Service Requests window. To add other SRs, repeat the procedure in [Step 4](#) and [Step 5](#).
- Step 6** In the Task Service Requests window, click **Next**. The Task Schedules window in [Figure 9-9](#) appears.

Figure 9-9 Task Schedules

- Step 7** Click **Now** to start the task immediately or **Create** to create a task schedule. When selecting **Now**, a line is added to the **Task Schedules** window. When selecting **Create**, the Task Schedule window in [Figure 9-10](#) appears.

Figure 9-10 Task Schedule

- Step 8** In the Task Schedule window, indicate when and how often to run the task.
- Step 9** Click **OK**. The scheduled task should now appear in the **Task Schedules** table.

**Note**

The default setting is to schedule a single TE Functional Audit task to take place immediately (“**Now**”).

- Step 10** Click **Next**. The Task Schedule window now shows the new task in its list of created tasks as shown in [Figure 9-11](#).

**Figure 9-11** Task Schedule with Scheduling Data

The screenshot shows the 'Task Schedules' window. At the top, it says 'Showing 1 - 1 of 1 record'. Below this is a table with the following columns: #, ☐, Schedule, Start Date and Time, End Date and Time, Max Runs, and Max Instances. The table contains one row with the following data: 1., ☐, 'Single run at 2005-11-08 23:44:00.0', '2005-11-08 23:44:00.0', 'not applicable', 'unlimited', and 'unlimited'. Below the table, there is a 'Rows per page:' dropdown set to '10' and a 'Go to page:' field set to '1' of '1'. There are 'Now', 'Create', and 'Delete' buttons. At the bottom, it says '- Step 2 of 3 -' and has '< Back', 'Next >', 'Finish', and 'Cancel' buttons.

#	<input type="checkbox"/>	Schedule	Start Date and Time	End Date and Time	Max Runs	Max Instances
1.	<input type="checkbox"/>	Single run at 2005-11-08 23:44:00.0	2005-11-08 23:44:00.0	not applicable	unlimited	unlimited

Rows per page: 10 Go to page: 1 of 1 Go

Now Create Delete

- Step 2 of 3 - < Back Next > Finish Cancel

- Step 11** A summary of the scheduled task appears as shown in [Figure 9-12](#).

**Figure 9-12** TE Functional Audit Task Summary

The screenshot shows the 'TE Func Audit Task Summary' window. It contains a table with the following data:

Name	TE Functional Audit 2005-11-08 23:37:55.956
Description	Created on 2005-11-08 23:37:55.956
Service Job IDs	8
Schedules	Single run at 2005-11-08 23:44:00.0

At the bottom, it says '- Step 3 of 3 -' and has '< Back', 'Next >', 'Finish', and 'Cancel' buttons.

TE Func Audit Task Summary

Name	TE Functional Audit 2005-11-08 23:37:55.956
Description	Created on 2005-11-08 23:37:55.956
Service Job IDs	8
Schedules	Single run at 2005-11-08 23:44:00.0

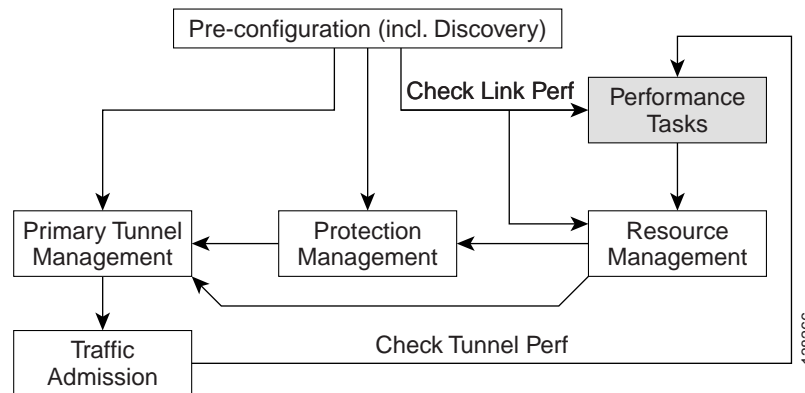
- Step 3 of 3 - < Back Next > Finish Cancel



**Step 12** Click **Finish**. This adds the task to the list of created tasks in the Tasks window (Figure 9-5).

To view the task logs for the created tasks, see [Viewing a Task Log, page 10-2](#).

## Creating a TE Interface Performance Task



This task calculates interface/tunnel bandwidth utilization using the Simple Network Management Protocol (SNMP).

Calculating utilization depends on how data is presented for the object you want to measure. Interface utilization is the primary measure used for network utilization. Because MIB-II variables are stored as counters, you must take two poll cycles and figure the difference between the two (hence, the delta used in the equation).

Three variables are required:

- task duration—how long the task will run (in secs)
- frequency—how frequent the data will be collected (in secs)
- interval—the distance between two poll cycles (in ms).

The following explains the variables used in the formulas:

- delta(traffic in)—the delta between two poll cycles of collecting the SNMP input object, which represents the number of inbound units of traffic.
- delta(traffic out)—the delta between two poll cycles of collecting the SNMP output object, which represents the number of outbound units of traffic
- bandwidth—the speed of the interface..

A more accurate method is to measure the input utilization and output utilization separately, using the following formula:

$$\text{Input utilization} = \frac{\text{delta(traffic in)} \times 8 \times 100}{(\text{number of seconds in delta}) \times \text{bandwidth}}$$

$$\text{Output utilization} = \frac{\text{delta(traffic out)} \times 8 \times 100}{(\text{number of seconds in delta}) \times \text{bandwidth}}$$

To create a TE Interface Performance task, use the following steps:

- Step 1 Navigate **Monitoring > Task Manager**.
- Step 2 Click **Create** to open the Create Task window in [Figure 9-13](#).

**Figure 9-13** Create TE Interface Performance Task

For a detailed description of the window elements in the Create Task window, see *Cisco IP Solution Center Infrastructure Reference*, 4.1.

- Step 3 Select **TE Interface Performance** in the drop-down list of the **Type** field.  
The Select TE Provider window in [Figure 9-14](#) appears.

Figure 9-14 Select TE Provider

Select TE Provider

Show TE Providers with Name matching \* Find

Showing 1 - 1 of 1 record

#		Provider Name
1.	<input checked="" type="radio"/>	Provider2

Rows per page: 10 Go to page: 1 of 1 Go

Step 1 of 4 - < Back Next > Finish Cancel

**Step 4** Click a radio button to select a TE provider.

**Step 5** Click **Next**. The TE Performance Collection window in Figure 9-15 appears.

Figure 9-15 TE Performance Collection

TE Performance Collection

Task Duration (sec): 1000

Task Frequency (sec): 100

Task Interval (msec): 10

Targets

Showing 0 of 0 records

<input type="checkbox"/>	Device	Type	Name
--------------------------	--------	------	------

Rows per page: 10 Go to page: 1 of 1 Go

Step 2 of 4 - < Back Next > TeTunnel TeLink Cancel

**Step 6** Enter desired values in the **Duration**, **Frequency**, and **Interval** fields.

**Step 7** Use the **Add** button to select a tunnel or link on which to run the interface performance task:

- **TE Tunnel**—Add a TE tunnel. The Select Tunnel(s) window in Figure 9-16 appears.
- **TE Link**—Add a TE link. The Select Link(s) window in Figure 9-17 appears.

Figure 9-16 Select Tunnel(s) - Interface Performance

TE Provider Provider2

Show Tunnels with  matching

Showing 1 - 5 of 26 records

#	<input type="checkbox"/>	Head	Dest	T#	Tunnel Name	Tunnel ID	Deploy Status	Policy	Type
1.	<input type="checkbox"/>	isctmp11	isctmp10	2	isctmp11:tunnel-te2	ISC-P1	DEPLOYED	ISC-P1-isctmp11:tunnel-te2	Managed
2.	<input type="checkbox"/>	isctmp11	isctmp1	1000	isctmp11:tunnel-te1000	ISC-P2	DEPLOYED	ISC-P2-isctmp11:tunnel-te1000	Managed
3.	<input type="checkbox"/>	isctmp11	isctmp12	1003	isctmp11:tunnel-te1003	ISC-P122	DEPLOYED	ISC-P122-isctmp11:tunnel-te1003	Managed
4.	<input type="checkbox"/>	isctmp11	isctmp8	1004	isctmp11:tunnel-te1004	ISC-P123	DEPLOYED	ISC-P122-isctmp11:tunnel-te1003	Managed
5.	<input type="checkbox"/>	isctmp11	isctmp10	1006	isctmp11:tunnel-te1006	ISC-P149	DEPLOYED	te_policy1	UnManaged

Rows per page:

138826

Figure 9-17 Select Link(s) - Interface Performance

Links associated with Performance Task

Show Links with:  matching

Showing 1-5 of 35 records

#	<input type="checkbox"/>	From	Link	To
1.	<input type="checkbox"/>	isctmp11	10.2.4.10<->10.2.4.9	isctmp12
2.	<input type="checkbox"/>	isctmp11	10.2.4.14<->10.2.4.13	isctmp12
3.	<input type="checkbox"/>	isctmp11	10.2.4.6<->10.2.4.5	isctmp8
4.	<input type="checkbox"/>	isctmp10	10.2.4.22<->10.2.4.21	isctmp12
5.	<input type="checkbox"/>	isctmp12	10.2.4.29<->10.2.4.30	isctmp7

Rows per page:

138827

- Step 8** Select one or more of tunnels and links and click **Next**. The selected tunnels and links are added to the **Targets** list in the TE Performance Collection window.
- Step 9** The Task Schedules window in [Figure 9-18](#) appears.

**Figure 9-18** Task Schedules

Task Schedules

Showing 0 of 0 records

#	Schedule	Start Date and Time	End Date and Time	Max Runs	Max Instances
---	----------	---------------------	-------------------	----------	---------------

Rows per page: 10

Go to page: 1 of 1

Now Create Delete

Step 3 of 4

< Back Next > Finish Cancel

- Step 10** Click **Now** or **Create** to create a task schedule. When you select **Create** to customize the schedule, the Task Schedule window in [Figure 9-19](#) appears (with **Now**, this step is skipped).



**Note** The default setting is to schedule a single TE Interface Performance task to take place immediately (“**Now**”).

**Figure 9-19** Task Schedule

Task Schedule

Single run: ☒ Now ☐ Once

Periodic Run: ☐ Minute ☐ Hourly ☐ Daily ☐ Weekly ☐ Monthly

Periodic Run Attributes

Run Interval:

Run Limits:

Start Date and Time

Date: November 7 2005

Time: 6 31 PM

End Date and Time (Default is unlimited)

Date: Month Day Year

Time: Hour Min AM

OK Cancel

- Step 11** In the Task Schedule window, make your selections to define when and how often to run the task.
- Step 12** Click **OK**. The scheduled task should now appear in the **Task Schedules** table as shown in [Figure 9-20](#).

**Figure 9-20** Task Schedules with Scheduling Data

**Task Schedules**

Showing 1 - 1 of 1 record

#	<input type="checkbox"/>	Schedule	Start Date and Time	End Date and Time	Max Runs	Max Instances
1.	<input type="checkbox"/>	Single run at 2005-11-07 18:31:00.0	2005-11-07 18:31:00.0	not applicable	unlimited	unlimited

Rows per page: 10

Go to page: 1 of 1 [Go](#)

[Now](#) [Create](#) [Delete](#)

- Step 3 of 4 -

[< Back](#) [Next >](#) [Finish](#) [Cancel](#)

**Step 13** Click **Next**. A summary of the scheduled task appears as shown in [Figure 9-21](#).

**Figure 9-21** Performance Task Summary

**Performance Task Summary**

Name	TE Interface Performance 2005-11-07 18:02:12.946
Task Duration (sec)	1000
Task Frequency (sec)	100
Task Interval (msec)	10
Devices	isctmp11 10.2.4.10<->10.2.4.9 isctmp11 isctmp11:tunnel-te1000
Schedules	Single run at 2005-11-07 18:31:00.0

- Step 4 of 4 -

[< Back](#) [Next >](#) [Finish](#) [Cancel](#)

**Step 14** Click **Finish**. This adds the task to the list of created tasks in the Tasks window ([Figure 9-22](#)).

**Figure 9-22** Tasks Window with New Performance Task

**Tasks**

Show Tasks with  matching  of Type

Showing 1 - 5 of 8 records

#	<input type="checkbox"/>	Task Name	Type	Targets	Schedule	User Name	Created on
1.	<input type="checkbox"/>	TE Interface Performance 2005-11-07 18:02:12.946	TE Interface Performance	TeLink:10.2.4.10<->10.2.4.9 TeTunnel:tunnel-te1000	Single run at 2005-11-07 18:31:00.0	admin	2005-11-07 18:11:39.401
2.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-11-07 00:31:32.56	Service Deployment	Job Id : 8	Schedule TE Primary SR deployment	admin	2005-11-07 00:31:32.56
3.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-11-06 16:15:37.027	Service Deployment	Job Id : 8	Schedule TE Primary SR deployment	admin	2005-11-06 16:15:37.027
4.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-11-06 16:01:09.867	Service Deployment	Job Id : 8	Schedule TE Primary SR deployment	admin	2005-11-06 16:01:09.867
5.	<input type="checkbox"/>	TE Discovery 2005-11-02 15:50:25.705	TE Discovery		Single run at 2005-11-02 15:50:00.0	admin	2005-11-02 15:50:25.705

Rows per page:

Auto Refresh: ☒

138831

To view the TE Performance Report that is generated for TE Interface Performance task(s), see [TE Performance Reports, page 10-4](#).

To view the task logs for the created tasks, see [Viewing a Task Log, page 10-2](#).

## SR History and Configlets

The history and configlets associated with individual service requests can be viewed from the Service Requests window when you select a service request and click the **Details** button.

The history of a service request is essentially a state change report. It lists the various states that elements associated with an SR has transitioned between and reports relevant details pertaining to these state changes.

Configlets for devices associated with service requests are in simple scrollable text format.

For more information about these features and how to manage service requests, see [Appendix B, “Managing Service Requests.”](#)

## Manage Lock

Whenever a task is performed that incurs a database update, which might affect the resource and hence the result of a tunnel computation, it locks the system before the update and releases it at completion of the update. If for some reason the lock is not released, other updates that require the lock are blocked.

The purpose of the lock feature is to prevent concurrent and mutually inconsistent planning activities from being committed to the database. Meaning, if each user takes the same snapshot of the the repository, performs computations, and tries to commit what he/she sees, the locking mechanism helps synchronize the commit and ensures that no commit invalidates other commits.

If the system is locked for prolonged periods of time, the administrator should check if anyone is performing long planning tasks and take note of which process locked the system and report it. If the administrator is sure that no one is using the system, it can be unlocked by using the lock manager.

Each system lock is linked to a TE provider. To unlock the TE provider, use the following steps:

- 
- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Providers**.
  - Step 2** The TE Providers window in [Figure 2-3](#) appears.
  - Step 3** Select a TE provider that is locked by clicking the corresponding check box.
  - Step 4** Click **Manage Lock**. The System Lock Management window in [Figure 9-23](#) appears.

**Figure 9-23 System Lock Management**

Provider: Provider1

User: admin

Process: TE Discovery Task

Timestamp: Oct 1, 2003 10:05:44 AM

Description:

Lock Status: ☒ Locked ☐ Unlocked

Unlock Close

122757

The text fields in this window are read-only.

- Step 5** To unlock, click the **Unlock** button.

The System Lock Management window closes and the **System Lock Status** field in the TE Providers window is updated accordingly.

---





## Task Monitoring

---

All deployment and collection tasks are monitored and the details of the tasks are logged. The information can be viewed using the task monitoring pages.

This chapter includes the following sections:

- [TE Task Logs, page 10-1](#)
  - [SR Deployment Logs, page 10-1](#)
  - [Logs Created from Task Manager, page 10-2](#)
  - [Viewing a Task Log, page 10-2](#)
- [TE Performance Reports, page 10-4](#)

## TE Task Logs

The TE task logs are used to view the result of running one or more TE tasks as described in [TE Tasks, page 9-5](#).

Different task logs are generated by different events:

- SR deployment logs
- Logs generated by tasks issued from the Task Manager, such as:
  - TE Discovery
  - TE Functional Audit
  - TE Interface Performance.

## SR Deployment Logs

When any service request is deployed, whether a managed or unmanaged primary tunnel or a backup tunnel, a log is generated. For tunnel SRs, deployment takes place in multiple phases depending on the type of SR and the task logs are created similarly:

- Primary tunnel SR—a three-phase logging process corresponding to a three-phase deployment (phases A, B, and C as shown in [Figure 10-1](#))
- Protection SR—a two-phase logging process corresponding to a two-phase deployment

In addition to the deployment logs, a ConfigAudit log is created regardless of the type of SR deployment, providing the deployment was successful.

## Logs Created from Task Manager

Specific instructions for how to generate and view a task log for a TE Discovery task are found in [Task Logs, page 3-7](#).

Instructions for how to generate and view a task log for the TE Functional Audit and TE Interface Performance tasks are found in [Creating a TE Task, page 9-6](#).

## Viewing a Task Log

A task log can be accessed from two different locations:

- The Tasks window
- The Service Requests window

### From the Tasks window

To view the task log for a TE task, you need to:

1. Access the Task Logs window.
2. Select the desired log and open it.

To view the task logs, use the following steps. A task log from the deployment of a managed primary tunnel has been used as an example.

- 
- Step 1** Navigate **Monitoring > Task Manager**.
- Step 2** Select **Logs** in the table of contents on the left side of the Tasks window. The Task Logs window in [Figure 10-1](#) appears.

**Figure 10-1 Task Logs**

#	Runtime Task Name	Action	Start Time	End Time	Status
1.	TE Interface Performance 2005-11-07 18:02:12.946_Mon_Nov_07_18:36:30_PST_2005_8	PerfCollection	2005-11-07 18:36:31.364	2005-11-07 18:53:16.704	Completed with errors
2.	Deploy Primary SR-ID 8 2005-11-07 00:31:32.56_Mon_Nov_07_00:31:36_PST_2005_7	ConfigAudit	2005-11-07 00:32:17.437	2005-11-07 00:33:11.803	Completed successfully
3.	Deploy Primary SR-ID 8 2005-11-07 00:31:32.56_Mon_Nov_07_00:31:36_PST_2005_7	Deployment Phase C	2005-11-07 00:31:41.193	2005-11-07 00:32:17.41	Completed successfully
4.	Deploy Primary SR-ID 8 2005-11-07 00:31:32.56_Mon_Nov_07_00:31:36_PST_2005_7	Deployment Phase B	2005-11-07 00:31:40.491	2005-11-07 00:31:41.168	Completed successfully
5.	Deploy Primary SR-ID 8 2005-11-07 00:31:32.56_Mon_Nov_07_00:31:36_PST_2005_7	Deployment Phase A	2005-11-07 00:31:37.183	2005-11-07 00:31:40.468	Completed successfully

Showing 1 - 5 of 15 records

Rows per page: 5 Go to page: 1 of 3

Auto Refresh: ☒ Service Requests View Log Delete

For an explanation of the various window elements, see [Task Log, page A-68](#).

**Step 3** Select a Task Log for viewing. A task that has been scheduled for multiple runs might have multiple instances to view.

Click the desired task in the **Action** column. The corresponding Task Log window in [Figure 10-2](#) appears.

**Figure 10-2** Task Log - Performance Collection with Error

**Task Log**

Log Level:  Component:

Date	Level	Component	Message
2005-11-07 18:36:36	OFF	GTL	Started CS Job for zone=/cs, Job Log
2005-11-07 18:36:40	OFF	GTL	CS Job Completed 1 for Collection Zone /cs Log
2005-11-07 18:36:40	SEVERE	trafMonJob	isctmp11:tunnel-te1000 Bandwidth is not set

136834

For an explanation of the various window elements, see [Task Log, page A-68](#).

The logged messages are shown in a table. This includes the time the log message was created and the severity level assigned to the log message.

There is a filter setting for the logging, which defaults to SEVERE. This means that only SEVERE messages in the log are shown. There are several different filter settings that can be selected according to the desired level of detail. To change the filter level, select the one that is required and click **Filter**.

How the log is structured depends on the type of task that was run.

**Step 4** Click **Return to Logs** to close the log window. This takes you back to the main Task Logs window.

**Step 5** To see the task SR, which in some cases is associated with a particular task log, select the desired task log and click the Service Requests button. The Tasks SRs window appears ([Figure 10-3](#)).

**Figure 10-3** Task SRs

The screenshot shows a web interface titled "Task SRs". At the top, there is a search bar with the text "Show Services with" followed by a dropdown menu set to "Job ID", the word "matching", an asterisk "\*" in a text field, and a dropdown menu set to "All". A "Find" button is to the right. Below the search bar, it says "Showing 0 of 0 records". A table with the following columns is displayed: #, ☐, Job ID, State, Type, Operation Type, Creator, Customer Name, Policy Name, and Description. The first row contains the values: 1., ☐, 8, a green box, DEPLOYED TE Tunnel, MODIFY, admin, an empty field, an empty field, and an empty field. Below the table, there is a "Rows per page:" dropdown set to "5". To the right, there are navigation icons and the text "Go to page: 1 of 1" with a "Go" button. At the bottom right, there are "Links" and "Return" buttons. A vertical text "138919" is on the far right edge.

For an explanation of the various window elements, see [Task Log, page A-68](#).

## From the Service Requests Window

To access the logs from the Service Requests window:

- Step 1** Navigate to Service Inventory > Inventory and Connection Manager > Service Requests.
- Step 2** Select a service request (only one).
- Step 3** Click the **Status** button and select **Logs**.
- Step 4** Select the log to view and click **View Log**. The Task Log window appears.
- Step 5** Select the log level from the drop-down menu and click **Filter**. The log levels are All, Severe, Warning, Info, Config, Fine, Finer, and Finest.

## TE Performance Reports

A TE Performance Report is created when you run a TE Interface Performance task as described in [Creating a TE Interface Performance Task, page 9-11](#).

It shows the traffic data collected from the TE Interface Performance task for selected tunnels and/or links. The TE Interface Performance task can run multiple times.

To view a TE Performance Report, use the following steps:

- Step 1** Navigate **Monitoring > TE Performance Report**.  
The TE Performance Report Table in [Figure 10-4](#) appears.

Figure 10-4 TE Performance Report Table

**Cisco Systems** IP Solution Center

Home | Shortcuts | Account | Index | Help | About | Logout

User: admin

Task Manager | Ping | SLA | TE Performance Report | Reports

You Are Here: Monitoring > TE Performance Report Customer: None

### TE Performance Report Table

Show Traffic with: All \* Find

Showing 1 - 2 of 2 records

#	Start Time	End Time	Device Name	Interface Name	Octets In	Octets Out	Speed	Util In	Util Out
1.	2005-10-24 23:00:25.477	2005-10-24 23:02:05.967	isctmp11	10.2.4.14<->10.2.4.13	0	0	622080000	0.0	0.0
2.	2005-10-24 23:00:26.299	2005-10-24 23:02:06.407	isctmp1	10.2.3.54<->10.2.3.53	0	72	100000000	0.0	0.084575738430023

Rows per page: 10 Go to page: 1 of 1 Go

Display Close Cancel

Reconcile Data: ☐ Peak ☐ Valley ☐ Average ☒ First

For an explanation of the various window elements in the report table, see [TE Performance Reports, page A-69](#).





## TE Topology

---

The TE Topology tool provides a graphical view of the network set up through the Cisco IP Solution Center Traffic Engineering Management (ISC TEM) web client. It gives a graphical representation of the various network elements, including devices, links, and tunnels. It also displays devices that ISC TEM is unable to identify but which have been discovered with the TE Discovery tool to be part of the network.

This section describes how to use the topology tool. A definition of fields and buttons in the topology GUI is found in [TE Topology, page A-5](#) in [Appendix A, “Traffic Engineering Management GUI”](#).

This chapter includes the following sections:

- [Overview, page 11-1](#)
- [Accessing the TE Topology Tool Page, page 11-2](#)
- [Using the TE Topology Interface Applet, page 11-2](#)
  - [Displaying and Saving Layouts, page 11-4](#)
  - [Using Maps, page 11-5](#)
  - [Using Highlighting and Attributes, page 11-8](#)
  - [Using Algorithms, page 11-10](#)

## Overview

The TE Topology tool can be activated from various locations within ISC. However, in this user guide the TE Topology tool is assumed to be accessed from the Traffic Engineering Management Services page.

The TE Topology tool is used to visualize the TE network based on the data contained in the repository. To that end, it provides a number of ways of manipulating the display, for example by applying algorithms to the graph layout, importing maps, and so on.

The tool is accessed from a TE Topology Interface Applet that displays the TE topology through a Java applet within the browser.

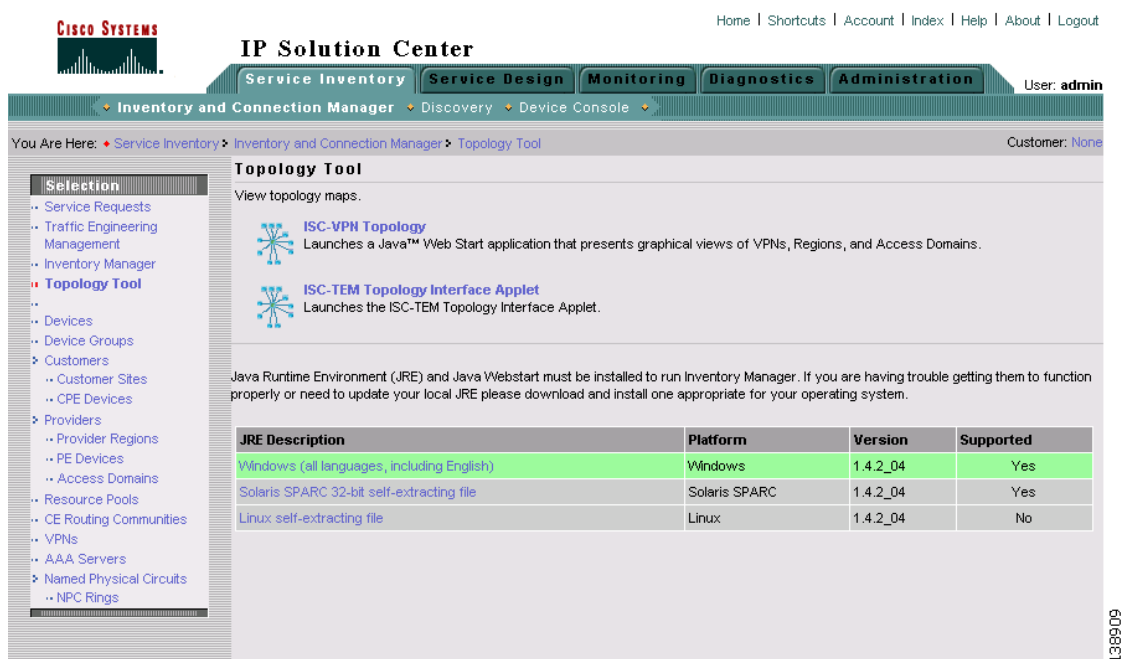
# Accessing the TE Topology Tool Page

The TE Topology tool is accessed as follows:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Topology**.

The Topology Tool window in [Figure 11-1](#) appears.

**Figure 11-1** Topology Tool



For a detailed description of the Topology Tool page, see *Cisco IP Solution Center Infrastructure Reference*, 4.1.

- Step 2** To start up the TE Topology tool, select **ISC-TEM Topology Interface Applet**.

## Using the TE Topology Interface Applet

The TE Topology Interface Applet (Topology Applet) provides a means of visualizing the network and tunnels present in the network. The web-based GUI is the primary means of visualizing the network information. The Topology Applet simply augments the web-based GUI to provide a different presentation format to the user.

The features offered through the Topology Applet are:

- TE Topology rendering
- Highlighting of network elements
- Tunnel overlay (unmanaged, primary, and backup)



- Topology layout persistence
- Integration with web page content.

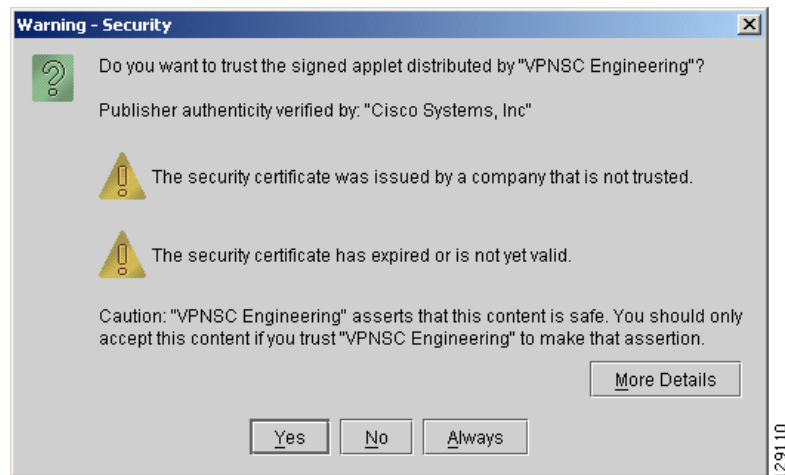
To access the Topology Applet, use the following steps:

**Step 1** Navigate to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Topology Tool**.

**Step 2** Click **ISC-TEM Topology Interface Applet**.

The security warning window in [Figure 11-2](#) appears.

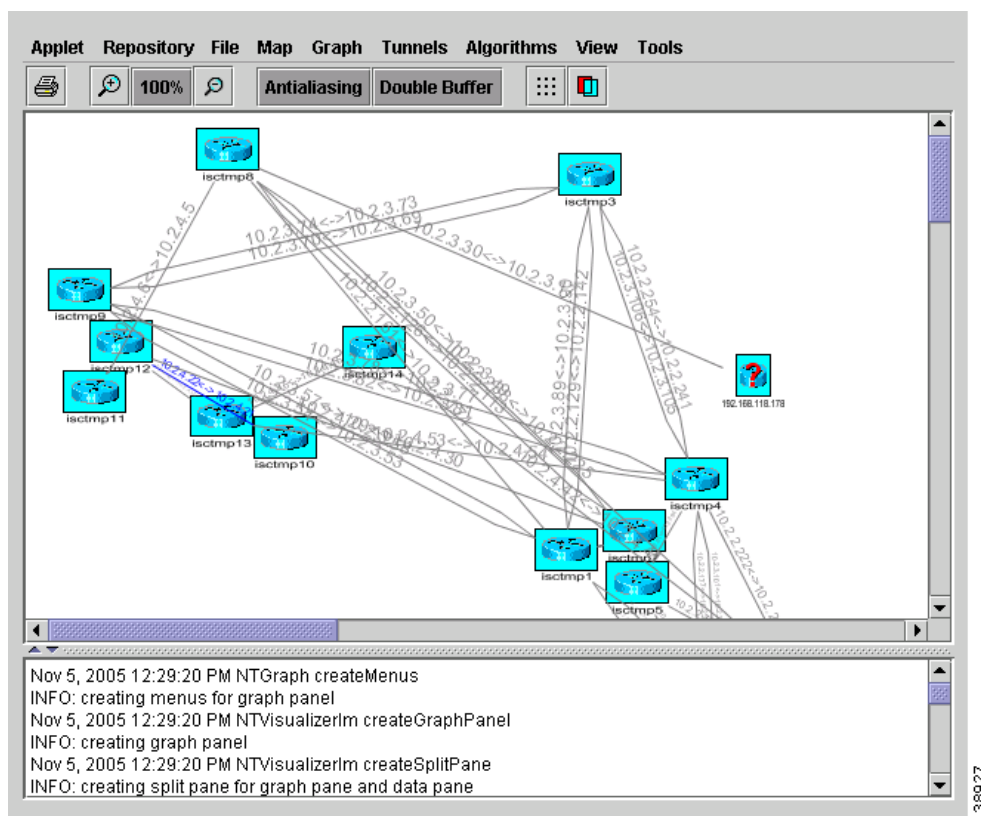
**Figure 11-2** Security Warning



**Step 3** Click **Yes** or **Always** to accept the authenticity of the security certificate.

The Topology Display applet window in [Figure 11-3](#) appears.

Figure 11-3 Topology Display Applet



Icons marked with red question marks signify devices unknown to ISC, for example non-Cisco devices. When activated with the Display button from another ISC TEM function (tunnel management window, resource modification window, etc.), any selected devices are highlighted in the display.

For an explanation of the various window elements in all the menus of the Topology Display, see [Topology Display, page A-5](#).

## Displaying and Saving Layouts

Use the two operations in the **Repository** menu, **Layout Graph** and **Save Graph Layout**, to display or save the current layout of the network graph.

Prior to generating the graph layout, the coordinates must be set on each of the network devices. Otherwise, the graph will have a random layout.

- **Layout Graph**—The graph is laid out from the repository. If a graph layout is already present, that layout is cleared once you click **Yes** in the **Clear Graph Layout** confirmation box. If the layout has not previously been saved, a random layout of the repository contents is drawn. If it has been saved previously, the saved layout is redrawn.
- **Save Graph Layout**—Save the current graph layout. Doing so will ensure that whenever the graph layout is cleared with **Layout Graph** or the topology applet is closed, the same layout will be created when the applet is restarted. If a map was used, the map is also redrawn.

## Using Maps

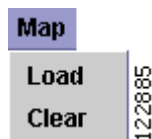
You can associate a map with each view. Currently, the topology viewer only supports maps in the Environmental Systems Research Institute, Inc. (ESRI) shape format. The following sections describe how to load maps and selectively view map layers and data associated with each map.

The map features are accessed from the **Map** menu in the Topology window.

To access the **Map** menu, use the following steps:

- 
- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Topology**.
  - Step 2** Start the **ISC TM Topology Interface Applet**. If link and node data for your network is already in the repository, a Progress Report lists the various network elements as the corresponding data is loaded.
  - Step 3** Select the **Map** menu. The menu in [Figure 11-4](#) appears.

*Figure 11-4 The Map Menu*



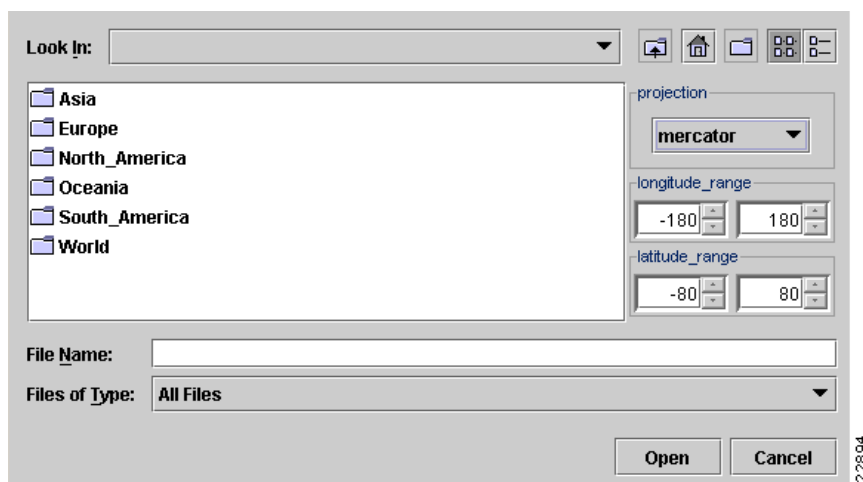
From the **Map** menu, you can either load or clear (remove) maps as described in the following.

---

## Loading a map

You might wish to set a background map showing the physical locations of the displayed devices. To load a map, use the following steps:

- 
- Step 1** In the menu bar, select **Map > Load**  
Providing the web map server is running, the Load Map window appears (see [Figure 11-5](#)).

**Figure 11-5 Load Map**

For an explanation of the various window elements, see [Load Map, page A-8](#).

**Step 2** Make your selections in the Load Map window.

The right-hand side of the window contains a small control panel, which allows you to select the projection in which a map is shown. A map projection is a projection which maps a sphere onto a plane. Typical projections are Mercator, Lambert, and Stereographic.

For more information on projections, consult the Map Projections section of Eric Weisstein's World of Mathematics at:

**<http://mathworld.wolfram.com/topics/MapProjections.html>**

For each projection, you can also select the region of the map to be shown. In most cases, the predefined values should be sufficient. The top level of the file hierarchy should contain folders for all major regions, such as Asia, Europe, North America, Oceania, and so on.

If desired, make changes to the settings in the **Longitude Range** and **Latitude Range** fields.

**Step 3** Navigate to the desired folder.

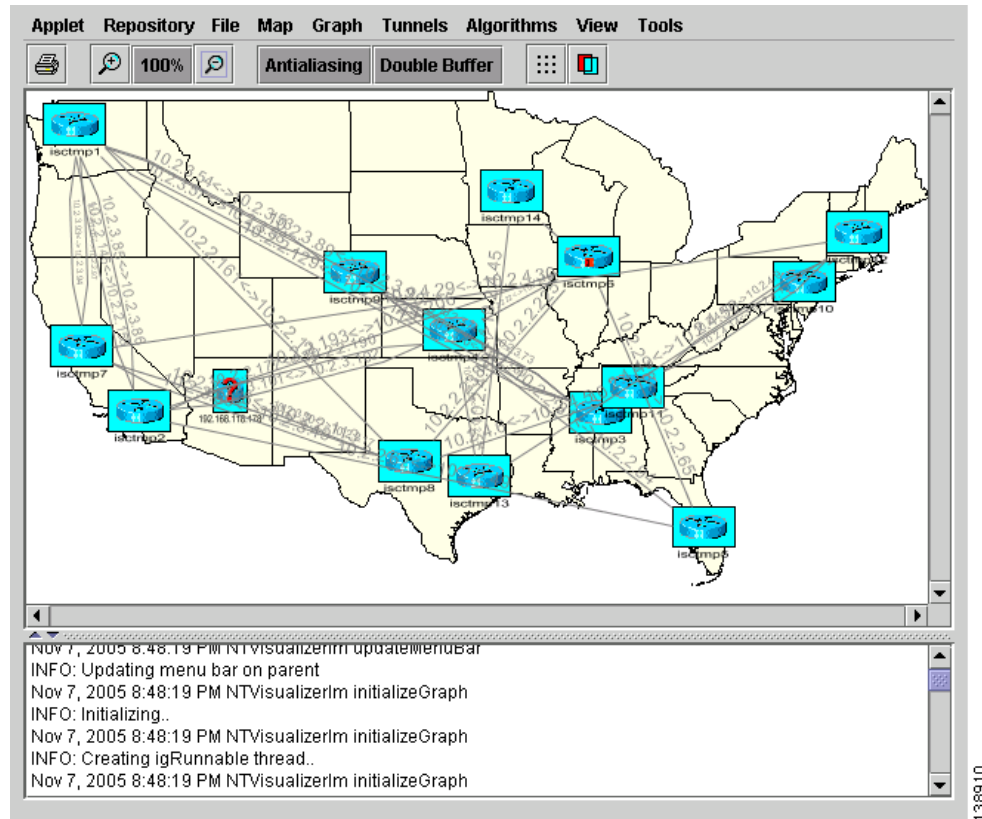
Each folder can contain either complete maps or folders for countries. Each map is clearly distinguished with the **Map** icon.

**Step 4** Select a map file and click **Open** to load the map.

Selecting the map file and clicking the **Open** button starts loading it. Maps can consist of several components and thus a progress dialog is shown informing you which part of the map file is loaded.

A map similar to the one in [Figure 11-6](#) appears.

Figure 11-6 Loaded Map



- Step 5** Use the various functions in the menus of the Topology Display window to manipulate the display contents in the Topology view. Some of these are described in subsequent sections. For a more complete description of the menu functions available, see [Topology Display, page A-5](#).

## Adding new maps

You might need to add your own maps to the selection of maps available to the Topology Tool. This is done by placing a map file in the **\$ISC\_HOME/resources/webserver/tomcat/webapps/ipsc-maps/data** directory or a subdirectory thereof within the ISC installation. To make this example more accessible, assume that you wish to add a map of Toowong, a suburb of Brisbane, the capital of Queensland. The first step to do so is to obtain maps from a map vendor. All maps must be in the ESRI shape file format (see **ESRI shapefile technical description**). In addition, a data file can accompany each shape file. Data files contain information about objects and the corresponding shapes are contained within the shape file. Let us assume that the vendor provided four files:

- toowong\_city.shp
- toowong\_city.dbf
- toowong\_street.shp
- toowong\_street.dbf

We have to create a .map file that informs the TE Topology tool about layers of the map. In this case we have two layers: a city and a street layer. The map file, say, Toowong.map, would thus have the following contents:

```
toowong_city
toowong_street
```

It lists all layers that create a map of Toowong. The order is important, as the first file forms the background layer, with other layers placed on top of the preceding layers.

Having obtained shape and data files and having written the map file, decide on its location. As mentioned, Toowong is a suburb of Brisbane, located in Queensland, Australia. All map files must be located in or under the **\$ISC\_HOME/resources/webserver/tomcat/webapps/ipsc-maps/data** directory. Since by default this directory contains a directory called **Oceania** intended for all maps from that region, simply create a path **Australia/Queensland/Brisbane** under the directory **Oceania**. Next, place all five files in this location. Once this is done, the map is automatically accessible to the topology viewer.

## Clearing Maps

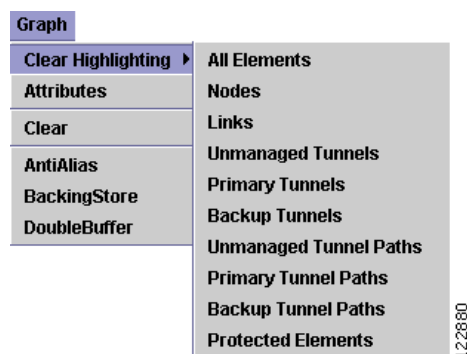
To clear the active map, select **Map > Clear** (see [Figure 11-3](#) and [Figure 11-4](#)).

Use this feature to clear (remove) the active map to leave only nodes and links in the corresponding network.

## Using Highlighting and Attributes

The **Graph** menu, shown in [Figure 11-7](#), provides access to a range of tools to manage and manipulate graphs.

**Figure 11-7**      **Graph Menu**



For an explanation of the various menu items, see the following sections as well as [Graph, page A-10](#).

Use the JavaServer Pages (to pagesto) to look at the list of nodes, links, and tunnels. From the JSP pages, select the display button at the bottom of the window to highlight elements.

The tools in the **Graph** menu serve to modify the appearance of the topology.

These are described in the following sections.

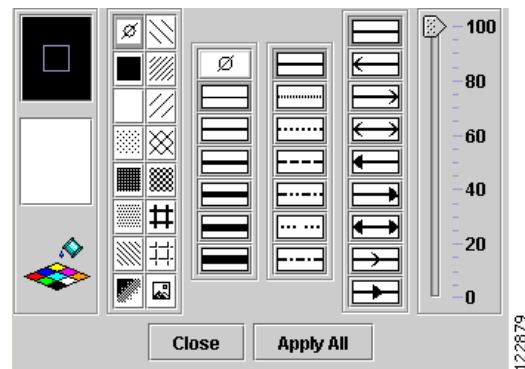
## Clear Highlighting

**Clear Highlighting** serves to remove highlighting from specific elements as listed in its submenu. For a description of the individual entries, see [Graph](#), page A-10.

## Add/Modify Attributes

When you select **Attributes** from the **Graph** menu, the Graphic Attributes window in [Figure 11-8](#) appears.

**Figure 11-8**      *Graphic Attributes*



The **Add/Modify Attributes** tool is used as follows:

- 
- Step 1**    Select graph elements (nodes/links) in the topology display. Use Ctrl/Shift to select multiple elements.
  - Step 2**    Navigate **Graph > Attributes** to open the Graphic Attributes window.
  - Step 3**    Change the desired attributes and click **Apply All**.
- 



**Note**      Only selected links ([Step 1](#)) are affected.

---

## Clear Current Graph Layout

Use the **Clear** function in the **Graph** menu to remove the topology graph from the current view.

Although this is also achieved with **Layout Graph** in the **Repository** menu, **Layout Graph** re-creates the graph last saved in the repository in addition to clearing the graph.

## Using AntiAlias, BackingStore, DoubleBuffer

**AntiAlias**, found in the **Graph** menu, is used to create smoother lines and a more pleasant appearance at the expense of performance.

**BackingStore** allows graphics content to be automatically saved when moved to the background and regenerated when returned to the foreground. This helps avoid superfluous refreshing.

**DoubleBuffer** enables double buffering for dragging elements on the graph.

## Using Algorithms

In the **Algorithms** menu, shown in [Figure 11-9](#), various algorithms can be used to enhance and otherwise alter the graph layout.



### Note

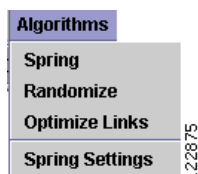
The algorithms only work when the nodes are interconnected with links.

**Spring** is a graph layout algorithm that optimizes the graph layout based on weights.

**Randomize** rearranges the nodes in the current topology layout at random.

If there are overlapping links, the layout can be optimized by selecting **Optimize Links**.

**Figure 11-9**      *Algorithms Menu*

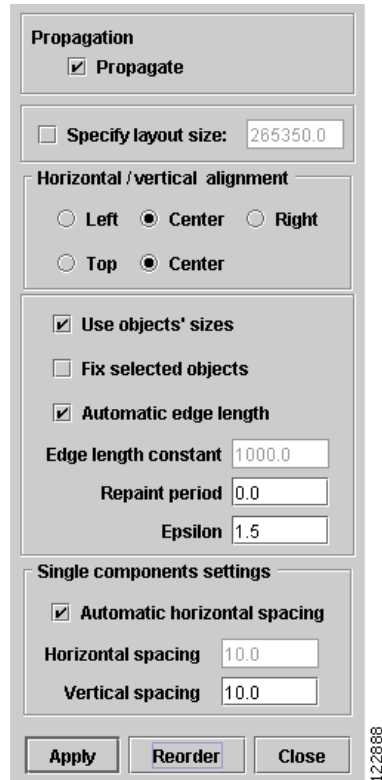


For further explanation of the **Algorithms** menu, see [Figure A-12 Algorithms Menu, page A-12](#).

The spring settings are used to enhance the appearance of the topology display according to user preferences. When selecting **Spring Settings**, the Spring Settings window in [Figure 11-10](#) appears.



Figure 11-10 Spring Settings



The Spring Settings dialog box is a vertical window with a light gray background. It contains several sections of controls:

- Propagation:** A checkbox labeled "Propagate" is checked.
- Specify layout size:** A checkbox is unchecked, followed by a text field containing "265350.0".
- Horizontal /vertical alignment:** Two rows of radio buttons. The first row has "Left", "Center" (selected), and "Right". The second row has "Top" and "Center" (selected).
- Use objects' sizes:** A checkbox is checked.
- Fix selected objects:** A checkbox is unchecked.
- Automatic edge length:** A checkbox is checked.
- Edge length constant:** A text field containing "1000.0".
- Repaint period:** A text field containing "0.0".
- Epsilon:** A text field containing "1.5".
- Single components settings:**
  - Automatic horizontal spacing:** A checkbox is checked.
  - Horizontal spacing:** A text field containing "10.0".
  - Vertical spacing:** A text field containing "10.0".

At the bottom of the dialog are three buttons: "Apply", "Reorder", and "Close". A small vertical text label "122888" is located to the right of the "Reorder" button.

For an explanation of the various fields in the Spring Settings window, see [Algorithms, page A-12](#).





## Traffic Engineering Management GUI

---

This chapter describes the Cisco IP Solution Center Traffic Engineering Management (ISC TEM) GUI and provides an explanation of the various fields, buttons, and other GUI elements. For a detailed description of the process flows for the various ISC TEM services, see the respective chapters and sections elsewhere in this user guide.

In this chapter, the different parts of the ISC GUI used by the ISC TEM component are described:

- [Accessing the TEM GUI, page A-1](#)
- [TE Providers, page A-3](#)
- [TE Topology, page A-5](#)
- [TE Nodes, page A-18](#)
- [TE Links, page A-21](#)
- [TE SRLGs, page A-30](#)
- [TE Explicit Paths, page A-33](#)
- [TE Protected Elements, page A-35](#)
- [Assign TE Resources, page A-40](#)
- [Create Managed TE Tunnel, page A-41](#)
- [Create Unmanaged TE Tunnel, page A-59](#)
- [Create TE Backup Tunnel, page A-59](#)
- [TE Traffic Admission, page A-64](#)
- [Administration, page A-67](#)
- [Monitoring, page A-67](#)

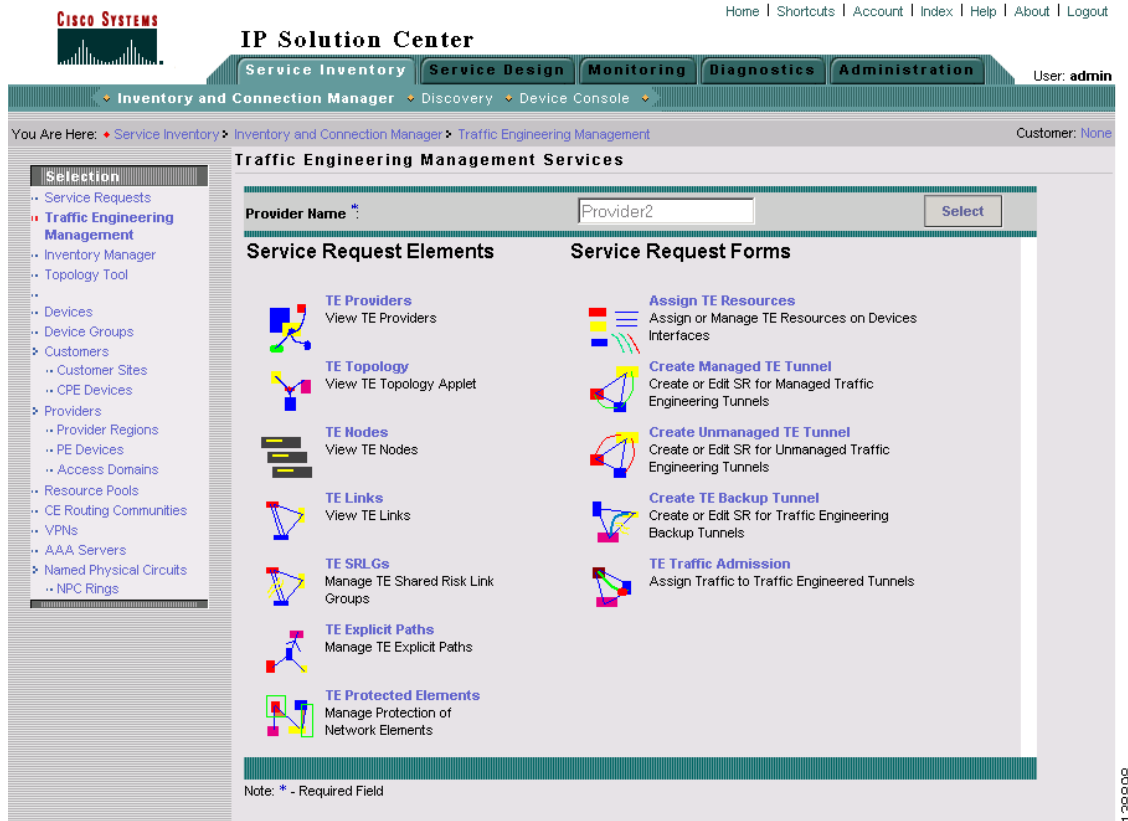
## Accessing the TEM GUI

The Traffic Engineering Management GUI forms part of the general Cisco ISC GUI.

This section describes the GUI elements in the Traffic Engineering Management Services window.

To access the TEM GUI, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**. The Traffic Engineering Management Services window in [Figure A-1](#) appears.

Figure A-1 Traffic Engineering Management Services



The main ISC TEM window includes the following service elements:

- Service Request Elements
  - **TE Providers**—Create and manage TE Providers.
  - **TE Topology**—View the ISC TEM application through a topology interface.
  - **TE Nodes**—View TE nodes and node details.
  - **TE Links**—View TE links.
  - **TE SRLGs**—Create and manage Shared Link Risk Groups (SRLGs).
  - **TE Explicit Paths**—Create and manage TE explicit paths.
  - **TE Protected Elements**—Manage protection of network elements.
- Service Request Forms
  - **Assign TE Resources**—Assign or manage TE resources on device interfaces.
  - **Create Managed TE Tunnel**—Create or edit SRs for managed TE tunnels.
  - **Create Unmanaged TE Tunnel**—Create or edit SRs for unmanaged TE tunnels.
  - **Create TE Backup Tunnel**—Create or edit SRs for TE backup tunnels .
  - **TE Traffic Admission**—Assign traffic to traffic-engineered tunnels.

# TE Providers

This section describes the GUI elements in the **TE Providers** tool.

To create a TE Provider, see [Creating a TE Provider, page 2-6](#).

To access the TE Providers window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Providers**. The TE Providers window in [Figure A-2](#) appears.

**Figure A-2** TE Providers

The TE Providers window contains the following fields:

- **Provider Name**—Name of TE provider.
- **System Lock Status**—Indicates whether or not the system lock is activated (**Locked** or **Unlocked**).

The following actions can be performed:

- **Create**—Create a TE provider.
- **Edit**—Edit the TE provider details.
- **Delete**—Delete a TE provider.
- **Manage Lock**—Manage the system lock status (see [Manage Lock, page 9-17](#)).

## Create/Edit TE Provider

To access the Create/Edit TE Provider window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Providers** and click **Create**.

The Create/Edit TE Provider window in [Figure A-3](#) appears.

Figure A-3 Create/Edit TE Provider

**Create/Edit TE Provider**

Provider Name \* :  Select

**Primary Route Generation Parameters:**

Default Primary RG Timeout (sec) \* :

**Backup Route Generation Parameters:**

Backup RG Timeout (sec) \* :

FRR Protection Type \* : ☒ Sub Pool ☐ Any Pool

Default Link Speed Factor \* :

Minimum Bandwidth Limit (kbps) \* :

Max. Load Balancing Tunnel Count \* :

**Discovery Default Parameters:**

Region for TE Devices \* :  Select

Customer for Primary Tunnels:  Select

Save Cancel

Note: \* - Required Field

122618

The Create/Edit TE Provider window contains the following fields:

- **Provider Name**—Name of the provider to be associated with the TE provider.
- **Default Primary RG Timeout**—Default computation timeout for primary tunnels.
- **Backup RG Timeout**—Computation timeout per element for backup tunnels (for each protected element, the timer is reset to zero before the ISC TEM attempts to protect it).
- **FRR Protection Type**—Fast Re-Route (FRR) protection type:
  - **Sub Pool**—Bandwidth will be reserved from Sub Pool.
  - **Any Pool**—Bandwidth will be reserved from Sub Pool or Global Pool.

For a definition of pool types, see [Bandwidth Pools, page 1-5](#).

- **Default Link Speed Factor**—Default multiplication factor to be applied to the link speed in order to determine move affected tunnels. that needs to be protected. The link's bandwidth can be multiplied by the link speed factor, and the resulting bandwidth is then available to FRR backup tunnels on the link after subtracting the RSVP bandwidth reserved for the link.

Interpretation of the link speed factor:

> 1.0 (overbooking)—more backup bandwidth than the link has available.

< 1.0 (underbooking)—less backup bandwidth than the link has available.

- **Minimum Bandwidth Limit**—Minimum bandwidth allowed for backup tunnels.
- **Max. Load Balancing Tunnel Count**—This is the maximum number of backup tunnels needed to protect a flow through a protected element. Here, a flow is defined as follows:

There are two flows in a protected link, one in each of the directions that traffic can flow. For a node, the number of flows depends on the number of neighbouring nodes for a particular node. There is a flow for each neighbour pair. So a node with 3 neighbours, A, B, and C, has 6 flows through it – A->B, A->C, B->A, B->C, C->A, C->B.

- **Region for TE Devices**—Name of provider region.
- **Customer for Primary Tunnels**—Customer for primary TE tunnels.

For step-by-step instructions on how to create or edit TE providers, go to [Creating a TE Provider, page 2-6](#).

## TE Topology

This section describes the various fields, buttons, and other GUI elements in the TE Topology GUI. For instructions on how to use the TE Topology tool, see [Chapter 11, “TE Topology”](#).

ISC TEM includes a TE Topology tool that is accessed as a **TE Topology Interface Applet** that displays the TE topology through a Java applet within the browser.

For specific instructions on how to use the topology applet, see [Using the TE Topology Interface Applet, page 11-2](#).



### Note

There are several ways to access the TE Topology tool, among others by using **Inventory and Connection Manager > Topology Tool** and **Inventory and Connection Manager > Traffic Engineering Management > Topology Tool**. In this section, it is assumed that the TE tools are accessed from the Traffic Engineering Management Services page.

## Topology Display

To access the **TE Topology** tool, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Topology** and select **ISC-TEM Topology Interface Applet**

The topology display appears immediately in a separate window as shown in [Figure A-4](#).

The screenshot displays the NTGraph application window. The top menu bar includes 'Applet', 'Repository', 'File', 'Map', 'Graph', 'Tunnels', 'Algorithms', 'View', and 'Tools'. Below the menu is a toolbar with icons for file operations, zooming (set to 100%), antialiasing, double buffering, and a color palette. The main area shows a network graph with nodes represented by blue router icons. Nodes are labeled 'isctmp1' through 'isctmp14'. Some nodes are connected by lines representing network links, with some links labeled with IP addresses and port numbers (e.g., '10.2.3.14<->10.2.3.73'). A red question mark icon is also present, labeled '192.168.118.178'. The bottom of the window features a status log with the following text:

```

Nov 5, 2005 12:29:20 PM NTGraph createMenus
INFO: creating menus for graph panel
Nov 5, 2005 12:29:20 PM NTVisualizerIm createGraphPanel
INFO: creating graph panel
Nov 5, 2005 12:29:20 PM NTVisualizerIm createSplitPane
INFO: creating split pane for graph pane and data pane









```

- **Repository**—Discard or save the layout graph.
- **File**—Gain access to the print functionality.
- **Map**—Load or clear maps. Is used to associate a map with a view.
- **Graph**—Access a range of tools to manage and manipulate graphs.
- **Tunnels**—View or update the tunnel layout.
- **Algorithms**—Randomize or optimize links and set spring settings.
- **View**—Modify the zoom level in the current view.
- **Tools**—Modify the magnetic grid settings and the layer visibility.

The **Topology Display** window toolbar contains the elements shown in [Table A-1](#).



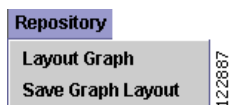
**Table A-1**      **Topology Display Toolbar Elements**

Icon	Purpose
	Print this view.
	Zoom the graph by a factor of 200%.
	Zoom the graph by a factor of 100%.
	Zoom the graph by a factor of 50%.
	Toggle antialiasing on/off. When drawing a view, this creates smoother lines and a more pleasant appearance at the expense of performance.
	Start/stop double buffering. This smooths the lines when dragging elements.
	Configure the magnetic grid in the current view.
	Manage active layers in the current view.

For instructions on how to use the Topology Display, see [Using the TE Topology Interface Applet, page 11-2](#).

## Repository

The **Repository** menu in [Figure A-5](#) serves to discard or save the layout graph.

**Figure A-5 Repository Menu**

The **Repository** menu contains the following elements:

- **Layout Graph**—If a graph layout is already present, the layout is cleared. If not, the layout of the elements in the repository is drawn. If a layout has previously been saved, the saved layout is re-created. Otherwise, a random layout is generated.
- **Save Graph Layout**—Save the current graph layout. Doing so ensures that whenever the graph layout is cleared with **Layout Graph** or the **Topology Display** applet is closed, the same layout is created when the applet is restarted.

## File

The **File** menu in [Figure A-6](#) provides access to the print functionality.

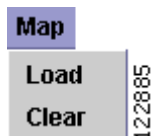
**Figure A-6 File Menu**

The **File** menu contains the following element:

- **Print**—Print the current topology view.

## Map

The **Map** menu in [Figure A-7](#) serves to load or clear maps.

**Figure A-7 Map Menu**

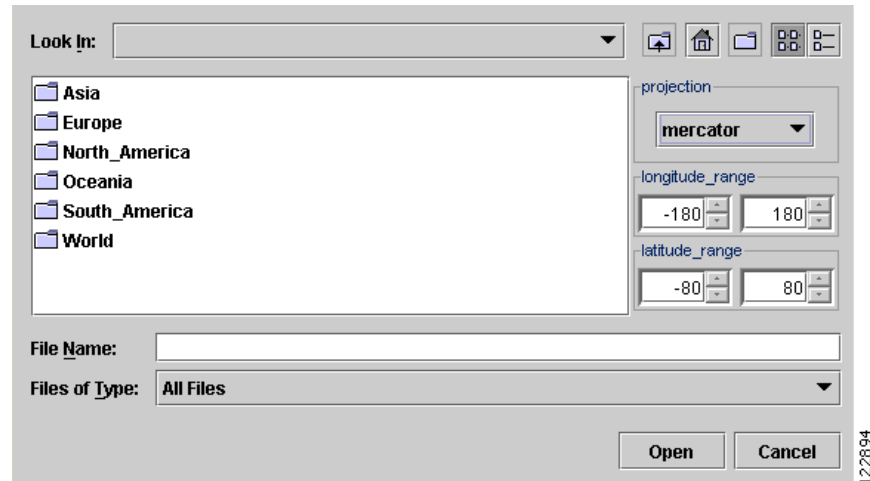
The **Map** menu contains the following elements:

- **Load**—Opens the Map Chooser for selecting a topology map.
- **Clear**—Clears the current topology map.

### Load Map

When selecting **Load** from the **Map** menu, the Map Chooser window in [Figure A-8](#) appears.

Figure A-8 Map Chooser






The Map Chooser window contains the following elements:



- **Look In**—Change the location from where to load the map.
- **File Name**—Specify the desired file name.
- **Files of Type**—Select the file type of the files to be displayed.
- **Open**—Open the selected directory or a topology map.
- **Cancel**—Close the **Map Chooser** window.
- **File Dialog Commands**—Serves to determine the desired directory and level of detail of data files.

The Map Chooser window navigation toolbar contains the elements shown in [Table A-2](#).

Table A-2 Map Chooser Toolbar Elements

Icon	Purpose
	Move to the parent directory of the current directory.
	Return to the home directory.
	Create a new folder in the selected directory or, if none are selected, the current directory.

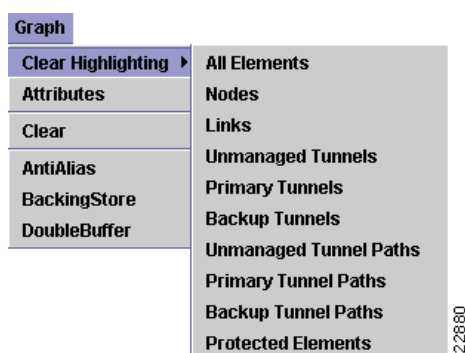
**Table A-2** Map Chooser Toolbar Elements (continued)

Icon	Purpose
	List the contents of the current directory.
	Provide type, size, and date and time details about files and directories in the current directory.

- **Projection**—Choose the projection in which a map is shown. A map projection is a projection which maps a sphere onto a plane. Typical projections are Mercator, Lambert, and Stereographic.
- **Longitude Range**—Choose a geographical longitude range.
- **Latitude Range**—Choose a geographical latitude range.

## Graph

The **Graph** menu in [Figure A-9](#) provides access to a range of tools to manage and manipulate graphs.

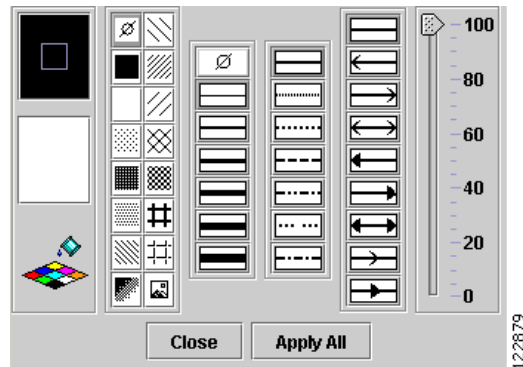
**Figure A-9** Graph Menu

The **Graph** menu contains the following elements:

- **Clear Highlighting**—Remove the highlighting of selected elements in the graph layout:
  - **All elements**—Highlighting of all network elements in the graph is cleared.
  - **Nodes**—Highlighting of all nodes in the graph is cleared.
  - **Links**—Highlighting of all links in the graph is cleared.
  - **Primary Tunnels**—Highlighting of all primary tunnels in the graph is cleared.
  - **Backup Tunnels**—Highlighting of all backup tunnels in the graph is cleared.
  - **Unmanaged Tunnel Paths**—Highlighting of all unmanaged tunnel paths in the graph is cleared.
  - **Primary Tunnel Paths**—Highlighting of all primary tunnel paths in the graph is cleared.
  - **Backup Tunnel Paths**—Highlighting of all backup tunnels paths in the graph is cleared.

- **Protected Elements**—Highlighting of all protected elements in the graph is cleared.
- **Attributes**—Opens the Graphics Attributes window in [Figure A-10](#).

**Figure A-10** Graphics Attributes Window



To understand the tools in the Graphics Attributes window, mouse over the various attributes. Choose the desired settings for line color, fill color and pattern, line thickness and style, arrow, and transparency.

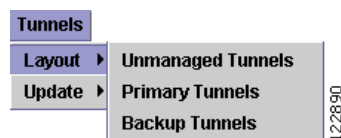
Click **Apply All** to activate your selections or **Close** to quit the Graphics Attributes window.

- **Clear**—As opposed to the **Layout Graph** item in the **Repository** menu, which also clears the current graph from the topology display, the **Clear** function in the **Graph** menu only clears the graph from the current view without re-creating it.
- **AntiAlias**—Activate antialiasing to smooth lines in the layout.
- **BackingStore**—Store graphics content when moved to the background and regenerate it when moved to the foreground. This helps avoid superfluous refreshing.
- **DoubleBuffer**—Start/stop double buffering. Smoothes the lines when dragging elements.

## Tunnels

The **Tunnels** menu in [Figure A-11](#) is used to highlight TE tunnels in the network.

**Figure A-11** Tunnels Menu



The **Tunnels** menu contains the following elements:

- **Layout**—Use **Layout** the first time you want to highlight tunnels using the repository.
  - **Unmanaged Tunnels**—Highlight unmanaged tunnels only.
  - **Primary Tunnels**—Highlight primary tunnels only.
  - **Backup Tunnels**—Highlight backup tunnels only.

**Note**

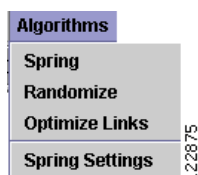
Selecting **Layout** repeatedly does not update the display.

- **Update**—Use **Update** to update tunnels in the display with the last instance of the repository.
  - **Unmanaged Tunnels**—Update the highlighting of unmanaged tunnels.
  - **Primary Tunnels**—Update the highlighting of primary tunnels.
  - **Backup Tunnels**—Update the highlighting of backup tunnels.

## Algorithms

In the **Algorithms** menu in [Figure A-12](#) various algorithms can be used to enhance and otherwise alter the graph layout.

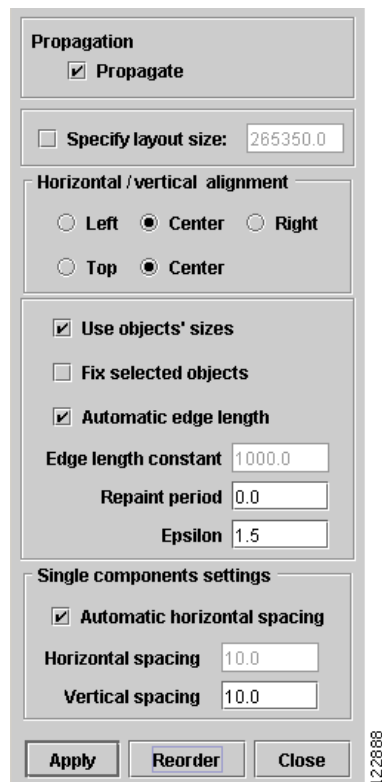
**Figure A-12**      *Algorithms Menu*



The **Algorithms** menu contains the following elements:

- **Spring**—Applies the Spring algorithm to the current graph layout using the attribute settings in the Spring Settings window.
- **Randomize**—Applies the Randomize algorithm to the nodes in the current topology layout.
- **Optimize Links**—This feature is used to move overlapping links apart when multiple links are present between nodes using the Links Optimization algorithm.
- **Spring Settings**—The spring settings are used to enhance the appearance of the topology display by setting attributes according to user preferences. When selecting **Spring Settings**, the Spring Settings window in [Figure A-13](#) appears.

Figure A-13 Spring Settings



The image shows a 'Spring Settings' dialog box with the following sections and controls:

- Propagation**: A checkbox labeled 'Propagate' which is checked.
- Specify layout size**: A checkbox labeled 'Specify layout size' which is unchecked, followed by a text input field containing '265350.0'.
- Horizontal / vertical alignment**: Two rows of radio buttons. The first row has 'Left', 'Center' (selected), and 'Right'. The second row has 'Top' and 'Center' (selected).
- Use objects' sizes**: A checkbox labeled 'Use objects' sizes' which is checked.
- Fix selected objects**: A checkbox labeled 'Fix selected objects' which is unchecked.
- Automatic edge length**: A checkbox labeled 'Automatic edge length' which is checked.
- Edge length constant**: A text input field containing '1000.0'.
- Repaint period**: A text input field containing '0.0'.
- Epsilon**: A text input field containing '1.5'.
- Single components settings**: A checkbox labeled 'Automatic horizontal spacing' which is checked.
- Horizontal spacing**: A text input field containing '10.0'.
- Vertical spacing**: A text input field containing '10.0'.
- Buttons**: 'Apply', 'Reorder', and 'Close' buttons at the bottom.

A small vertical text '122888' is visible on the right side of the dialog box.

The **Spring Settings** menu contains the following elements:

- **Propagate**—Propagate the various settings in the Spring Settings window to all child layouts.
- **Specify layout size**—Specify the layout size in pixels.
- **Horizontal / vertical alignment**—Align the topology graph in the Topology Display.
- **Use objects' sizes**—Use the objects' actual layout sizes without scaling.
- **Fix selected objects**—Fix the location of selected objects in the Topology Display.
- **Automatic edge length**—Allow the topology application to automatically assign an appropriate length to each link.
- **Edge length constant**—If **Automatic edge length** is not selected, you can specify a fixed edge length here.
- **Repaint period**—Sets the period (number of loops) used to repaint objects when the objects are being laid out in a graph.
- **Epsilon**—The epsilon constant determines when the iterative process for the Spring algorithm should stop. The greater this constant, the faster the layout, but the more distant the final position from the optimal layout.
- **Automatic horizontal spacing**—Let the topology application automatically determine the horizontal spacing between the devices in the graph.
- **Horizontal spacing**—Specify a fixed horizontal spacing between the devices in the graph.
- **Vertical spacing**—Specify a fixed vertical spacing between the devices in the graph.

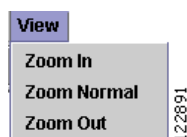
After you have made your selections, you can do any of the following:

- **Apply**—Save the Spring settings.
- **Reorder**—Rerun the Spring algorithm to reorder the graph elements based on the Spring settings.
- **Close**—Close the Spring Settings window without saving the selections.

## View

The **View** menu in [Figure A-14](#) allows zooming in the current view.

**Figure A-14** View Menu



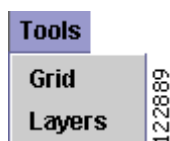
The **View** menu contains the following elements:

- **Zoom In**—Increases the magnification level.
- **Zoom Normal**—Resets the magnification level to the default setting.
- **Zoom Out**—Decreases the magnification level.

## Tools

The **Tools** menu in [Figure A-15](#) allows you to modify the magnetic grid settings and the layer visibility. Different network elements are drawn in different layers. Individual layers can be turned on or off using the Layers menu.

**Figure A-15** Tools Menu



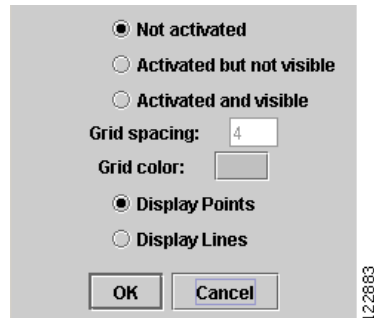
The **Tools** menu contains the following elements:

- **Grid**—Allows you to add a background grid to the graph based on the selections in the **Magnetic Grid** window.
- **Layers**—Allows you to select the layers to be displayed in the graph using the **Layer Visibility** window.

## Grid

The Magnetic Grid window in [Figure A-16](#) allows you to modify the magnetic grid settings. An activated grid appears under the graph layout in the Topology Display.



**Figure A-16**      **Magnetic Grid**

The Grid window contains the following elements:

- **Not activated**—Tells the application not to place a magnetic grid in the Topology Display.
- **Activated but not visible**—The network elements are not visible but still snaps to grid.
- **Activated and visible**—Make the grid active and visible in the Topology Display.
- **Grid spacing**—Set the spacing between the lines in the grid.
- **Grid color**—Click the square to open the color palette to set the grid line color as described in [Grid Color, page A-15](#).
- **Display points**—Display links using dotted lines.
- **Display lines**—Display links using solid lines.

Click **OK** to apply the settings or click **Cancel** to cancel the operation and return to the Topology Display window.

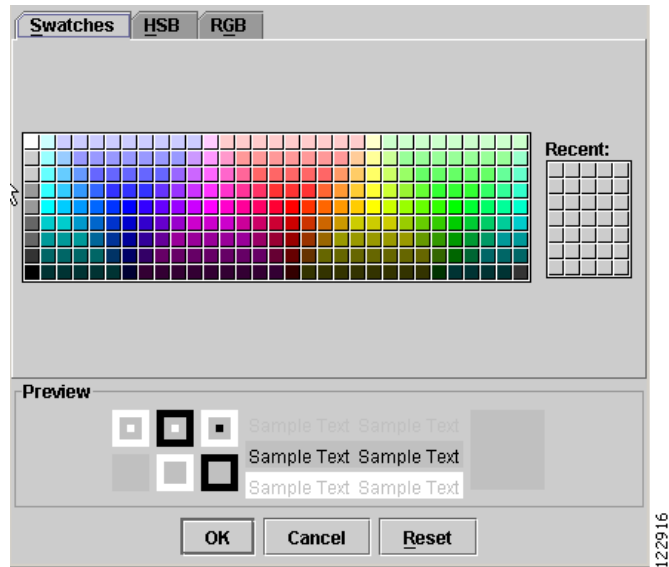
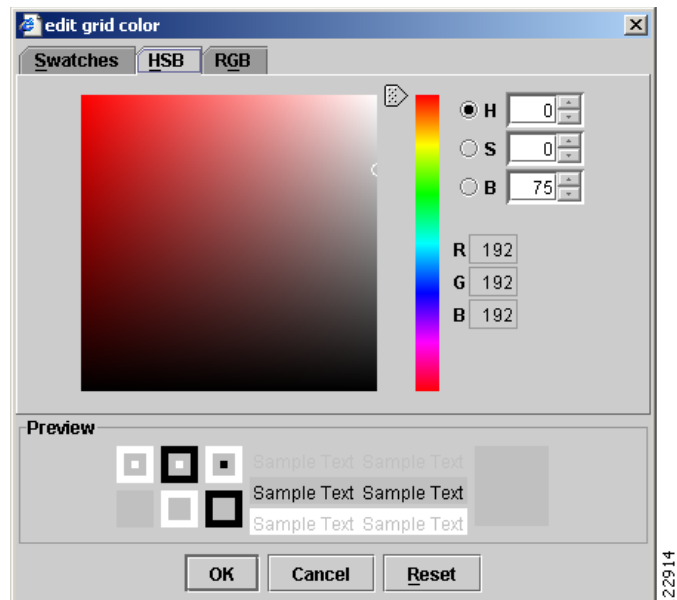
### Grid Color

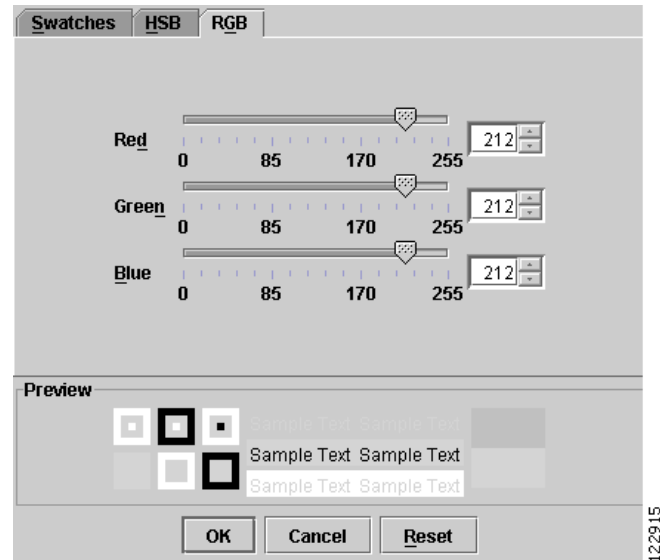
The Grid Color window in [Figure A-17](#) has three tabs:

**Swatches**—The Swatches palette (shown) provides color swatches for making rapid color choices.

**HSB**—The HSB palette in [Figure A-18](#) is used to set hue, saturation, and brightness.

**RGB**—The RGB window in [Figure A-19](#) is used to set the color intensity for red, green, and blue, respectively.

**Figure A-17** *Edit Grid Color - Swatches***Figure A-18** *Edit Grid Color - HSB Settings*

**Figure A-19** Edit Grid Color - RGB Settings

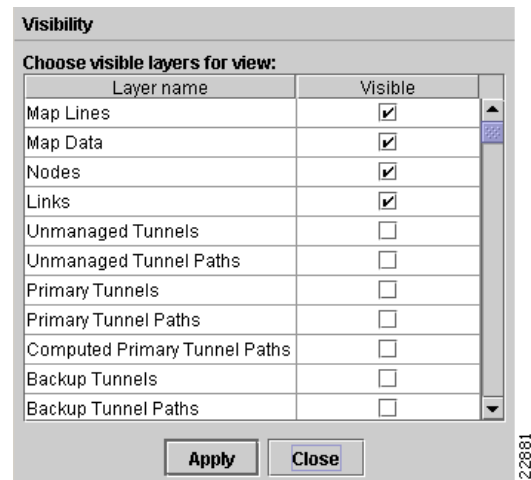
Make the desired changes and click **OK**.

Click **Reset** to reapply the default settings.

## Layers

The various network elements are organized into layers that can be turned on and off to display only the part of the TE network that you want to see.

Select **Tools > Layers** to access the Layer Visibility window shown in [Figure A-20](#).

**Figure A-20** Layer Visibility

In the Layer Visibility window, specify which layers should be visible by clicking the corresponding check boxes in the **Visible** column:

- **Map Lines**—Select to display map lines.
- **Map Data**—Select to display map data.
- **Nodes**—Select to display TE nodes.
- **Links**—Select to display TE links.
- **Unmanaged Tunnels**—Select to display TE unmanaged tunnels.
- **Unmanaged Tunnel Paths**—Select to display TE unmanaged tunnel paths.
- **Primary Tunnels**—Select to display TE primary tunnels.
- **Primary Tunnel Paths**—Select to display TE primary tunnel paths.
- **Computed Primary Tunnel Paths**—Select to display paths for computed primary tunnels.
- **Backup Tunnels**—Select to display TE backup tunnels.
- **Backup Tunnel Paths**—Select to display TE backup tunnel paths.

Click **Apply** to apply the settings or click **Close** to cancel the changes and quit the Layer Visibility window.

## TE Nodes

This section describes the GUI elements in the **TE Nodes** tool.

The nodes of the TE network can be viewed after running a **TE Discovery** task. For instructions on how to run a **TE Discovery** task, see [Chapter 3, “TE Network Discovery.”](#)

The **TE Nodes** tool gives access to both textual and visual information about the nodes discovered in the TE network.

To access the TE Nodes window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Nodes**. The TE Nodes List window in [Figure A-21](#) appears.

Figure A-21 TE Nodes List

**TE Nodes List**

Provider: Provider2

Show Devices with:  TE routers matching

Showing 1 - 10 of 15 records

#	<input type="checkbox"/>	Device Name	IGP ID	MPLS TE ID	Type	OS
1.	<input type="checkbox"/>	192.168.118.178	192.168.118.178	192.168.118.178	UNKNOWN	-
2.	<input type="checkbox"/>	isctmp1	192.168.118.176	192.168.118.176	CISCO_ROUTER	IOS
3.	<input type="checkbox"/>	isctmp11	192.168.118.166	192.168.118.166	CISCO_ROUTER	IOS_XR
4.	<input type="checkbox"/>	isctmp10	192.168.118.167	192.168.118.167	CISCO_ROUTER	IOS_XR
5.	<input type="checkbox"/>	isctmp12	192.168.118.168	192.168.118.168	CISCO_ROUTER	IOS_XR
6.	<input type="checkbox"/>	isctmp13	192.168.118.171	192.168.118.171	CISCO_ROUTER	IOS
7.	<input type="checkbox"/>	isctmp8	192.168.118.183	192.168.118.183	CISCO_ROUTER	IOS
8.	<input type="checkbox"/>	isctmp2	192.168.118.189	192.168.118.189	CISCO_ROUTER	IOS
9.	<input type="checkbox"/>	isctmp6	192.168.118.211	192.168.118.211	CISCO_ROUTER	IOS
10.	<input type="checkbox"/>	isctmp5	192.168.118.212	192.168.118.212	CISCO_ROUTER	IOS

Rows per page:  Go to page:  of 2

138928

The columns in the nodes list table provides the following information:

- **Device Name**—Hostname for the device.
- **IGP ID**—Interior Gateway Protocol (IGP) ID.
- **MPLS TE ID**—TE ID assigned by the router.
- **Type**—The device type. An **UNKNOWN** device type could signify a non-Cisco device.
- **OS**—Router operating system (IOS or IOS\_XR).

The following actions can be performed:

- **Close**—Close the Topology Display, if open.
- **Display**—Show the topology for one or more nodes in the TE network.
- **Details**—Show configuration details for a selected node.
- **Find**—You can search for particular devices by selecting the device type in the drop-down menu **Show Devices with** and specify matching criteria in the **TE routers matching** field.



Note

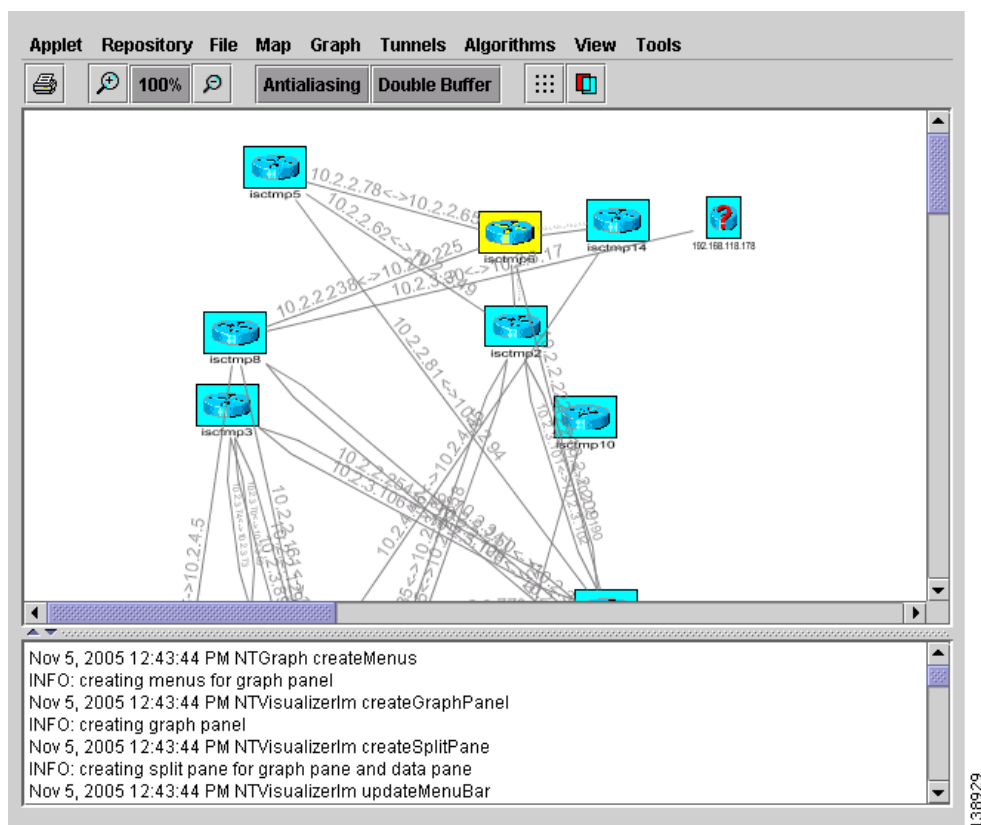
Sorting on MPLS TE ID is not supported.

## Display TE Nodes

The Topology Display can be invoked to highlight selected nodes.

Go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**. Click **TE Nodes**. Select one or more devices by clicking the corresponding check boxes. Click the **Display** button. The **Topology Display** applet in [Figure A-22](#) appears.

**Figure A-22** TE Nodes Topology Display



Any nodes that were selected before the applet was started are highlighted in the display. Unknown devices are marked with a red question mark.

For a description of how to use the **Topology Display** features, see [Topology Display, page A-5](#).

## View Node Details

To view the detailed information about a particular node, use the following steps, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Nodes**.

Select a device by clicking the corresponding check box. Click the **Detail** button. The TE Node Details window in [Figure A-23](#) appears.

**Figure A-23**      **TE Node Details**

TE Node Details	
Router Name:	iscntp13
IGP ID:	192.168.118.171
MPLS TE ID:	192.168.118.171
Interfaces:	FastEthernet0/0/0 10.2.4.53/30 GigabitEthernet2/0/0 10.2.4.46/30 GigabitEthernet1/0/0 10.2.4.50/30
Topology Map Coordinates:	(0,0,0,0)
OS:	IOS

The TE Node Details window contains the following fields:

- **Router Name**—Hostname of the router
- **IP Address**—IP address of the router
- **MPLS TE ID**—TE ID assigned by the router
- **Interfaces**—TE interfaces on the routers
- **Topology Map Coordinates**—Coordinates of the nodes in the Topology Display.
- **OS**—Router operating system.

Click **OK** to close the TE Node Details window.

## TE Links

This section describes the GUI elements in the **TE Links** tool.

The links of the TE network can be viewed after running a **TE Discovery** task. For instructions of how to run a **TE Discovery** task, see [Chapter 3, “TE Network Discovery.”](#)

The TE Links window gives access to both textual and visual information about the links discovered in the network.

To access the TE Links window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Links**. The TE Links List window in [Figure A-24](#) appears.

Figure A-24 TE Links List

**TE Links List**

**TE Provider** Provider2

Show TE Links with  matching  All

Showing 1 - 5 of 35 records

#	<input type="checkbox"/>	End Device A	Type	Interface A	End Device B	Type	Interface B	Label	Admin Status
1.	<input type="checkbox"/>	isctmp11	CISCO_ROUTER	POS0/2/0/0	isctmp12	CISCO_ROUTER	POS0/3/0/0	10.2.4.10<->10.2.4.9	UP
2.	<input type="checkbox"/>	isctmp11	CISCO_ROUTER	POS0/3/0/1	isctmp12	CISCO_ROUTER	POS0/1/0/1	10.2.4.14<->10.2.4.13	UP
3.	<input type="checkbox"/>	isctmp11	CISCO_ROUTER	POS0/0/0/0	isctmp8	CISCO_ROUTER	POS5/0	10.2.4.6<->10.2.4.5	UP
4.	<input type="checkbox"/>	isctmp10	CISCO_ROUTER	POS0/2/0/0	isctmp12	CISCO_ROUTER	POS0/4/0/0	10.2.4.22<->10.2.4.21	UP
5.	<input type="checkbox"/>	isctmp12	CISCO_ROUTER	GigabitEthernet0/2/0/0	isctmp7	CISCO_ROUTER	GigabitEthernet5/0	10.2.4.29<->10.2.4.30	UP

Rows per page:

Go to page:  of 7

The columns in the links list table provides the following information:

- **End Device A**—Hostname on endpoint A of the link.
- **Type**—Type of device for end device A.
- **Interface A**—Interface name on endpoint A of the link.
- **End Device B**—Hostname on endpoint B of the link.
- **Type**—Type of device for end device B.
- **Interface B**—Interface name on endpoint B of the link.
- **Label**—IP addresses of the interfaces on the link.
- **Admin Status**—Indicates whether the link is **UP** or **DOWN**.



**Note** This is local to ISC TEM. It is not the network interface status.

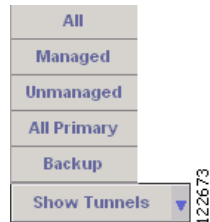
The following actions can be performed:

- **Close**—Close the Topology Display applet if open.
- **Display**—Open the Topology Display applet to visualize one or more links in the TE network.
- **Details**—Show link details.
- **Show Tunnels**—Display only tunnels that meet the following criteria (see [Figure A-25](#)):
  - **All**—Show all tunnels.
  - **Managed**—Show managed tunnels.
  - **Unmanaged**—Show unmanaged tunnels.
  - **All Primary**—Show all primary tunnels.
  - **Backup**—Show backup tunnels.

For more information about the Show Tunnels feature, see [Show Tunnels, page A-25](#).

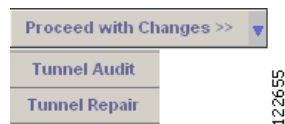


Figure A-25 Show Tunnels Options



- **Edit:**
  - **Interface A**—Edit the resources associated with interface A on the link.
  - **Interface B**—Edit the resources associated with interface B on the link.
- **Change Status:**
  - **Enable**—Make a link active (**UP** in the **Admin Status** column).
  - **Disable**—Deactivate a link (**DOWN** in the **Admin Status** column).
- **Proceed with Changes >>** (see Figure A-26): For verifying a resource change that might impact tunnel placement.
  - **Tunnel Audit**—If you disable an interface, **Tunnel Audit** checks if the status change affects existing managed tunnels.
  - **Tunnel Repair**—If **Tunnel Audit** reveals that Tunnel Placement is affected, **Tunnel Repair** can be used to move the tunnel away from the links to be disabled.

Figure A-26 TE Links List - Proceed with Changes



- **Cancel**—Cancel the operation and return to the Traffic Engineering Management Services window.
- **Find**—You can search for particular links by specifying a device type or a label in the drop-down menu **Show TE Links with** and specifying matching criteria in the **Matching** field.

## Display TE Links

The Topology Display can be invoked to highlight selected links.

Go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Links**. Select one or more devices by clicking the corresponding check boxes. Click the **Display** button. The **Topology Display Applet** in Figure A-4 appears.

Any selected links in the display are highlighted.

For a description of how to use the **Topology Display** features, see [Using the TE Topology Interface Applet, page 11-2](#).

For an explanation of the GUI elements in the **TE Topology Display** applet, see [Topology Display, page A-5](#).

# View Link Details

To view the detailed information about a particular link, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Links**. Select a device by clicking the corresponding check box. Click the **Detail** button. The TE Objects Details window in [Figure A-27](#) appears.

Figure A-27 TE Objects Details

TE Objects Details

TE Link Details

Link:

10.2.4.53<->10.2.4.54

Device: isctmp13, Interface: FastEthernet0/0/0

	TotalAllocated BW (kbps)	GlobalPool BW (kbps)	SubPool BW (kbps)
bw[0]	20	49980	30000
bw[1]	0	49980	30000
bw[2]	0	49980	30000
bw[3]	0	49980	30000
bw[4]	0	49980	30000
bw[5]	0	49980	30000
bw[6]	0	49980	30000
bw[7]	0	49980	30000

GlobalUtil: 0%, SubpoolUtil: 0%

Managed TotalAllocated BW (kbps)

1000

Managed Unallocated GlobalPool BW (kbps)

49000

Managed Unallocated SubPool BW (kbps)

30000

Managed GlobalUtil (%)

2.0%

Managed SubpoolUtil (%)

0.0%

Device: isctmp4, Interface: FastEthernet3/0

	TotalAllocated BW (kbps)	GlobalPool BW (kbps)	SubPool BW (kbps)
bw[0]	0	50000	30000
bw[1]	0	50000	30000
bw[2]	0	50000	30000
bw[3]	0	50000	30000
bw[4]	0	50000	30000
bw[5]	0	50000	30000
bw[6]	0	50000	30000
bw[7]	0	50000	30000

GlobalUtil: 0%, SubpoolUtil: 0%

Managed TotalAllocated BW (kbps)

0

Managed Unallocated GlobalPool BW (kbps)

50000

Managed Unallocated SubPool BW (kbps)

30000

Managed GlobalUtil (%)

0.0%

Managed SubpoolUtil (%)

0.0%

Admin Status: UP

OK

The **TE Links Details** contains the following fields:

- **Link**—IP addresses of Endpoint A and Endpoint B.
- **Endpoint A/Endpoint B:**

- **Device**—Hostname of the device.
- **Interface**—Interface name.
- **TotalAllocated BW**—The total amount of allocated bandwidth on the link by tunnel hold priority (bw[0]-bw[7]).
- **GlobalPool BW**—The allocated Global Pool bandwidth on the link by tunnel hold priority (bw[0]-bw[7]).
- **SubPool BW**—The allocated Sub Pool bandwidth on the link by tunnel hold priority (bw[0]-bw[7]).
- **GlobalUtil**—Global Pool bandwidth utilization percentage.
- **SubpoolUtil**—Sub Pool bandwidth utilization percentage.
- **Managed TotalAllocated BW**—The total amount of allocated managed bandwidth (hold priority 0).
- **Managed Unallocated GlobalPool BW**—The total amount of managed bandwidth (hold priority 0) not allocated in the Global Pool.
- **Managed Unallocated SubPool BW**—The total amount of managed bandwidth (hold priority 0) not allocated in the Sub Pool.
- **Managed GlobalUtil (%)**—Global Pool bandwidth utilization resulting from all managed tunnels passing through the link.
- **Managed SubpoolUtil (%)**—Sub Pool bandwidth utilization resulting from all managed tunnels passing through the link.
- **Admin Status**—Indicates whether the link is **Up** or **Down**.

## Show Tunnels

This feature allows you to display which TE tunnels (primary and/or backup) pass through a particular TE Link and helps facilitate the tunnel planning and placement processes. In addition, you can see which tunnels are impacted when an interface (or link) in the TE network is shut down.

To view specific types of tunnels using the **Show Tunnels** button, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Links**. Select the desired link in the **TE Links List** (Figure A-24) and click **Show Tunnels** and select the type of tunnel you want to list.

The Show TE Tunnel List window in Figure A-28 appears.

**Figure A-28 Show TE Tunnel List**

**Show TE Tunnel List**

**TE Link:** isctmp4 FastEthernet2/1 <-> isctmp3 FastEthernet3/1 (10.2.3.106<->10.2.3.105)  
**Type:** Managed Primary Tunnels

Showing 1 - 1 of 1 record

#	<input type="checkbox"/>	Tunnel ID	T#	Head	Dest	Tunnel Type	Deploy Status	Policy	BW	BW Quota
1.	<input type="checkbox"/>	ISC-P7	1	isctmp3	isctmp4	Managed	DEPLOYED	ISC-P7-isctmp3:Tunnel1	40000	

Rows per page: 10 Go to page: 1 of 1 Go

Details OK

122672

The TE Managed Primary Tunnels SR window contains the following elements:

The columns in the tunnel list provides the following information:

- **Tunnel ID**—Unique tunnel identifier used within ISC TEM.
- **T#**—Tunnel number on the head router.
- **Head**—Hostname of the head router.
- **Dest**—Hostname of the destination router.
- **Tunnel Type**—Type of tunnel (managed or unmanaged).
- **Deploy Status**—Tunnel deployment status.
- **Policy**—TE policy for the tunnel.
- **BW**—Tunnel bandwidth. If the tunnel is auto-bw enabled, BW shows the higher of tunnel bandwidth and maximum automatic bandwidth.
- **BW Quota**—move affected tunnels. this backup tunnel can protect. The router limits the LSPs that can use this backup tunnel so that the sum of the bandwidth of the LSPs does not exceed the specified amount of bandwidth. If there are multiple backup tunnels, the router will use the best-fit algorithm.

To view the tunnel details for a particular tunnel, select a tunnel in the Show TE Tunnel List window and click **Detail**.

**Figure A-29**      **Show Tunnels - TE Objects Details**

TE Tunnel Details	
Type:	Managed TE Tunnel
Tunnel:	isctmp3:Tunnel1 (ISC-P7) isctmp3 <-> isctmp4 BW: 40000 kbps
Status:	Op: up, Admin: up
State:	DEPLOYED, Conformed
LSP configured:	10.2.3.106
LSP in use:	10.2.3.106 <-> 192.168.118.213
AutoBW:	Disabled

OK

For an explanation of the various GUI elements, see [View Managed Primary Tunnel Details, page A-43](#).

## Edit Interface

To edit information about a particular link, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Links**. Select the desired link in the **TE Links List** ([Figure A-24](#)). Click **Edit > Interface A** or **Edit > Interface B** to edit one of the interfaces on the link.

The TE Resource Modification window in [Figure A-30](#) appears.

Figure A-30 TE Resource Modification

**TE Resource Modification**

<b>SR Job ID:</b> New		<b>Provider:</b> Provider2	<b>SR ID:</b> New
<b>SR State:</b> REQUESTED		<b>Creator:</b>	<b>Type:</b> ADD
Device/Interface:	isctmp11 : POS0/2/0/0		
Peer Device/Interface:	isctmp12 : POS0/3/0/0		
Description:	<input type="text"/>		
Link Bandwidth (Kbps):	<input type="text" value="2488320"/>		
Max Global (BC0) Reservable (Kbps) *:	<input type="text" value="45000"/>		
Max Sub Pool (BC1) Bandwidth (Kbps) *:	<input type="text" value="30000"/>		
Attribute Bits (0x0-0xFFFFFFFF) *:	<input type="text" value="0x0"/>		
TE Metric *:	<input type="text" value="2000"/>		
Propagation Delay *:	<input type="text" value="0"/>		
Max Delay Increase *:	<input type="text" value="0"/>		
Link Speed Factor *:	<input type="text" value="1.0"/>		
<input type="button" value="Continue &gt;&gt;"/> <input type="button" value="Cancel"/>			

Note: \* - Required Field

138921

The TE Resource Modification window contains the following fields:

- **Device/Interface**—Name of device and interface.
- **Peer Device/Interface**—Name of device and interface for the other endpoint of the link.
- **Description**—Service request description.
- **Link Bandwidth**—Total bandwidth of the link.
- **Max Global (BC0) Reservable**—Maximum amount of bandwidth in kbps that can be reserved by TE Tunnels.
- **Max Sub Pool (BC1) Bandwidth**—Maximum amount of bandwidth in kbps that can be reserved by sub pool TE Tunnels. The range is from 1 to the value of **Max Global Reservable**.
- **Attribute Bits**—Links attributes to be compared to a tunnel's affinity bits during selection of a path. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.
- **TE Metric**—Metric used to override the Interior Gateway Protocol (IGP) administrative weight (cost) of the link.
- **Propagation Delay**—The time it takes for traffic to travel along a link from the head interface to the tail interface.
- **Max Delay Increase**—Used in computations of FRR backup-tunnels to constrain the propagation delay of a backup-tunnel for the link. A max delay increase for a link might need to be set to loosen the delay constraint when generating backup tunnels, as it is difficult to find backup tunnel paths where there is no increase in the delay compared with the flow being protected.

- **Link Speed Factor**—Multiplication factor to be applied to the link speed in order to determine move affected tunnels. that needs to be protected.

The following actions can be performed:

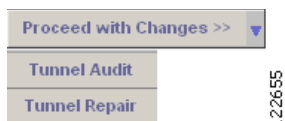
- **Continue >>**—Proceed to the confirmation page shown in [Figure A-31](#).
- **Cancel**—Cancel the operation and return to the TE Links List window.

**Figure A-31** TE Resource Modification (Confirmation Page)

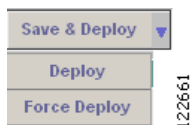
The screenshot displays the 'TE Resource Modification' window. At the top, it shows 'SR Job ID: New', 'SR State: REQUESTED', 'Provider: Provider2', 'Creator:', 'SR ID: New', and 'Type: ADD'. Below this are several input fields: 'Device/Interface:' with value 'isctmp11 : POS0/2/0/0', 'Peer Device/Interface:' with value 'isctmp12 : POS0/3/0/0', 'Description' (empty), 'Link Bandwidth (Kbps):' with value '2488320', 'Max Global (BC0) Reservable (Kbps) \*:' with value '45000', 'Max Sub Pool (BC1) Bandwidth (Kbps) \*:' with value '30000', 'Attribute Bits (0x0-0xFFFFFFFF) \*:' with value '0x0', 'TE Metric \*:' with value '2000', 'Propagation Delay \*:' with value '0', 'Max Delay Increase \*:' with value '0', and 'Link Speed Factor \*:' with value '1.0'. At the bottom right are three buttons: '<< Edit', 'Proceed with Changes >>', and 'Save & Deploy'. A note at the bottom left states 'Note: \* - Required Field'. A vertical text '138922' is on the right edge.

The **Confirmation Page** provides a view-only snapshot of the SR data and offers the following options:

- **<< Edit**—Return to the TE Resource Modification window.
- **Proceed with Changes >>** ([Figure A-32](#))—For verifying a resource change that can impact tunnel placement.
  - **Tunnel Audit**—If you change a resource, **Tunnel Audit** checks if the change affects existing managed tunnels.
  - **Tunnel Repair**—If **Tunnel Audit** reveals that Tunnel Placement is affected, **Tunnel Repair** can be used to move affected tunnels.

**Figure A-32** TE Links List - Proceed with Changes

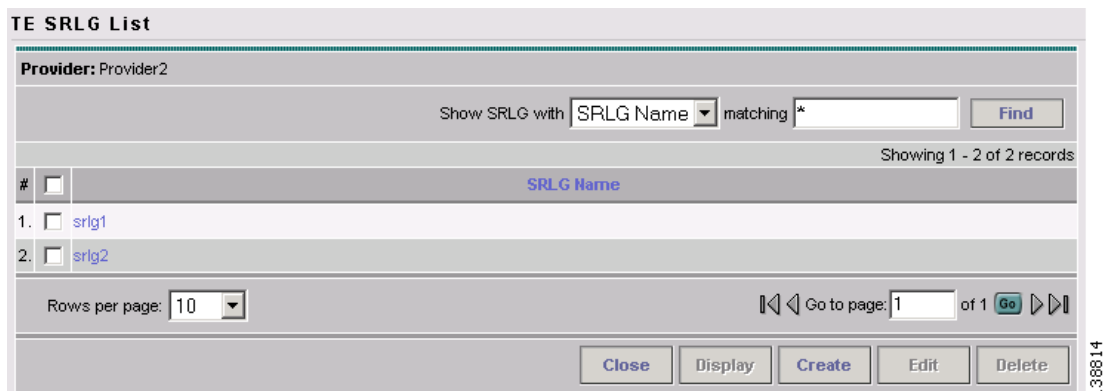
- **Save & Deploy** (Figure A-33)—For committing resource changes that do not impact tunnel placement. There are two options for saving and deploying the resource modification SR to the network:
  - **Deploy**—Use **Deploy** when the service request state is **Requested** or **Invalid**. This places the Resource Modification SR in the deployment queue.
  - **Force Deploy**—Use **Force Deploy** when the service request state is **Deployed** or **Failed Audit**. This could be useful when the provisioning failed, so that you need to force through the deployment of the Resource Modification SR for this provider to the network.

**Figure A-33** TE Links List - Save & Deploy Tunnels

## TE SRLGs

This section describes the GUI elements in the **TE SRLGs** tool. It is used to manage Shared Risk Link Groups (SRLGs) as part of ISC TEM protection management.

To access the TE SRLGs window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE SRLGs**. The TE SRLG List window in Figure A-37 appears.

**Figure A-34** TE SRLG List

The TE SRLG List window lists SRLGs by name.



The following actions can be performed:

- **Close**—Close the Topology Display.
- **Display**—Open the Topology Display applet to visualize the SRLG.
- **Create**—Create an SRLG.
- **Edit**—Edit an SRLG.
- **Delete**—Delete one or more SRLGs.
- **Show SRLG with**—You can search for particular SRLGs by specifying matching criteria in the **Matching** field and clicking **Find**.

## Create/Edit TE SRLG

This section describes the GUI elements in the TE SRLG Editor, which is used to both create and edit SRLGs.

The process of creating an SRLG is described in [Create SRLG, page 7-3](#).

To access the TE SRLG Editor, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE SRLGs**. In the TE SRLGs window, to create an SRLG click **Create** or to edit select an SRLG that you want to edit by clicking the corresponding check box and clicking **Edit**.

In either case, the TE SRLG Editor window in [Figure A-35](#) appears.

**Figure A-35** TE SRLG Editor

TE SRLG Editor

Provider Name \*:

SRLG Name \*:

Links :

#	<input type="checkbox"/>	Device From	Label	Device To
1.	<input type="checkbox"/>	isctmp8	10.2.2.126<->10.2.2.113	isctmp7
2.	<input type="checkbox"/>	isctmp1	10.2.3.85<->10.2.3.86	isctmp2
3.	<input type="checkbox"/>	isctmp1	10.2.3.89<->10.2.3.90	isctmp3
4.	<input type="checkbox"/>	isctmp1	10.2.2.129<->10.2.2.142	isctmp3
5.	<input type="checkbox"/>	isctmp1	10.2.3.93<->10.2.3.94	isctmp7

Showing 1 - 5 of 9 records

Rows per page: 5

Go to page: 1 of 2 Go

Add Link Remove Link

Save Cancel

The TE SRLG Editor window contains the following GUI elements:

- **Provider Name**—Name of the TE provider.
- **SRLG Name**—Unique name to identify the SRLG.

The columns in the TE SRLG Editor provide the following information:

- **Device From**—Hostname of the TE device that the link originates from.
- **Label**—IP addresses of the source and destination interfaces.
- **Device To**—Hostname of the TE destination device.

The following actions can be performed:

- **Add Link**—Add a link to the SRLG.
- **Remove Link**—Remove selected links from the SRLG.
- **Save**—Save the created or modified SRLG.
- **Cancel**—Cancel the operation and return to the TE SRLG List window.

**Step 4** When clicking **Add Link** to associate a link with the SRLG, the links associated with the SRLG window in [Figure A-36](#) appears. This table displays links that can be added to the SRLG.

**Figure A-36** Links associated with SRLG

Links associated with SRLG			
Show Links with: <input type="text" value="Device Name"/> Matching <input type="text" value="*"/> <input type="button" value="Find"/>			
Showing 1 - 10 of 32 records			
#	<input type="checkbox"/>	From Device	To Device
1.	<input type="checkbox"/>	isctmp4	isctmp9
2.	<input type="checkbox"/>	isctmp7	isctmp3
3.	<input type="checkbox"/>	isctmp4	isctmp9
4.	<input type="checkbox"/>	isctmp4	isctmp3
5.	<input type="checkbox"/>	isctmp4	isctmp3
6.	<input type="checkbox"/>	isctmp4	isctmp9
7.	<input type="checkbox"/>	isctmp5	isctmp4
8.	<input type="checkbox"/>	isctmp6	isctmp5
9.	<input type="checkbox"/>	isctmp6	isctmp4
10.	<input type="checkbox"/>	isctmp2	isctmp5

Rows per page:  Go to page:  of 4

The columns in the TE SRLG Editor provide the following information:

- **From Device**—Hostname of the TE device that the link originates from.
- **Link**—IP addresses of the source and destination devices.
- **To Device**—Hostname of the TE destination device.

The following actions can be performed:

- **Select**—Add selected links to the SRLG.
- **Cancel**—Cancel the operation and return to the TE SRLG Editor window.
- **Show Links with**—You can search for particular links by specifying matching criteria in the **Matching** field and clicking **Find**.

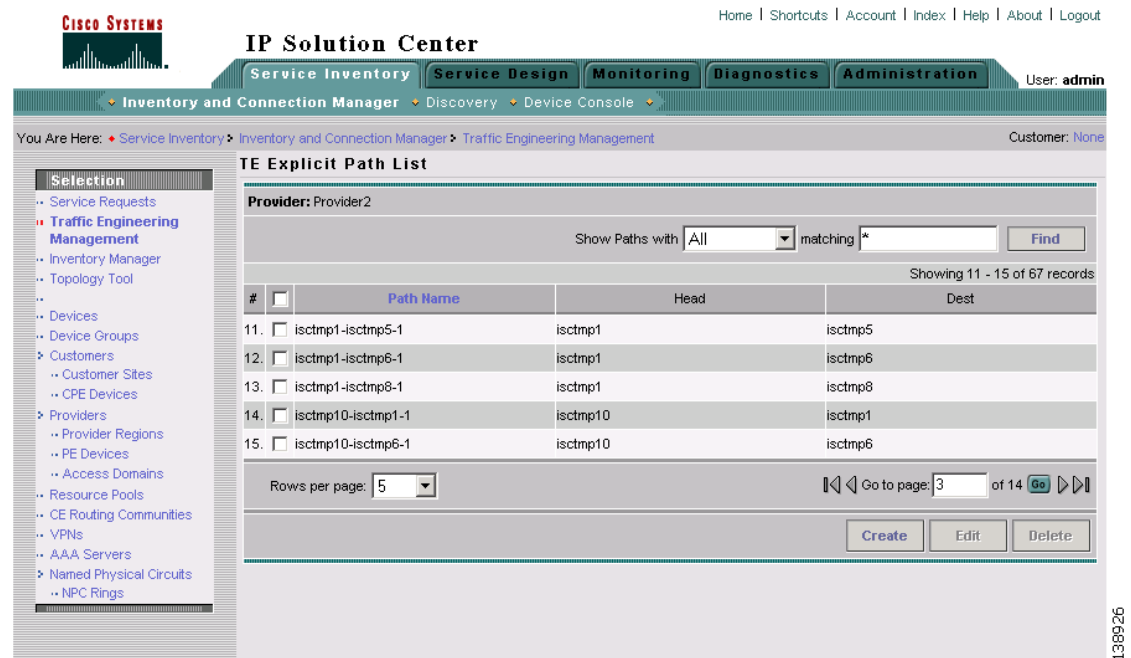
# TE Explicit Paths

This section describes the GUI elements in the **TE Explicit Path** tool.

TE explicit paths can be created after the execution of a **TE Discovery** task. For instructions on how to create an explicit path, see [Create Explicit Path, page 5-4](#).

To access the TE Explicit Path List window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Explicit Paths**. The TE Explicit Path List window in [Figure A-37](#) appears.

**Figure A-37** TE Explicit Path List



The columns in the TE Explicit Path list provides the following information:

- **Path Name**—Name of the explicit path.
- **Head**—Hostname of the head router.
- **Dest**—Hostname of the destination router.

The following actions can be performed:

- **Create**—Create an explicit path.
- **Edit**—Edit an explicit path.
- **Delete**—Delete an explicit path.
- **Find**—You can search for particular links by selecting the search variable in the drop-down menu **Show Paths with** and specify matching criteria in the **Matching** field.

## Create/Edit Explicit Path

This section describes the elements in the create and edit explicit path windows.

To create or edit an explicit path, see [Create Explicit Path, page 5-4](#).

The New TE Explicit Path window appears when you select **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Explicit Paths** to open the TE Explicit Path List window and click **Create**. The New TE Explicit Path window in [Figure A-38](#) appears.

**Figure A-38**      *New TE Explicit Path*

**New TE Explicit Path**

Path Name \*:

Head Router \*:

Links:

Showing 0 of 0 records

#	Device	Outgoing Interface	Outgoing IP	Next Hop	Incoming Interface	Incoming IP
Rows per page: 10    Go to page: 1 of 1 <input type="button" value="Go"/>						

Provision Preference \*: ☒ Outgoing Interface ☐ Incoming Interface

Note: \* - Required Field

122643

The New TE Explicit Path window contains the following GUI elements

- **Path Name**—Name of explicit path.
- **Head Router**—Name of the head router.
- **Links** (table)—Lists the links added for the current path and contains the following information:
  - **Device**—Hostname of the TE device that the path originates from.
  - **Outgoing Interface**—Interface name of the outgoing interface from the originating device.
  - **Outgoing IP**—IP address of the outgoing interface.
  - **Next Hop**—Hostname of the next hop device.
  - **Incoming Interface**—Incoming interface name on the next hop device.
  - **Incoming IP**—Incoming interface IP address on the next hop device.
- **Provision Preference**—Preference for provisioning the **next-address** subcommand of the **ip explicit-path** command. Choose between **Outgoing Interface** and **Incoming Interface**.
  - **Outgoing Interface**—Outgoing interface on the router.
  - **Incoming Interface**—Incoming interface on the router.

The following actions can be performed:

- **Add Link**—Add a link to the explicit path.

- **Delete Link**—Delete a link in the explicit path.
- **Save**—Save all the explicit path data entered.
- **Cancel**—Cancel the operation and return to the TE Explicit Path List window.

When clicking **Add Link** to add a blank line to the hop list table, the Select Next Hop window in [Figure A-39](#) appears.

**Figure A-39** Select Next Hop

#	Outgoing Interface	Outgoing IP	Next Hop	Type	Incoming Interface	Incoming IP
1.	<input type="radio"/> FastEthernet2/0/1	10.2.2.145	isctmp2	CISCO_ROUTER	FastEthernet1/0	10.2.2.158
2.	<input type="radio"/>		isctmp2	CISCO_ROUTER	Loopback0	192.168.118.189
3.	<input type="radio"/> FastEthernet2/1/0	10.2.3.54	isctmp9	CISCO_ROUTER	FastEthernet2/0	10.2.3.53
4.	<input type="radio"/>		isctmp9	CISCO_ROUTER	Loopback0	192.168.118.219
5.	<input type="radio"/> FastEthernet2/1/1	10.2.3.57	isctmp9	CISCO_ROUTER	FastEthernet2/1	10.2.3.58
6.	<input type="radio"/> FastEthernet1/0/0	10.2.2.161	isctmp8	CISCO_ROUTER	FastEthernet3/0	10.2.2.174
7.	<input type="radio"/>		isctmp8	CISCO_ROUTER	Loopback0	192.168.118.183
8.	<input type="radio"/> FastEthernet1/1/0	10.2.2.110	isctmp7	CISCO_ROUTER	FastEthernet0/0	10.2.2.97
9.	<input type="radio"/>		isctmp7	CISCO_ROUTER	Loopback0	192.168.118.214
10.	<input type="radio"/> FastEthernet3/1/0	10.2.3.93	isctmp7	CISCO_ROUTER	FastEthernet4/0	10.2.3.94

Showing 1 - 10 of 14 records

Rows per page: 10 Go to page: 1 of 2

Select Cancel

The columns in the TE Explicit Path list provide the following information:

- **Outgoing Interface**—Interface name of the outgoing interface from the originating device.
- **Outgoing IP**—IP address of the outgoing interface.
- **Next Hop**—Hostname of the next hop device.
- **Type**—Device type.
- **Incoming Interface**—Incoming interface name on the next hop device.
- **Incoming IP**—Incoming interface IP address on the next hop device.

## TE Protected Elements

This section describes the **TE Protected Elements** GUI.

For instructions on how to configure protected elements, see [Configure Element Protection, page 7-5](#).

## Protection Management

To access the TE Protection Management window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management**. Click **TE Protected Elements**.

The TE Protection Management window in [Figure A-40](#) appears.

**Figure A-40** TE Protection Management

The columns in the TE Protection Management table provide the following information:

- **Element Name**—Name of the network element to be protected.
- **Type**—Network element type (node, link, or SRLG).
- **Protection Status**—The protection status displayed is determined from the last time an audit was performed. The audit is performed either explicitly by the user or when the protection SR is deployed. The protection status is stated for each network element as either **Protected**, **Not Fully Protected**, or **Unknown**. Click on the column header, **Protected**, to sort elements according to protection status.

The following actions can be performed:

- **Close**—Close topology.
- **Display**—Open the Topology Display applet to visualize one or more protected elements.
- **Compute Backup** ([Figure A-41](#))—Automatically calculate the optimal backup tunnel for:
  - **All Elements**—all network elements listed, whether selected or not.
  - **Selected Elements**—all selected network elements.

**Figure A-41** Compute Backup Button

- **Audit Protection** ([Figure A-42](#))—Perform a protection audit on:
  - **All Elements**—all network elements listed, whether selected or not.
  - **Selected Elements**—all selected network elements.

**Figure A-42 Audit Protection**

- **Add**—Add a new protection element.
- **Delete**—Delete a protection element.
- **Cancel**—Cancel the operation and return to the Traffic Engineering Management Services window.
- **Find**—You can search for particular elements by selecting the All, Node, Link, or SRLG in the Show drop-down menu and specify matching criteria in the Matching field.

## Compute Backup

This section describes the Compute Backup GUI.

For instructions on how to run Compute Backup on all or selected elements, see [Configure Element Protection, page 7-5](#).

To run Compute Backup, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Protected Elements**. The TE Protection Management window in [Figure A-40](#) appears.

In the TE Protection Management window, select one or more elements for which you want ISC TEM to calculate a backup path.

Click **Compute Backup** and select one of the following:

- All Elements
- Selected Elements

The window in [Figure A-43](#) appears.

Figure A-43 TE Protection Computation Results

**TE Protection Computation Results**

**Element:**

Show  with name matching

Showing 1 - 10 of 37 records

#	<input type="checkbox"/>	Element Name	Type	Report	Status
1.	<input type="checkbox"/>	isctmp7	Node		InvalidTunnels
2.	<input checked="" type="checkbox"/>	isctmp7	Node	violationBadBackupTunnel	InvalidTunnels
3.	<input type="checkbox"/>	isctmp7	Node	violationBadBackupTunnel	InvalidTunnels
4.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
5.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
6.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
7.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
8.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
9.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels
10.	<input type="checkbox"/>	isctmp7	Node	violationNoBackupTunnels	InvalidTunnels

Rows per page:  Go to page:  of 4

**Violation and Warning:**

**Backup Tunnels:**

Op	Tunnel ID	Head	Dest	T#	BW	Path	Protection Type	Report
<input type="button" value="Accept Solution"/> <input type="button" value="Cancel"/>								

The **Element:** table displays the outcome of the computation for each element in the protection computation. The status for each element is indicated by at least one row per element in the table. If the status is not valid, the table will contain one row per warning or violation.

The **Element:** table contains the following columns:

- **Element Name**—Name of the network element to be protected.
- **Type**—Network element type (node, link, or SRLG).
- **Report**—Warning or violation associated with an element, if any, as reported by the computation engine.
- **Status**—Computation status of the network element:
  - Valid Tunnels—The element is fully protected by backup tunnels.
  - InvalidTunnels—An Audit Protection detected that the element was not fully protected by the existing backup tunnels.
  - No Solution Exists—A Compute Backup has proven that it is not possible to fully protect the element.

The following actions can be performed:

- **Close**—Close the Topology Display applet if open.
- **Display**—Open the Topology Display applet to visualize one or more protected elements and their protection tunnel(s). The Topology Display is shown in [Figure A-4](#).



- **Details**—List backup tunnels and violations/warnings for the selected network element. The information is displayed in the **Backup Tunnels:** section and the **Violation and Warning:** section, if applicable, as shown in Figure A-44.

**Violation and Warning:** pane—Describes the selected violation/warning and any relevant details about the corresponding link or flow.

Figure A-44 TE Protection Computation Results with Backup Tunnels

**TE Protection Computation Results**

**Element:**  
Show  with name matching    
Showing 1 - 4 of 4 records

#	<input type="checkbox"/>	Element Name	Type	Report	Status
1.	<input type="checkbox"/>	10.2.2.33<->10.2.2.46	Link	NoSolutionExists	NoSolutionExists
2.	<input type="checkbox"/>	10.2.2.33<->10.2.2.46	Link	violationNoBackupTunnels	NoSolutionExists
3.	<input type="checkbox"/>	10.2.2.33<->10.2.2.46	Link	violationNoBackupTunnels	NoSolutionExists
4.	<input checked="" type="checkbox"/>	isctmp4	Node	ValidTunnels	ValidTunnels

Rows per page:

**Backup Tunnels:**

Op	Tunnel ID	Head	Dest	T#	BW	Path	Protection Type	Report
ADD	ISC-B61	isctmp5	isctmp2		800	Computed Path	Protection	
ADD	ISC-B62	isctmp2	isctmp9		736	isctmp2->isctmp9-2	Protection	
ADD	ISC-B66	isctmp3	isctmp9		736	isctmp3->isctmp9-1	Protection	
ADD	ISC-B65	isctmp9	isctmp5		5000	Computed Path	Protection	
ADD	ISC-B63	isctmp2	isctmp5		2800	isctmp2->isctmp5-2	Protection	
ADD	ISC-B60	isctmp5	isctmp9		736	Computed Path	Protection	
ADD	ISC-B64	isctmp9	isctmp2		5000	isctmp9->isctmp2-2	Protection	
ADD	ISC-B67	isctmp3	isctmp2		2200	isctmp3->isctmp2-1	Protection	
ADD	ISC-B68	isctmp3	isctmp5		2200	isctmp3->isctmp5-1	Protection	
DELETE	ISC-B33	isctmp5	isctmp4	2	10	isctmp5->isctmp4-1	Side-effect	
DELETE	ISC-B28	isctmp2	isctmp1	1	100	isctmp2->isctmp1-1	Activating	
DELETE	ISC-B29	isctmp2	isctmp3	2	45	isctmp2->isctmp3-1	Activating	
DELETE	ISC-B39	isctmp9	isctmp8	3	10	isctmp9->isctmp8-2	Activating	

The columns in the tunnel list provide the following information:

- **Op**—SR operation on the tunnel. This can be either of the following:
  - **ADD**—Indicates a new tunnel calculated by the computation.
  - **DELETE**—Signifies that the computation found an existing backup tunnel that do not provide adequate protection on the element and, therefore, should be deleted.
  - <blank>—An existing backup tunnel is providing sufficient protection.
- **Tunnel ID**—Unique tunnel identifier used within ISC TEM.
- **Head**—Hostname of the head router.
- **Dest**—Hostname of the destination router.
- **T#**—Tunnel number on the head router.
- **BW**—move affected tunnels. the tunnel reserves on the links that it passes through.
- **Path**—Tunnel path in the form of either a computed path or an existing path . Click to view the path.

- **Protection Type**—Protection side-effect from activating the tunnel. There are three protection types:
  - **Protection tunnels**—Tunnels that can be activated to provide protection for a specified element.
  - **Side-effect tunnels**—Tunnels that are activated to protect a neighboring element, but which are also activated when a specified element fails.
  - **Activated tunnels**—Tunnels that are activated when a specified element fails, and which may or may not provide protection for the specified element or its neighbors.
- **Report**—If it says **yes** in the **Report** field, the tunnel is associated with the selected violation/warning. A blank field indicates that no report was generated.

The following actions can be performed (buttons):

- **Accept Solution**—Accept the proposed element protection solution and place the backup tunnels in the TE Protection SR window for further action.
- **Cancel**—Discard the proposed element protection solution and return to the TE Protection Management window.
- **Find**—You can search for particular elements by selecting the element type in the drop-down menu **Show** and specifying matching criteria in the **with name matching** field.

## Audit Protection

This section describes the Audit Protection GUI.

For instructions on how to run Audit Protection on all or selected elements, see [Configure Element Protection, page 7-5](#).

To run Audit Protection, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Protected Elements**. The TE Protection Management window in [Figure A-40](#) appears.

In the TE Protection Management window, select one or more elements for which you want ISC TEM to perform an Audit Protection computation.

Click **Audit Protection** and select one of the following:

- All Elements
- Selected Elements

ISC TEM reports **FRR Audit Protection in progress** and the same computation result window as for Compute Backup in [Figure A-43](#) appears.

The GUI for the rest of the process is identical to that described for [Compute Backup, page A-37](#).

## Assign TE Resources

To access the TE Resource Management part of the TEM GUI, click **Assign TE Resources** in the Traffic Engineering Management Services window (see [Figure A-1](#)).

The graphical user interface for **Assign TE Resources** is identical to that of **TE Links**. For an explanation of the GUI elements of this window, see [TE Links, page A-21](#).

The process of assigning TE resources is explained in [Chapter 4, “TE Resource Management.”](#)

# Create Managed TE Tunnel

In this section, the GUI used to create managed traffic engineering tunnels is explained. For step-by-step instructions on how to create a managed TE tunnel, see [Chapter 5, “Basic Tunnel Management.”](#)

To access the Create Managed TE Tunnel window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Create Managed TE Tunnel**.

The TE Managed Primary Tunnels SR window in [Figure A-45](#) appears.

**Figure A-45** TE Managed Primary Tunnels SR

The screenshot shows the Cisco IP Solution Center interface. The main window is titled "TE Managed Primary Tunnels SR". It includes a sidebar with a "Selection" menu containing options like Service Requests, Traffic Engineering Management, Inventory Manager, Topology Tool, Devices, Device Groups, Customers, Customer Sites, CPE Devices, Providers, Provider Regions, PE Devices, Access Domains, Resource Pools, CE Routing Communities, VPNs, AAA Servers, Named Physical Circuits, and NPC Rings. The main content area displays a table of tunnels. The table has columns: #, Op, Tunnel ID, T#, Head, Dest, Policy, BW, AutoBW, Deploy Status, Verified, and Allow Reroute. The table shows 5 records of tunnels. Below the table, there are controls for rows per page (set to 5) and a "Go to page" field (set to 1 of 5). At the bottom, there are buttons for "Close", "Display", "Details", "Admit", "Create", "Edit", "Delete", "Import", "Placement Tools", "Proceed with Changes >>", "Save & Deploy", and "Cancel".

#	Op	Tunnel ID	T#	Head	Dest	Policy	BW	AutoBW	Deploy Status	Verified	Allow Reroute
1.	<input type="checkbox"/>	ISC-P1	2	isctmp11	isctmp10	ISC-P1-isctmp11:tunnel-te2	2	false	DEPLOYED	succeed	false
2.	<input type="checkbox"/>	ISC-P2	1000	isctmp11	isctmp1	ISC-P2-isctmp11:tunnel-te1000	200	false	DEPLOYED	succeed	false
3.	<input type="checkbox"/>	ISC-P122	1003	isctmp11	isctmp12	ISC-P122-isctmp11:tunnel-te1003	500	false	DEPLOYED	succeed	false
4.	<input type="checkbox"/>	ISC-P123	1004	isctmp11	isctmp8	ISC-P122-isctmp11:tunnel-te1003	500	false	DEPLOYED	succeed	false
5.	<input type="checkbox"/>	ISC-P3	1	isctmp10	isctmp6	ISC-P2-isctmp11:tunnel-te1000	1000	false	DEPLOYED	succeed	false

The TE Managed Primary Tunnels SR window contains the following elements:

The columns in the tunnel list provides the following information:

- **Op**—SR operation on the tunnel. This can be one of the following:
  - **ADD**—Indicates a newly added tunnel.
  - **MODIFY**—Indicates a modified existing tunnel.
  - **DELETE**—Indicates an existing tunnel to be deleted.
  - **ADMIT**—Indicates an existing tunnel to be admitted by tunnel computation.
- **Tunnel ID**—Unique tunnel identifier used within ISC TEM.
- **T#**—Tunnel number on the head router.

- **Head**—Hostname of the head router.
- **Dest**—Hostname of the destination router.
- **Policy**—TE policy for the tunnel.
- **BW**—The tunnel bandwidth. If the tunnel is auto-bw enabled, BW shows the higher of tunnel bandwidth and maximum automatic bandwidth.
- **AutoBW**—Auto Bandwidth enabled if **true**, otherwise **false**.
- **Deploy Status**—Tunnel deployment status.
- **Verified**—Indicates whether tunnel verification was successful (**succeed**, **failed**, or **unknown**).
- **Allow Reroute**—Specifies whether reroute is allowed (**true** or **false**). If reroute is not allowed, the tunnel cannot be set to movable, and hence cannot be rerouted by the operation (placement, grooming, or repair).

The following actions can be performed (buttons):

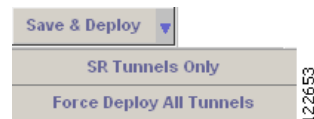
- **Close**—Close the Topology Display applet if open.
- **Display**—Open a Topology Display for the network and highlight the selected primary tunnel(s). Selected tunnels are marked in color with directional arrows.
- **Details**—Open the TE Tunnel Details window, which provides type, status, LSP, and other information about the tunnel.
- **Admit**—Admit selected tunnels not previously verified into the managed topology. This feature is used only for discovered tunnels that failed verification or for migrating unmanaged tunnels.
- **Create**—Create a managed primary tunnel.
- **Edit**—Edit a selected primary tunnel.
- **Delete**—Delete selected primary tunnels.
- **Import**—Import tunnel data from import XML file.
- **Placement Tools**—These tools are available only when no change has been made to the tunnels. Apply the following functions against the current topology and tunnels:
  - **Groom**—Analyse the managed tunnels in the network and reroute them to reduce the maximum link utilisation.
  - **Tunnel Audit**—Determine if changes to previously made SRLGs or backup tunnels have caused constraint violations in managed tunnels (this can occur when managed tunnels have FRR protection constraints).
  - **Tunnel Repair**—Repair any managed tunnel constraint violations revealed by Placement Tools > Tunnel Audit.

The Placement Tools GUI is described in [Planning Tools, page A-52](#).

- **Proceed with Changes >>**—For verifying changes in tunnels. When tunnels have been created, deleted, admitted, or their attributes altered, you can proceed with one of the following placement tools:
  - **Tunnel Audit**—Checks what constraint violations modifications to tunnels might cause.
  - **Tunnel Placement**—Admit new tunnels and modify tunnels already admitted into the network.
  - **Tunnel Repair**—Resolve inconsistencies caused by changes to bandwidth requirements or delay parameters of existing tunnels by moving as few existing tunnels as possible to accommodate the changes.

- **Save & Deploy** (Figure A-46)—For committing tunnel changes that do not impact tunnel placement. There are two options for saving and deploying SR tunnels to the network:
  - **SR Tunnels Only**—Deploy all tunnel changes that does not impact tunnel placement, or if no changes were made to the SR, use this to re-deploy the SR that was in **Requested** or **Invalid** state.
  - **Force Deploy All Tunnels**—Force deployment of all tunnels in this SR. This could be useful when previous provisioning of the SR has failed, so that it is necessary to force through the deployment of all tunnels in the SR.

Figure A-46 Save & Deploy Tunnels



- **Cancel**—Cancel the operation and return to the Traffic Engineering Management Services window.
- The tunnel SR search tool allows you to look for particular tunnels by selecting tunnel characteristics in the drop-down menu **tunnels with** and specify matching criteria in the **Matching** field:
- **Show:**
    - **Existing**—Show existing tunnels already deployed in the TE network.
    - **SR**—Show tunnels not yet deployed in the TE network.
  - **Tunnels with:**
    - **All**—Show all managed tunnels under the current provider.
    - **Tunnel Number**—Tunnel number on the head router.
    - **Head Device**—Full or partial name of the tunnel head device.
    - **Destination Device**—Full or partial host name of the tail device of the tunnel.
    - **Head, Dest Devices**—Exact host name of the head and tail devices of the tunnel.
    - **Deploy Status**—Tunnel deployment status.
    - **Policy Name**—Name of the TE policy.
  - **Matching/Equal**—Specify matching criteria for your search. Wildcards are accepted. **Matching** changes to **Equal** if **Head, Dest Device** is selected in the drop-down menu. For **Equal**, the exact host name of the head or tail device must be entered (wildcards not accepted).
  - **Find**—Click the **Find** button when the search criteria has been entered.

## View Managed Primary Tunnel Details

This section describes the elements in the TE Managed Primary Tunnel Details window.

To view the details of a TE managed primary tunnel, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management. > Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window in Figure A-45 appears.

To view the details of a particular managed primary tunnel, select the desired tunnel by first clicking the corresponding check box and then clicking the **Details** button. When clicking **Details**, the TE Tunnel Details window in Figure A-47 appears.

Figure A-47 TE Tunnel Details

TE Tunnel Details	
Type:	Managed TE Tunnel
Tunnel:	isctmp7:Tunnel152 (ISC-P1) isctmp7 <-> isctmp8 BW: 10 kbps
Status:	Op: up, Admin: up
State:	DEPLOYED, Conformed
LSP configured:	10.2.3.50
LSP in use:	10.2.3.50 <-> 192.168.118.183
AutoBW:	Disabled
OK	

122714

The TE Tunnel Details window contains the following elements:

- **Type**—Managed or unmanaged.
- **Tunnel**—Tunnel name, head and destination routers, and total bandwidth.
- **Status**—The operational and administrative status of the TE tunnels as of the latest **TE Discovery** task.
- **State**—Indicates whether the tunnel state is DEPLOYED or NOT DEPLOYED and whether it is Conformed or Not Conformed.
- **LSP configured**—The LSP that the tunnel is configured to use as its lowest path option.
- **LSP in use**—Actual LSP in the network as of the latest **TE Discovery** task.
- **AutoBW**—Auto Bandwidth **Enabled** or **Disabled**.

## Create TE Managed Primary Tunnel

This section describes the GUI elements in the Create TE Managed Primary Tunnel SR and Edit TE Managed Primary Tunnel windows. The create feature is here used as an example.

To create a TE Managed Primary Tunnel SR, see [Chapter 5, “Basic Tunnel Management.”](#)

To access the Create TE Managed Primary Tunnel SR window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window appears. Click **Create**, to open the Create TE Managed Primary Tunnel window as shown [Figure A-48](#).

Figure A-48 Create TE Managed Primary Tunnel

**Create TE Managed Primary Tunnel**

<b>SR Job ID:</b> New	<b>SR ID:</b> New	<b>SR State:</b> REQUESTED
<b>Tunnel ID:</b>	<b>Creator:</b>	<b>Type:</b> ADD

Head Device \* :

Destination Device \* :

Tunnel Policy \* :

Tunnel Bandwidth (Kbps):

Tunnel Number:  Auto Gen ☒

Customer:

Auto BW:

Enable: ☐

Freq (sec):

Min (Kbps):

Max (Kbps):

**Path Options:**

Showing 1 - 2 of 2 records

<input type="checkbox"/>	Option #	Path Name	Path Type	Lock Down
<input type="checkbox"/>	1	System Path	Explicit	<input type="checkbox"/>
<input type="checkbox"/>	2	Dynamic Path	Dynamic	<input type="checkbox"/>

Rows per page: 5

Note: \* - Required Field

The Create TE Managed Primary Tunnel window contains the following elements:

- **Head Device**—Head device for the tunnel.
- **Destination Device**—Destination device for the tunnel.
- **Tunnel Policy**—A set of rules established for a tunnel.
- **Tunnel Bandwidth**—Total allocated bandwidth of the tunnel.
- **Tunnel Number**—Tunnel number corresponding to the tunnel interface name.
  - **Auto Gen**—Check this box to generate the tunnel number automatically. Otherwise, enter a desired number.



**Note** If a manually entered tunnel number is too low, it could prevent deployment.

**Note**

MPLS-TE tunnels can potentially interfere with multicast GRE tunnels. ISC TEM creates new tunnels using auto-gen and this tunnel number might already be used by an MDT GRE tunnel. As a result, ISC TEM uses high tunnel numbers to avoid any complications.

- **Customer**—Selected customer for the tunnel.
- **Auto BW**—A way to configure a tunnel for automatic bandwidth adjustment and to control the manner in which the bandwidth for a tunnel is adjusted.
  - **Enable**—Check this box to enable automatic bandwidth.
  - **Freq**—Interval between bandwidth adjustments.
  - **Min**—Minimum automatic bandwidth, in kbps, for this tunnel.
  - **Max**—Maximum automatic bandwidth, in kbps, for this tunnel.

Path options:

- **Option #**—Sequential number of available explicit paths.
- **Path Name**—Name of the explicit path. In case of an existing path, the name is a URL that links to the Explicit Path Viewer (see [Figure 5-16](#)).
  - **System Path**—ISC system generated explicit path. For managed tunnels, the first path has to be an explicit path. If a tunnel contains a system path, the planning function will generate an optimal path for the tunnel.
  - **Dynamic Path**—A dynamic path is provisioned by allowing the head router to find a path. The **dynamic** keyword is provisioned to the routers.
- **Path Type**—Path option type, Explicit or Dynamic.
- **Lock Down**—Disables reoptimization check on the tunnel, if checked, meaning the path cannot be changed.

The following actions can be performed:

- **Add**—Add a path option. This opens the Select TE Explicit Path window in [Figure A-52](#).
- **Delete**—Delete a path option.
- **OK**—Accept all changes and return to the TE Managed Primary Tunnels SR window.
- **Cancel**—Cancel the operation and return to the TE Managed Primary Tunnels SR window.

## Select Devices and Policy

To select a **Head Device** in the Create TE Managed Primary Tunnel window ([Figure A-48](#)), click the corresponding **Select** button to open the Select Device for TE Head Router window shown in [Figure A-49](#).



**Figure A-49**      *Select Device for TE Head Router*

Device for **TE Head Router**

Show Devices with:  matching

Showing 1 - 5 of 14 records

#	Device Name	IGP ID	MPLS TE ID	Admin Status
1.	<input type="radio"/> isctmp1	192.168.118.176	192.168.118.176	UP
2.	<input type="radio"/> isctmp11	192.168.118.166	192.168.118.166	UP
3.	<input type="radio"/> isctmp10	192.168.118.167	192.168.118.167	UP
4.	<input type="radio"/> isctmp12	192.168.118.168	192.168.118.168	UP
5.	<input type="radio"/> isctmp13	192.168.118.171	192.168.118.171	UP

Rows per page:  Go to page:  of 3

The Select Device for TE Head Router window contains the following elements:

- **Device Name**—Hostname for the device.
- **IGP ID**—Interior Gateway Protocol (IGP) ID.
- **MPLS TE ID**—TE ID assigned by the router.
- **Admin Status**—Indicates whether the router is **UP** or **DOWN**.

The following actions can be performed:

- **Select**—Accept the selected device and return to the previous window.
- **Cancel**—Cancel the operation and return to the previous window.
- **Find**—You can search for particular devices by selecting the device type in the drop-down menu **Show Devices with** and specify matching criteria in the **Matching** field.

**Figure A-50**      *Select Device for TE Tail Router*

Device for **TE Tail Router**

Show Devices with:  matching

Showing 1 - 5 of 15 records

#	Device Name	IGP ID	MPLS TE ID	Admin Status
1.	<input type="radio"/> 192.168.118.178	192.168.118.178	192.168.118.178	UP
2.	<input type="radio"/> isctmp1	192.168.118.176	192.168.118.176	UP
3.	<input type="radio"/> isctmp11	192.168.118.166	192.168.118.166	UP
4.	<input type="radio"/> isctmp10	192.168.118.167	192.168.118.167	UP
5.	<input type="radio"/> isctmp12	192.168.118.168	192.168.118.168	UP

Rows per page:  Go to page:  of 3

For a description of the GUI elements in the Select Device for TE Tail Router window, see the explanation for the [Select Device for TE Head Router](#) window.

**Figure A-51** Select Managed TE Tunnel Policy

#	Policy Name	Pool Type	Setup Priority	Hold Priority	Affinity	Affinity Mask	Delayed Constraint	FRR Protection
1.	man1	GLOBAL	0	0	0x0	0xFFFF		None
2.	pm-none	GLOBAL	0	0	0x0	0xFFFF		None

The Select Managed TE Tunnel Policy window contains the following elements:

- **Policy Name**—Name of the TE policy.
- **Pool Type**—Tunnel bandwidth pool type for this policy. For a definition of pool types, see [Bandwidth Pools, page 1-5](#).
  - **SUB POOL**—Bandwidth will be reserved from Sub Pool.
  - **GLOBAL**—Bandwidth will be reserved from Global Pool.
- **Setup Priority**—Priority used when signaling an LSP for the tunnel to determine, which of the existing tunnels can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 hold priority.
- **Hold Priority**—Priority associated with an LSP for the tunnel to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.
- **Affinity**—Attribute values required for links carrying the tunnel (bit values are either 0 or 1).
- **Affinity Mask**—Attribute values to be checked. If a bit in the mask is 0, a link's attribute value of that bit is irrelevant. If a bit in the mask is 1, the link's attribute value and the tunnel's required affinity for that bit must match.
- **Delayed Constraint**—True or false value. If true, the tunnel has a maximum delay that its path must not exceed.
- **FRR Protection**—Used to enable an MPLS traffic engineering tunnel to use a backup tunnel in the event of a link failure if a backup tunnel exists.
  - **None**—No backup tunnel needed.
  - **Best Effort**—Use backup tunnel if available.
  - **Link and SRLG**—Specifies that primary tunnels should be routed only through links and SRLGs that are protected by FRR backup tunnels.
  - **Link, SRLG and Node**—Specifies that primary tunnels should be routed only through links, SRLGs and nodes that are protected by FRR backup tunnels.

## Select TE Explicit Path

An explicit path is added to a tunnel by clicking **Add** in the tunnel editor. The Select TE Explicit Path window in [Figure A-52](#) appears.

**Figure A-52**      *Select TE Explicit Path*

#	Path Name	Head	Dest
1.	Dynamic		

Showing 1 - 1 of 1 record

Rows per page: 10    Go to page: 1 of 1    Go

Select Cancel

122662

Two path types are available:

**Explicit Path**—A fixed path from a specific head to a specific destination device.

**Dynamic Path**—A path that is provisioned by allowing the head router to find the path. The **dynamic** IOS keyword is provisioned to the routers. This signifies that the router calculates a valid path.

## Explicit Path Viewer

When creating a primary tunnel, the **Path Options** list by default suggests a **System** path and a **Dynamic** path. If an explicit path is added, this link will be selectable as shown in the **Path Options** section of the create window in [Figure A-53](#). By clicking an explicit path link, a non-editable Explicit Path Viewer in [Figure A-54](#) appears.

**Figure A-53**      *Path Options*

<input type="checkbox"/>	Option #	Path Name	Path Type	Lock Down
<input type="checkbox"/>	1	isctmp1-isctmp8	Explicit	<input type="checkbox"/>
<input type="checkbox"/>	2	Dynamic Path	Dynamic	<input type="checkbox"/>

Showing 1 - 2 of 2 records

122648

For an explanation of the various GUI elements, see [Create Managed TE Tunnel, page A-41](#).

**Figure A-54** TE Explicit Path Viewer

Path Name \*: isctmp11-isctmp10-1

Head Router \*: isctmp11

Links:

Showing 1 - 2 of 2 records

#	Device	Outgoing Interface	Outgoing IP	Next Hop	Type	Incoming Interface	Incoming IP
1.	isctmp11	POS0/3/0/1	10.2.4.14	isctmp12	CISCO_ROUTER	POS0/1/0/1	10.2.4.13
2.	isctmp12	POS0/4/0/0	10.2.4.21	isctmp10	CISCO_ROUTER	POS0/2/0/0	10.2.4.22

Rows per page: 10 Go to page: 1 of 1 Go

Provision Preference \*: Outgoing Interface Incoming Interface

Close

Note: \* - Required Field

For an explanation of the various GUI elements, see [Create/Edit Explicit Path, page A-34](#).

## Import Tunnel

This section describes the GUI elements in the import tunnel feature.

For instructions on how to import TE tunnels, see the [Import Primary Tunnel, page 6-8](#).

The tunnel import function is found under **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Create Managed TE Tunnel**, which opens the TE Managed Primary Tunnels SR window (see [Figure A-62](#)).

When you click **Import** to start the import process, the Select Import File window in [Figure A-55](#) appears.



**Note** The Import button is only enabled when there are no uncommitted new, changed, or deleted tunnels in the service request.

**Figure A-55** Select Import File

Look in: /scratch/opt/isc-4.1/resources/java/xml/com/cisco/vpr Find Up

Showing 1 - 1 of 1 record

#	File Name	Size	Last Modified
1.	sample.xml	1004	October 18, 2005 2:18:33 PM PDT

Rows per page: 5 Go to page: 1 of 1 Go

Select Cancel

The Select Managed TE Tunnel Policy window contains the following elements:

- **File Name**—Name of XML file.

- **Size**—Size in kilobytes of XML file.
- **Last Modified**—Date and time when the file was last modified.

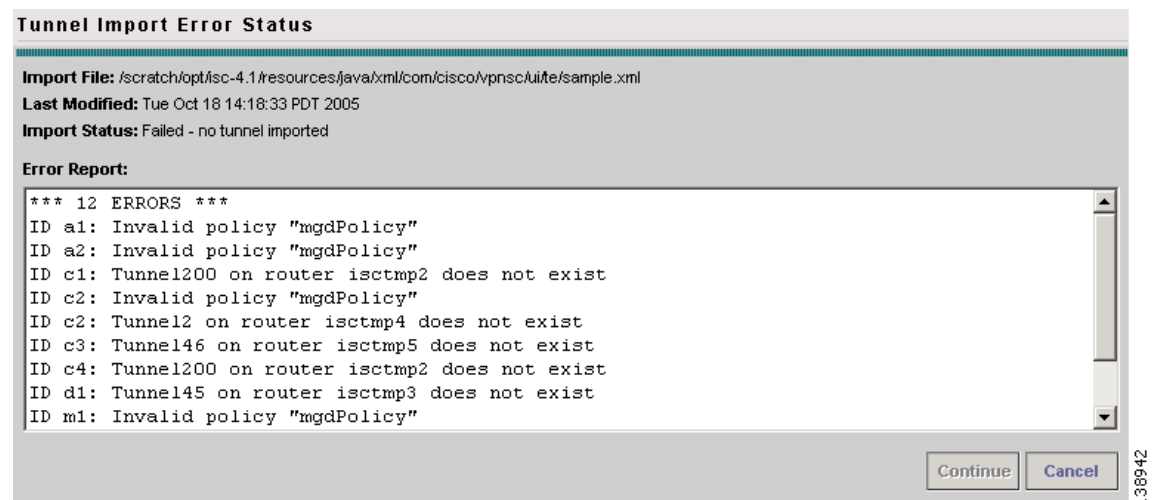
The following actions can be performed:

- **Select**—Accept the selected XML file(s) and start the tunnel import operation.
- **Cancel**—Cancel the tunnel import operation and return to the TE Managed Primary Tunnels SR window.
- **Find**—Specify the directory containing the XML import files and directories to import in the **Look in** field and click **Find**. This brings up the data import directory and the XML files contained are listed in the accompanying table.
- **Up**—Go to the parent directory.

### Import Error Status Window

When you click **Select** to start the import operation, the system parses the file, and if any error is detected, it will be reported in the Tunnel Import Error Status window shown in [Figure A-56](#).

**Figure A-56** Tunnel Import Error Status



The Tunnel Import Error Status window contains the following elements:

- **Import File**—Directory containing XML import files and directories.
- **Last Modified**—Date and time when the file was last modified.
- **Import Status**—There are two possible Import Status values:
  - **Failed**—Critical errors are present and the import process cannot continue.
  - **Partial Success**—There are either non-critical errors or warnings or both in the file. In this case the error tunnel is reported and skipped and the warning tunnel is processed with certain defaults applied. There is no “Success” status because when there are no errors or warnings, the Tunnel Import Error Status window will not appear.

The following actions can be performed:

- **Continue**—If the import operation is partially successful, click **Continue** to accept system treatment for errors/warnings and continue with the import operation.
- **Cancel**—Cancel import operation and return to the previous window.

## Edit TE SR (Primary or Backup)

The tunnels editor windows differ only very slightly from the create tunnel windows. All fields in the editor windows are found in the create windows for both primary managed, primary unmanaged, and backup tunnels (see [Chapter 5, “Basic Tunnel Management”](#)).

The only difference from the create window is that the head and destination device and tunnel number fields are not editable and the **Path Options** table lists existing path options on the tunnel rather than the default **System** and **Dynamic** paths.

## Planning Tools

This section describes the GUI elements in the sequence of windows used by the planning tools Tunnel Audit, Tunnel Placement, Tunnel Repair, and Grooming. Screenshots from Tunnel Repair has been used as an example but it covers the GUI elements for all four processes.

To use the planning tools, see [Placement Tools, page 6-11](#)

To access the Create TE Managed Primary Tunnel SR window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Create Managed TE Tunnel**. The TE Managed Primary Tunnels SR window in [Figure A-62](#) appears.

There are two ways to activate the planning tools:

- When one or more tunnels have been created or their attributes altered (see [Create Primary Tunnel, page 6-2](#)), Tunnel Audit, Tunnel Placement, and Tunnel Repair can be activated by selecting **Proceed with Changes >>**.
- When no changes have taken place, Grooming, Tunnel Audit, and Tunnel Repair can be accessed by selecting **Placement Tools**.

As an example, assume that we run Tunnel Repair on a set of tunnels as described in [Tunnel Repair, page 6-22](#).

## Movable Tunnel Selection Window

When selecting **Tunnel Repair** from the **Placement Tools** button, the Movable Tunnel Selection window in [Figure A-57](#) appears.

Figure A-57 Movable Tunnel Selection

**Movable Tunnel Selection**

<b>Computation Type</b>	Tunnel Repair							
<b>Maximum computation duration (Timeout in sec)</b> *	100							
<b>Maximum number of tunnel moves</b>								
Number of reroutable tunnels selected as movable: 4 of 4    Non-reroutable tunnels: 2								
Show tunnels with <input type="text" value="All"/> matching * <input type="text" value=""/> <input type="button" value="Find"/>								
Showing 1-6 of 6 records								
#	<input type="checkbox"/> Movable	Allow Reroute	Tunnel ID	T#	Head	Dest	Policy	BW
1.	<input type="checkbox"/> yes	true	ISC-P66	3	isctmp1	isctmp2	ISC-P1-isctmp8:Tunnel44444	3
2.	<input type="checkbox"/> NA	false	ISC-P1	44444	isctmp8	isctmp6	ISC-P1-isctmp8:Tunnel44444	103
3.	<input type="checkbox"/> NA	false	ISC-P2	44	isctmp2	isctmp3	ISC-P2-isctmp2:Tunnel44	0
4.	<input type="checkbox"/> yes	true	ISC-P132	3	isctmp2	isctmp8	ISC-P2-isctmp2:Tunnel44	120
5.	<input type="checkbox"/> yes	true	ISC-P138	2	isctmp6	isctmp7	ISC-P2-isctmp2:Tunnel44	100
6.	<input type="checkbox"/> yes	true	ISC-P35	2	isctmp4	isctmp6	ISC-P2-isctmp2:Tunnel44	100
Rows per page: <input type="text" value="10"/>		Go to page: <input type="text" value="1"/> of 1 <input type="button" value="Go"/>						
<input type="button" value="Set Movable"/>		<input type="button" value="Set Unmovable"/>						
<input type="button" value="Back"/>		<input type="button" value="Proceed"/>						
<input type="button" value="Cancel"/>								

Note: \* - Required Field

122642

The Movable Tunnel Selection window contains the following elements:

- **Computation Type**—Indicates which tool is used for the computation (Placement, Repair, Grooming).
- **Maximum computation duration**—The maximum amount of time allowed for the computation before timeout occurs.
- **Maximum number of tunnel moves**—The maximum number of tunnels that can be moved during Tunnel Repair.
- **Number of reroutable tunnels selected as movable**—Indicates how many reroutable tunnels among the ones shown in the tunnel list are movable.
- **Non-reroutable**—Indicates how many tunnels among the ones shown in the tunnel list are not movable. This is set in the tunnel editor.
- **Find**—You can search for particular tunnels by selecting the search variable in the drop-down menu **Show tunnels with**, specifying matching criteria, and clicking **Find**.

**Show tunnels with** options:

- **All**—Show all managed tunnels under the current provider.
- **Tunnel Number**—Tunnel number on the head router.
- **Head Device**—Full or partial name of the tunnel head device.
- **Destination Device**—Full or partial host name of the tail device of the tunnel.
- **Head, Dest Devices**—Exact host name of the head and tail devices of the tunnel.

- **Deploy Status**—Tunnel deployment status.
- **Policy Name**—Name of the TE policy.

**matching/equal**—Specify matching criteria for your search. Wildcards are accepted. **matching** changes to **equal** if **Head, Dest Device** is selected in the drop-down menu. For **equal**, the exact host name of the head or tail device must be entered (wildcards not accepted).

- **Movable**—Indicates whether the tunnel is movable (**yes**, **no** or **NA**). This setting can be toggled by clicking **Set Movable** and **Set Unmovable**.
- **Allow Reroute**—Specifies whether reroute is allowed (**true** or **false**). If reroute is not allowed, the tunnel cannot be set to movable.
- **Tunnel ID**—Unique tunnel identifier used within ISC TEM.
- **T#**—Tunnel number on the head router.
- **Head**—Hostname of the head router.
- **Dest**—Hostname of the destination router.
- **Policy**—TE policy for the tunnel.
- **BW**—The tunnel bandwidth. If the tunnel is auto-bw enabled, BW shows the higher of tunnel bandwidth and maximum automatic bandwidth.

The following actions can be performed:

- **Set Movable**—Set selected tunnel to movable.
- **Set Unmovable**—Set selected tunnel to unmovable.
- **<< Back**—Return to the previous window.
- **Proceed >>**—Proceed to computation.
- **Cancel**—Cancel the operation and return to the previous window.

## TE Primary Tunnel Computation SR - Changes Window

Still using **Tunnel Repair** as an example, after selecting **Proceed >>** from the Movable Tunnel Selection window, the TE Primary Tunnel Computation Results - Changes window in [Figure A-58](#) appears.

The figure shows the computation results window after clicking **Detail** to obtain detailed information about the tunnel and view the status of the change request.



Figure A-58 TE Primary Tunnel Computation Results - Tunnel Repair Changes (Details)

**TE Primary Tunnel Computation Results - Changes**

**Computation Status:** CONSTRAINT\_VIOLATIONS\_REPORTED-NO\_SOLUTION\_EXISTS  
**Tunnels - unplaced:** 0 of 9 **moved:** 0  
**Bandwidth - unplaced:** 49100 of 56490

Global Util.		Sub Pool Util.	
<b>Solution</b>	max. 75.0% max.mod. 12.5%	max. 90.0%	max.mod. 70.0%
<b>Original</b>	max. 75.0% max.mod. 12.5%	max. 90.0%	max.mod. 70.0%

**Changes:** 0 achieved of 1  
 Showing 1 - 1 of 1 record

#	Achieved	Origin	Type	Object ID
1.	<input checked="" type="checkbox"/> no	User	Tunnel Modify Change	ISC-P8284

Rows per page: 10 Go to page: 1 of 1 **Go**

**Change Type:** Tunnel Modify Change  
**Achieved:** no  
**Description:** Request to modify one or more attributes of an existing tunnel

**Requested Tunnel**  
**ID:** isctmp9:Tunnel3  
**Head:** isctmp9  
**Tail:** isctmp1  
**Policy:** ISC-P8262-isctmp1:Tunnel4  
**Bandwidth:** 50000  
**Path:** isctmp9->isctmp1-2

Changed Attributes	New Value	Achieved
BW	50000	no

**Close Display Details**

**<< Back View Report >> Save & Deploy Cancel**

The TE Primary Tunnel Computation Results - Changes window contains the following elements:

Status section (top):

- **Computation Status**—Indicates whether the computation succeeded or failed.
- **Tunnels:**
  - **unplaced**—Number of unplaced tunnels out of the total.
  - **moved**—Number of tunnels that were moved.
- **Bandwidth - unplaced**—Amount of tunnel bandwidth that was not placed out of the total bandwidth of all existing and new tunnels.
- **Global Util.**—Global Pool bandwidth utilization percentage. For a description of the various utilization values, see [TE Primary Tunnel Computation Results - Report, page A-57](#) under the quality report.
- **Sub Pool Util.**—Sub Pool bandwidth utilization percentage. For a description of the various utilization values, see [TE Primary Tunnel Computation Results - Report, page A-57](#) under the quality report.
- **Solution**—Utilization for the generated solution.
- **Original**—Utilizations for the original placement.

Changes section (left):

- **Changes**—Number of changes achieved out of the total number of changes.
  - **Achieved**—Indicates whether a specific change is successful (**Yes** or **No**).
  - **Origin**—The originator of the change. Can be **user** (change by user) or **compute** (from a computation, e.g. rerouting of a tunnel).
  - **Type**—The type of change requested: **Tunnel Add Change**, **Tunnel Modify Change**, **Tunnel Remove Change**, or **Element Modify Change**.
  - **Object ID**—A tunnel or link ID.

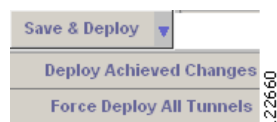
Information section (right):

- **Change Type**—The type of change requested: **Tunnel Add Change**, **Tunnel Modify Change**, **Tunnel Remove Change**, or **Element Modify Change**.
- **Achieved**—Indicates whether a specific change is successful (**Yes** or **No**).
- **Description**—Description of the computation attempt.
- **ID**—Tunnel ID.
- **Head**—Hostname of the head router.
- **Tail**—Hostname of the destination router.
- **Policy**—TE policy for the tunnel.
- **Bandwidth**—Bandwidth used in computation.
- **Path**—Tunnel path in the form of either a computed path or an existing path . Click to view the path.
- Changed attribute table:
  - **Changed Attributes**—Lists the tunnel attributes that have changed.
  - **New Value**—New value of the attribute.
  - **Achieved**—Indicates whether a specific change is successful (**Yes** or **No**).

The following actions can be performed:

- **Close**—Close the Topology Display applet if open.
- **Display**—Invoke the Topology Display to view selected links and/or tunnels in the network. Selected links/tunnels are displayed with a unique color.
- **Detail**—Open the detail panel in the right side of the Computation Result window to see the tunnel/link information.
- **<< Back**—Return to the previous window.
- **View Report >>**—View a list of generated reports. The Report window appears (see [Figure A-60](#)).
- **Save & Deploy** ([Figure A-59](#))—For committing all user originated and system computed changes. There are two options for saving and deploying tunnel SRs to the network:
  - **Deploy Achieved Changes**—Place all achieved changes in the deployment queue.
  - **Force Deploy All Tunnels**—Force deployment of all elements in the SR. This could be useful when previous provisioning of the SR has failed, so that it is necessary to force through the deployment of all tunnels in the SR.

**Figure A-59 Save & Deploy**



- **Cancel**—Cancel the operation and return to either the Links List, TE Managed Primary Tunnels SR, or the TE Resource Management SR window depending on the originating flow.

## TE Primary Tunnel Computation Results - Report

To view the computation reports, click **View Report >>**. The TE Primary Tunnel Computation Results - Report window in [Figure A-60](#) appears.

In this case, there is both a quality report and a violation report. In that case, a detail report such as the violation report in [Figure A-61](#) will appear. Warning and violation reports have different fields and they are all described in [Appendix C, “Warnings and Violations.”](#)

Select the desired report and click the **Detail** button

**Figure A-60** TE Managed Primary Tunnels SR - Tunnel Repair Report (Details)

**TE Primary Tunnel Computation Results - Report**

**Computation Status:** CONSTRAINT\_VIOLATIONS\_REPORTED-NO\_SOLUTION\_EXISTS  
**Tunnels -** unplaced 0 of 9 **moved:** 0  
**Bandwidth -** unplaced 49100 of 56490

**Report:** Showing 1 - 2 of 2 records

#	Report Type	Summary Info
1.	<input checked="" type="checkbox"/> qualityReport	
2.	<input type="checkbox"/> violationLinkPoolOversubscribed isctmp9/FastEthernet2/1,GLOBAL_POOL	

Rows per page: 10 Go to page: 1 of 1

**Details**

**Report Type:** qualityReport  
**Description:** relates to only 0 priority tunnels  
**Achievement:** CONSTRAINT\_VIOLATIONS\_REPORTED  
**Termination:** COMPLETED  
**Solution:** NO\_SOLUTION\_EXISTS  
**Optimality:** NO\_OPTIMALITY\_PROOF

**Tunnel Placement:**

	%Placed	Placed	Unplaced	Total
<b>Tunnels -Solution</b>	100.0	9	0	9
<b>original</b>	100.0	9	0	9
<b>Bandwidth -Solution</b>	0.0	7390	49100	56490
<b>original</b>	100.0	7390	0	7390

**Tunnels moved** 0

**TE-Metric Sum(Primary Tunnel Paths)**

	-Solution
<b>original</b>	113

**Utilization:**

	%Median	%Mean	%Max.	%Max. Modifiable
<b>Global Pool -solution</b>	0.0	3.47	75.0	12.5
<b>original</b>	0.0	3.47	75.0	12.5
<b>Sub Pool -solution</b>	0.0	10.48	90.0	70.0
<b>original</b>	0.0	10.48	90.0	70.0

**<< View Result**

The TE Primary Tunnel Computation Results - Report window contains the following elements:

Status section (top): described above ([Figure A-58](#)).

Report section (left):

- **Report Type**—There are three basic report types: a **qualityReport** (generated every time), warning reports, and violation reports.
- **Summary Info**—Summary information about the findings of the report.

Information section (right):

- **Report Type**—See description above.
- **Description**—Specific information about the report.

- **Achievement**—Success or failure of the computation attempt/solution (**SUCCESS** or **CONSTRAINT\_VIOLATIONS\_REPORTED**).
- **Solution**—Indicates whether a solution was found (**SOLUTION\_FOUND**, **PARTIAL\_SOLUTION\_FOUND** or **NO\_SOLUTION\_FOUND**).
- **Termination**—Indicates whether the computation was completed:
  - **COMPLETED**—The computation completed processing before the time limit.
  - **TIMED\_OUT**—The computation was not able to complete processing within the time limit. The solution presented is the best solution it was able to find in the time available.
- **Optimality**—Indicates whether the computation was optimal:
  - **OPTIMAL\_FOR\_ALL\_CRITERIA**—The solution generated has proven to be the best for all optimization criteria.
  - **NO\_OPTIMALITY\_PROOF**—The solution's optimality is unknown.
  - **OPTIMAL\_FOR\_DEMAND\_SELECTION**—The solution generated has proven to be the best in terms of total bandwidth placed, but utilization optimality is unknown.
  - **OPTIMAL\_FOR\_SUB\_POOL\_PATH\_SELECTION**—The solution generated has proven to be the best in terms of total bandwidth placed and maximum sub pool utilization, but has not proven to be optimal in terms of global pool utilization.

Tables:

- **Tunnel Placement**—Tables that compares various tunnel placement attributes of the original configuration with the solution configuration.
  - **Tunnels**: Attributes of the original and computed tunnels.
  - **Bandwidth**: Attributes of the tunnel bandwidth.
  - **%Placed**—Percentage of tunnels that were successfully placed.
  - **Placed**—Number of tunnels that were successfully placed.
  - **Unplaced**—Number of tunnels that were not placed.
  - **Total**—Total number of tunnels.
  - **Tunnels moved**—Number of tunnels moved from their original paths.
  - **TE-Metric Sum (Primary Tunnel Paths)**—TE metric sum for the computed and the original paths.
- **Utilization**—The table compares utilization measurements of the original configuration with the solution configuration
  - **Global Pool**—Comparison data for various Global Pool attributes.
  - **Sub Pool**—Comparison data for various Sub Pool attributes.
  - **Median**—Utilization of the link that is the middle link when all links are ordered by utilization.
  - **Max. Modifiable**—Utilization value for the most utilized link that has movable tunnels passing through it.
  - **Mean**—Average link utilization for the network as a whole.
  - **Max.**—Utilization value for the most utilized link in the topology.

The following actions can be performed:

Changes actions (buttons, left):

- **Detail**—When a report is selected, the **Detail** button displays the contents of the report, which can contain warnings or violations, in the right window pane.



**Note** For a description of possible warnings and violations in ISC TEM, see [Appendix C, “Warnings and Violations.”](#)

- << **View Result**—Return to the Changes window.

**Figure A-61** TE Managed Primary Tunnels SR - Violation Report (Details)

**TE Primary Tunnel Computation Results - Report**

Computation Status: CONSTRAINT\_VIOLATIONS\_REPORTED-NO\_SOLUTION\_EXISTS  
Tunnels - unplaced 0 of 9 moved: 0  
Bandwidth - unplaced 49100 of 56490

		Global Util.		Sub Pool Util.	
Solution	max. 75.0%	max.mod. 12.5%	max. 90.0%	max.mod. 70.0%	
Original	max. 75.0%	max.mod. 12.5%	max. 90.0%	max.mod. 70.0%	

**Report:** Showing 1 - 2 of 2 records

#	Report Type	Summary Info
1.	<input type="checkbox"/> qualityReport	
2.	<input checked="" type="checkbox"/> violationLinkPoolOversubscribed	isctmp9/FastEthernet2/1, GLOBAL_POOL

Rows per page: 10 Go to page: 1 of 1 Go

**Report Type:** violationLinkPoolOversubscribed  
**Description:** The specified bandwidth pool for a directed link is over-subscribed by Primary Tunnels that pass through it  
**Directed Link:**  
**Head Device/Interface:** isctmp9/10.2.3.58  
**Tail Device/Interface:** isctmp1/10.2.3.57  
**Pool:** GLOBAL\_POOL  
**Pool Bandwidth:** 20000  
**Primary Tunnel:**

Name	Head Device	Tail Device	Bandwidth	Pool	Path
isctmp9:Tunnel3	isctmp9	isctmp1	50000	GLOBAL	isctmp9->isctmp1-2

<< View Result

In [Figure A-61](#), the top status section and the left Report section contain the same fields as in [Figure A-60](#).

## Create Unmanaged TE Tunnel

The only two differences between the managed and the unmanaged tunnel GUIs is that the path option table does not automatically populate the two System/Dynamic paths and that the **Conformance** status is only indicated for unmanaged primary tunnels (for an explanation of the conformance concept, see [Conformant/Non-Conformant Tunnels, page 1-4](#)).

For a description of the rest of the GUI, see [Create Managed TE Tunnel, page A-41](#).

## Create TE Backup Tunnel

To access the TE Protection SR window for managing backup tunnels, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > Create TE Backup Tunnel**. The TE Protection SR window in [Figure A-62](#) appears.

Figure A-62 TE Protection SR

**TE Protection SR**

SR Job ID: 9      Provider: Provider2      SR State: REQUESTED  
 SR ID: New      Creator:      Type: ADD

Description:

Show  Tunnels with  matching

Showing 1 - 5 of 47 records

#	Op	Tunnel ID	T#	Head	Dest	BW Quota	Deploy Status	Conformance
1.	<input type="checkbox"/>	ISC-B30	3	isctmp11	isctmp12	2	LOST	Yes
2.	<input type="checkbox"/>	ISC-B31	1001	isctmp11	isctmp8	30000	LOST	Yes
3.	<input type="checkbox"/>	ISC-B141	1002	isctmp11	isctmp8	30000	DEPLOYED	Yes
4.	<input type="checkbox"/>	ISC-B142	1005	isctmp11	isctmp12	1000	DEPLOYED	No
5.	<input type="checkbox"/>	ISC-B143	1000	isctmp12	isctmp5	1000	DEPLOYED	No

Rows per page:       Go to page:  of 10

The TE Protection SR window contains the following elements:

The columns in the tunnel list provides the following information:

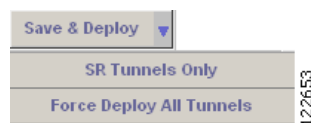
- **Op**—Current SR operation on the tunnel. This can be one of the following:
  - **ADD**—Indicates a newly added tunnel, either calculated by the system or entered by the user.
  - **MODIFY**—Indicates a modified existing tunnel.
  - **DELETE**—Indicates an existing tunnel to be deleted, either computed by the system or originated by the user.
- **Tunnel ID**—Unique tunnel identifier used within ISC TEM.
- **Head**—Hostname of the head router.
- **Dest**—Hostname of the destination router.
- **T#**—Tunnel number on the head router.
- **BW Quota**—move affected tunnels. this backup tunnel can protect. The router limits the LSPs that can use this backup tunnel so that the sum of the bandwidth of the LSPs does not exceed the specified amount of bandwidth. If there are multiple backup tunnels, the router will use the best-fit algorithm.
- **Deploy Status**—Tunnel deployment status.
- **Conformance**—Indicates whether the tunnel is found to be conformant when running discovery. A tunnel is non-conformant if it has a non-zero bandwidth reservation and a zero hold or setup priority. If a tunnel is entered through ISC TEM, it is always conformant.

The following actions can be performed (buttons):

- **Close**—Close the Topology Display applet if open.

- **Display**—Open a Topology Display for the network and highlight the selected backup tunnel(s). The selected tunnel(s) is/are marked in color with directional arrows.
- **Details**—Open the TE Tunnel Details window, which provides type, status, LSP, and other information about the tunnel.
- **Create**—Create a backup tunnel.
- **Edit**—Edit the selected backup tunnel.
- **Delete**—Delete the selected backup tunnels.
- **Audit SR**—Audit protection of protected elements using all existing backup tunnels and proposed changes in the SR.
- **Save & Deploy (Figure A-63)**—For committing resource changes in the SR. Two options for saving and deploying Backup Tunnel SRs to the network:
  - **SR Tunnels Only**—Deploy all tunnel changes in the SR, or if no changes were made to the SR, use this to re-deploy the SR that was in **Requested** or **Invalid** state.
  - **Force Deploy All Tunnels**—Force deployment of all tunnels in this SR. This could be useful when previous provisioning of the SR has failed, so that it is necessary to force through the deployment of all tunnels in the SR.

Figure A-63 Save & Deploy Tunnels



- **Cancel**—Cancel the operation and return to the Traffic Engineering Management Services window.

The tunnel SR search tool allows you to look for particular tunnels by selecting tunnel characteristics in the drop-down menu **tunnels with** and specify matching criteria in the **Matching** field:

- **Show:**
  - **Existing**—Show existing tunnels already deployed in the network.
  - **SR**—Show tunnels not yet deployed in the network.
- **tunnels with:**
  - **All**—Show all managed tunnels under the current provider.
  - **Tunnel Number**—Tunnel number on the head router.
  - **Head Device**—Full or partial name of the tunnel head device.
  - **Destination Device**—Full or partial host name of the tail device of the tunnel.
  - **Head, Dest Devices**—Exact host name of the head and tail devices of the tunnel.
  - **Tunnel Status**—Tunnel deployment status.
  - **Conformance**—Conformant or non-conformant tunnel.
- **matching/equal**—Specify matching criteria for your search. Wildcards are accepted. **matching** changes to **equal** if **Head, Dest Device** is selected in the drop-down menu. For **equal**, the exact host name of the head or tail device must be entered (wildcards not accepted).
- **Find**—Click the **Find** button when the search criteria has been entered.

## Create TE Backup Tunnel Window

From the TE Protection SR window, click **Create** to access the Create TE Backup Tunnel window shown in [Figure A-64](#).

**Figure A-64** Create TE Backup Tunnel

**Create TE Backup Tunnel**

SR Job ID: New      SR ID: New      SR State: REQUESTED  
Tunnel ID:      Creator:      Type: ADD

Head Device \*:

Destination Device \*:

Protected Interface(s) \*:

Backup Bandwidth Limit (kbps) \*:   
☒ Any Pool BW    
☐ Sub Pool (BC1) BW  Global Pool (BC0) BW

Tunnel Number:  Auto Gen ☒

Tunnel Bandwidth (kbps):

Tunnel Pool Type:   
☐ Global Pool (BC0)   
☐ Sub Pool (BC1)

Setup Priority (0-7):

Hold Priority (0-7):

Affinity (0x0-0xFFFFFFFF):

Affinity Mask (0x0-0xFFFFFFFF):

**Path Options:**

Showing 0 of 0 records

<input type="checkbox"/>	Option #	Path Name	Path Type	Lock Down
Rows per page: 10      Go to page: 1 of 1 <input type="button" value="Go"/>				
				<input type="button" value="Add"/> <input type="button" value="Delete"/>
				<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Note: \* - Required Field

129257

The Create TE Backup Tunnel window contains the following elements:

- **Head Device**—Head device for the tunnel. For selecting devices, see [Figure A-49](#).
- **Destination Device**—Destination device for the tunnel. For selecting devices, see [Figure A-50](#).
- **Protected Interface**—Interface(s) on the head router that this backup tunnel protects.
- **Backup Bandwidth Limit**—Bandwidth protected by the backup tunnel.
  - **Any Pool BW**—Bandwidth set aside for the protection of either the Sub Pool or the Global Pool.



- **Sub Pool (BC1) BW**—Bandwidth set aside for the Sub Pool.
- **Global Pool (BC0) BW**—Bandwidth set aside for the Global Pool.

For a definition of pool types, see [Bandwidth Pools, page 1-5](#).

- **Tunnel Number**—Tunnel number corresponding to the tunnel interface name.
  - **Auto Gen**—Check this box to generate the tunnel number at provisioning time. Otherwise, enter a desired number.




---

**Note** If a manually entered tunnel number is too low, it could prevent deployment.

---

- **Tunnel Bandwidth**—Total allocated bandwidth of this backup tunnel (display only).
- **Tunnel Pool Type**—Tunnel bandwidth pool type for this policy (display only). For a definition of pool types, see [Bandwidth Pools, page 1-5](#).
  - **Global Pool (BC0)**—Bandwidth will be reserved from Global Pool.
  - **Sub Pool (BC1)**—Bandwidth will be reserved from Sub Pool.
- **Setup Priority (0-7), Hold Priority (0-7), Affinity, Affinity Mask**—All manually created backup tunnels should have setup and hold priorities of 0 and affinity value and mask of 0x0 for them to be able to protect an element. See definitions accompanying [Figure A-51](#).

Path options:

- **Option #**—Sequential number of available explicit paths.
- **Path Name**—Name of the explicit path.
- **Path Type**—Explicit path type (**Explicit** or **Dynamic**)
- **Lock Down**—Disables reoptimization check on the tunnel, if checked.

The following actions can be performed (buttons):

- **Add**—Add a path option. This opens the Select TE Explicit Path window in [Figure A-52](#).
- **Delete**—Delete a path option.
- **OK**—Accept all changes and return to the TE Managed Primary Tunnels SR window.
- **Cancel**—Cancel the operation and return to the TE Managed Primary Tunnels SR window.

## Select TE Protected Interface

When clicking the Select button in the backup tunnel editor to select a TE protected interface, the window in [Figure A-65](#) appears.

Figure A-65 Select TE Protected Interface

#	Interface Name	IP Address	Next Hop
1.	ATM5/0.1	10.2.2.49	isctmp2
2.	FastEthernet3/0	10.2.2.81	isctmp4
3.	FastEthernet0/1	10.2.2.17	isctmp1

Rows per page: 10 Go to page: 1 of 1

Select Cancel

The Select TE Protected Interface window contains the following elements:

- **Interface Name**—Name of the interface to be protected.
- **IP Address**—IP address of the interface.
- **Next Hop**—Name of the next hop device.

The following actions can be performed:

- **Select**—Accept the selected interface and return to the previous window.
- **Cancel**—Cancel the operation and return to the previous window.

## TE Traffic Admission

This section describes the GUI elements in the TE Traffic Admission SR window.

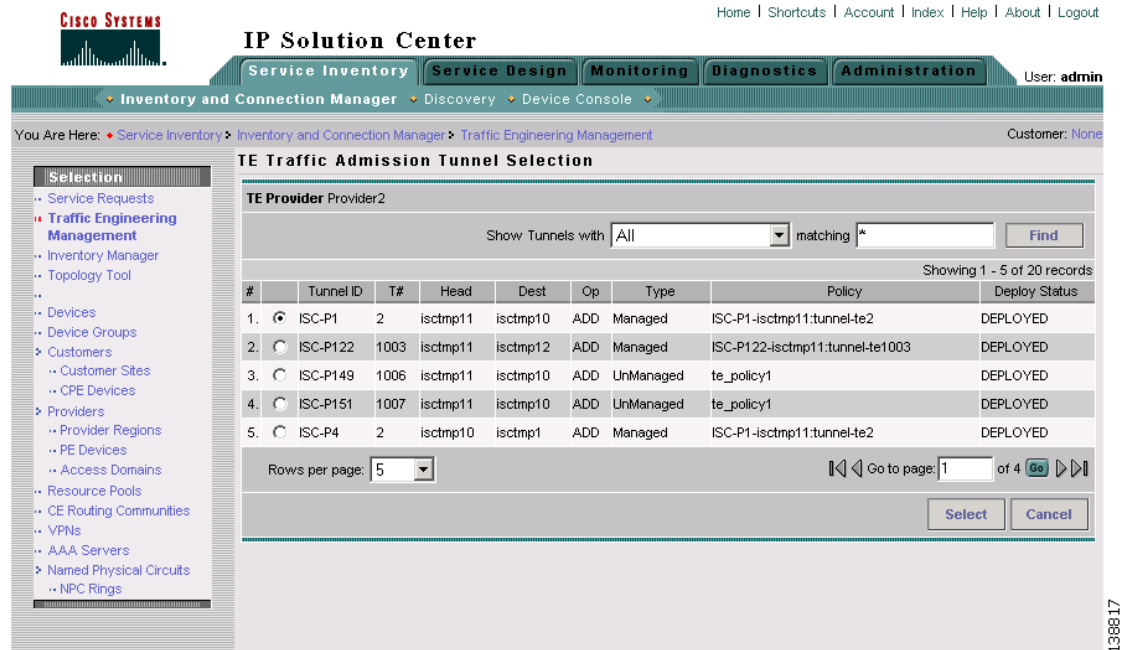
To assign traffic to traffic-engineered tunnels, see [Chapter 8, “Traffic Admission.”](#)

### Select TE Tunnel for Admission

To access the TE Traffic Admission SR window, go to **Service Inventory > Inventory and Connection Manager > Traffic Engineering Management > TE Traffic Admission**.

Prior to reaching the main TE Traffic Admission SR window, a tunnel has to be selected as shown in [Figure A-66](#).

Figure A-66 Select TE Tunnel for Admission



The **TE Traffic Admission SR** list contains the following columns:

- **Op Type**—SR operation on the tunnel, can be either **ADD**, **MODIFY**, **DELETE**, or **ADMIT**.
- **Tunnel ID**—Unique tunnel identifier used within ISC TEM.
- **T#**—Tunnel number on the head router.
- **Head**—Hostname of the head router.
- **Dest**—Hostname of the destination router.
- **Deploy Status**—Can be **Pending**, **Deployed**, or **Functional**.
- **Type**—Managed or unmanaged.
- **Policy**—Tunnel policy.

## TE Traffic Admission SR

After selecting a TE tunnel by clicking the corresponding radio button and clicking **Select**, the TE Traffic Admission SR window in [Figure A-67](#) appears.

Figure A-67 TE Traffic Admission SR

**TE Traffic Admission SR**

SR Job ID: SR ID: SR State: REQUESTED Type: ADD

Tunnel Name: isctmp11:tunnel-te2

Description:

Autoroute Announce: ☐ On ☒ Off

Autoroute Metric:  ☒ Absolute ☐ Relative

Static Routes: Showing 0 of 0 records

	Destination	Distance
Rows per page: 5	Go to page: 1 of 1 <input type="button" value="Go"/>	

The main TE Traffic Admission SR window contains the following fields:

- **Tunnel**—Tunnel name.
- **Description**—Service request description.
- **Autoroute announce**—Used to specify that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.
  - **On**—Autoroute announce is enabled.
  - **Off**—Autoroute announce is disabled.
- **Autoroute Metric**—Used to specify the Multiprotocol Label Switching (MPLS) traffic engineering tunnel metric that the Interior Gateway Protocol (IGP) enhanced shortest path first (SPF) calculation uses.
  - **Absolute**—Absolute metric mode; you can enter a positive metric value.
  - **Relative**—Relative metric mode; you can enter a positive, negative, or zero value.
- **Static Routes**—Lists any static routes that the tunnel uses.
- **Destination**—Name of the static route for the tunnel destination.
- **Distance**—Administrative distance (cost).

The following actions can be performed:

- **Add**—Add static route.
- **Edit**—Edit selected static route.
- **Delete**—Delete selected static routes.
- **Save SR**—Save service request to the SR pool.
- **Cancel**—Cancel the operation and return to the previous window.

# Administration

The administrative features directly relevant to ISC TEM are described in [Chapter 9, “Administration”](#). However, since most administrative features of ISC TEM are general to ISC, these are described in *Cisco IP Solution Center Infrastructure Reference, 4.1*.

## Monitoring

This section describes the GUI elements in the following windows:

- [TE Task Logs](#) (see also [TE Task Logs, page 10-1](#))
- [TE Performance Reports](#) (see also [TE Performance Reports, page 10-4](#)).

## TE Task Logs

The TE task logs are used to view the result of running one or more TE tasks as described in [TE Task Logs, page 10-1](#).

To view the task log for a TE task, navigate **Monitoring > Tasks > Logs**. The Task Logs window in [Figure A-68](#) appears.

**Figure A-68** Task Logs

**Task Logs**

Show Runtime Tasks with Task Name matching

Showing 1 - 5 of 15 records

#	<input type="checkbox"/>	Runtime Task Name	Action	Start Time	End Time	Status
1.	<input type="checkbox"/>	TE Interface Performance 2005-11-07 18:02:12.946_Mon_Nov_07_18:36:30_PST_2005_8	PerfCollection	2005-11-07 18:36:31.364	2005-11-07 18:53:16.704	Completed with errors
2.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-11-07 00:31:32.56_Mon_Nov_07_00:31:36_PST_2005_7	ConfigAudit	2005-11-07 00:32:17.437	2005-11-07 00:33:11.803	Completed successfully
3.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-11-07 00:31:32.56_Mon_Nov_07_00:31:36_PST_2005_7	Deployment Phase C	2005-11-07 00:31:41.193	2005-11-07 00:32:17.41	Completed successfully
4.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-11-07 00:31:32.56_Mon_Nov_07_00:31:36_PST_2005_7	Deployment Phase B	2005-11-07 00:31:40.491	2005-11-07 00:31:41.168	Completed successfully
5.	<input type="checkbox"/>	Deploy Primary SR-ID 8 2005-11-07 00:31:32.56_Mon_Nov_07_00:31:36_PST_2005_7	Deployment Phase A	2005-11-07 00:31:37.183	2005-11-07 00:31:40.468	Completed successfully

Rows per page:

Auto Refresh: ☒

138833

The Task Logs window contains the following GUI elements:

- **Runtime Task Name**—Automatically attributed task name specifying when the runtime task was created.
- **Action**—Type of task, for example **TE Discovery**, **TE Functional Audit**, or **TE Interface Performance**.
- **Start Time**—The date and time when the runtime task was started.
- **End Time**—The date and time when the runtime task ended.
- **Status**—Indicates the present status of the runtime task.



#### Note

Specific instructions for how to view a task log for a **TE Discovery** task are found in the TE Discovery section [Task Logs, page 3-7](#).

## Task Log

To access the individual log associated with a given task, from the Task Logs window click the corresponding link in the **Action** field or select a check box and click **View Log**. The Task Log window in [Figure A-69](#) appears.

**Figure A-69** Task Log

The screenshot shows the 'Task Log' window. At the top, there are filters for 'Log Level' (set to 'Warning') and 'Component' (set to '\*'). A 'Filter' button is to the right. Below the filters is a table with the following data:

Date	Level	Component	Message
2005-11-07 18:36:36	OFF	GTL	<a href="#">Started CS Job for zone=/cs, Job Log</a>
2005-11-07 18:36:40	OFF	GTL	<a href="#">CS Job Completed 1 for Collection Zone /cs Log</a>
2005-11-07 18:36:40	SEVERE	trafMonJob	isctmp11:tunnel-te1000 Bandwidth is not set

At the bottom right of the window is a 'Return to Logs' button. The number 138834 is visible on the right edge of the window.

How the log is structured depends on the type of task that was run. Here the **Level** column indicates the severity of the recorded event and the Component column states in which component of ISC the event occurred.

The following actions can be performed:

- **Filter**—Select the desired log level, optionally enter exact **Component** name, and click **Find**.
- **Return to Logs**—Return to the Runtime Actions window.

To see the task SR associated with a particular task log, select the desired task log in the Task Logs window and click the **Service Requests** button. The Tasks SRs window in [Figure A-70](#) appears.

**Figure A-70** Task SRs

The screenshot shows the 'Task SRs' window. At the top, there is a search bar with 'Show Services with' followed by a dropdown menu set to 'Job ID', a text input field containing an asterisk, and a dropdown menu set to 'All'. A 'Find' button is to the right. Below this, it says 'Showing 0 of 0 records'. The main table has columns: #, a checkbox, Job ID, State, Type, Operation Type, Creator, Customer Name, Policy Name, and Description. The first row shows: 1., a checked checkbox, 8, a green box labeled 'DEPLOYED', DEPLOYED TE Tunnel, MODIFY, admin, and empty fields for Customer Name, Policy Name, and Description. At the bottom, there is a 'Rows per page' dropdown set to 5, a 'Go to page' field set to 1 of 1, and 'Go', 'Links', and 'Return' buttons.

#		Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Description
1.	<input checked="" type="checkbox"/>	8	DEPLOYED	DEPLOYED TE Tunnel	MODIFY	admin			

The Task SRs window contains the same GUI elements as the ones in the Service Requests window, namely the following:

- **Job ID**—Job ID for the SR.
- **State**—Indicates whether the tunnel state is DEPLOYED or NOT DEPLOYED and whether it is Conformed or Not Conformed.
- **Type**—The type of service request, indicating which service issued the request. For a detailed description of the possible service types, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.
- **Operation Type**—SR operation on the tunnel, can be either **ADD**, **MODIFY**, **DELETE**, or **ADMIT**. Applicable only to tunnels in the current SR.
- **Creator**—ID for the user who created the SR.
- **Customer Name**—Name of the customer to which the SR applies.
- **Policy Name**—Name of the policy associated with the SR.
- **Description**—SR description provided by the user.

## TE Performance Reports

Performance reports are created when you run a **TE Interface Performance** task as described in [Creating a TE Interface Performance Task, page 9-11](#).

To view a performance report, go to **Monitoring > TE Performance Report**. The **TE Performance Report Table** in [Figure A-71](#) appears.

Figure A-71 TE Performance Report Table

**Cisco Systems** IP Solution Center

Home | Shortcuts | Account | Index | Help | About | Logout

Service Inventory Service Design **Monitoring** Diagnostics Administration User: admin

Task Manager Ping SLA **TE Performance Report** Reports

You Are Here: Monitoring > TE Performance Report Customer: None

### TE Performance Report Table

Show Traffic with: All \* Find

Showing 1 - 2 of 2 records

#	Start Time	End Time	Device Name	Interface Name	Octets In	Octets Out	Speed	Util In	Util Out
1.	2005-10-24 23:00:25.477	2005-10-24 23:02:05.967	isctmp11	10.2.4.14<->10.2.4.13	0	0	622080000	0.0	0.0
2.	2005-10-24 23:00:26.299	2005-10-24 23:02:06.407	isctmp1	10.2.3.54<->10.2.3.53	0	72	100000000	0.0	0.084575738430023

Rows per page: 10 Go to page: 1 of 1 Go

Display Close Cancel

Reconcile Data: ☐ Peak ☐ Valley ☐ Average ☒ First

The TE Performance Report Table window contains the following GUI elements:

- **Report table**—The table shows a list of Interface Performance tasks
  - **Start Time**—The date and time when the runtime task was started.
  - **End Time**—The date and time when the runtime task ended.
  - **Device Name**—Name of the device.
  - **Interface Name**—IP addresses of the interfaces on the link.
  - **Octets In**—Number of inbound octets of traffic.
  - **Octets Out**—Number of outbound octets of traffic.
  - **Speed**—Speed of the interface.
  - **Util In**—Interface utilization for inbound traffic.
  - **Util Out**—Interface utilization for outbound traffic
- **Reconcile Data**—When an Interface Performance task has been run multiple times on an interface, you can choose to reconcile the data according to the following criteria:
  - **Peak**—Select the highest interface utilization.
  - **Valley**—Select the lowest interface utilization.
  - **Average**—Select the average interface utilization.
  - **First**—Select the first occurrence of interface utilization.



You can perform the following actions:

- **Find**—Filter out performance data according the criteria selected in the drop-down menu.
- **Cancel**—Quit the report page.
- **Close**—Close the Topology Display applet if open.
- **Display**—Invoke the Topology Display to view selected links and/or tunnels in the network. Selected links/tunnels are displayed with a unique color.





## Managing Service Requests

---

This chapter describes how to manage service requests and how to access task logs.

To apply TE device changes to network devices, you must deploy the TE service request. When you deploy a TE service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

This chapter includes the following sections:

- [Accessing the Service Requests Window, page B-1](#)
- [Service Request Operations, page B-2](#)
  - [Viewing Service Request Details, page B-3](#)
  - [Editing a Service Request, page B-6](#)
  - [Decommissioning a Service Request \(Only Applies to TE Traffic Admission SRs\), page B-7](#)
  - [Purging a Service Request, page B-9](#)
- [Verifying Service Requests, page B-9](#)
- [Service Request States, page B-9](#)

## Accessing the Service Requests Window

To manage TE service requests, go to **Service Inventory > Inventory and Connection Manager > Service Requests**.

[Figure B-1](#) shows the Service Requests window.

Figure B-1 Service Requests List

The screenshot shows the IP Solution Center interface. The top navigation bar includes links for Home, Shortcuts, Account, Index, Help, About, and Logout. The main menu has tabs for Service Inventory, Service Design, Monitoring, Diagnostics, and Administration. The left sidebar shows a tree view of the system components. The main content area displays the Service Requests window. At the top of this window, there is a search bar with a dropdown for 'Show Services with' (set to Job ID), a text input for 'matching', and a dropdown for 'of Type' (set to All). Below this is a table of service requests. The table has columns for #, Job ID, State, Type, Operation Type, Creator, Customer Name, Policy Name, Last Modified, and Description. There are 7 records listed. The first record is Job ID 3, State REQUESTED, Type L2VPN, Operation Type ADD, Creator admin, Customer Name Customer1, Policy Name L2VpnPolicy1, Last Modified 9/20/05 6:59 PM, and Description. The second record is Job ID 4, State FAILED\_DEPLOY, Type QoS, Operation Type ADD, Creator admin, Customer Name Customer1, Policy Name 3550-DSCP, Last Modified 9/23/05 10:57 AM, and Description. The third record is Job ID 5, State REQUESTED, Type L2VPN, Operation Type ADD, Creator admin, Customer Name Customer1, Policy Name L2VpnPolicy2, Last Modified 9/20/05 7:00 PM, and Description. The fourth record is Job ID 6, State REQUESTED, Type VPLS, Operation Type ADD, Creator admin, Customer Name Customer2, Policy Name VPLSPolicy1, Last Modified 9/20/05 7:01 PM, and Description. The fifth record is Job ID 7, State REQUESTED, Type VPLS, Operation Type ADD, Creator admin, Customer Name Customer2, Policy Name VPLSPolicy2, Last Modified 9/20/05 7:01 PM, and Description. The sixth record is Job ID 8, State DEPLOYED, Type MPLS, Operation Type ADD, Creator admin, Customer Name Customer1, Policy Name MPLSPolicy\_PCE, Last Modified 9/23/05 1:46 PM, and Description. The seventh record is Job ID 13, State DEPLOYED, Type QoS, Operation Type ADD, Creator admin, Customer Name Customer1, Policy Name Sample\_A, Last Modified 9/23/05 2:04 PM, and Description. Below the table, there is a 'Rows per page' dropdown set to 10, and a 'Go to page' field set to 1 of 1. At the bottom, there is an 'Auto Refresh' checkbox checked, and a row of buttons: Create, Details, Status, Edit, Deploy, Decommission, and Purge.

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	3	REQUESTED	L2VPN	ADD	admin	Customer1	L2VpnPolicy1	9/20/05 6:59 PM	
2.	4	FAILED_DEPLOY	QoS	ADD	admin	Customer1	3550-DSCP	9/23/05 10:57 AM	
3.	5	REQUESTED	L2VPN	ADD	admin	Customer1	L2VpnPolicy2	9/20/05 7:00 PM	
4.	6	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy1	9/20/05 7:01 PM	
5.	7	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy2	9/20/05 7:01 PM	
6.	8	DEPLOYED	MPLS	ADD	admin	Customer1	MPLSPolicy_PCE	9/23/05 1:46 PM	
7.	13	DEPLOYED	QoS	ADD	admin	Customer1	Sample_A	9/23/05 2:04 PM	

The Service Requests window shows the current list of service requests for this username. The list includes the following information about each service request:

- **JobID**—The job number assigned to the service request by ISC. [Table B-1](#) describes ISC service request states.
- **State**—The transition state for the service request. See [Service Request States, page B-9](#) for more information.
- **Type**—The type of service request. For example, MPLS VPN, L2VPN, VPLS, QoS, or TE.
- **Operation Type**—The operation type for the service request. For example, ADD means that you are adding this service request, MODIFY that a service request has been changed from an earlier state, and DELETE that you are decommissioning this service request.
- **Creator**—Username identity of person who created or last modified the service request.
- **Customer Name**—Customer name for the service request.
- **Policy Name**—Name of policy assigned to this service request.
- **Last Modified**—Date and time the service request was created or last modified.
- **Description**—Optional text description of the service request.

## Service Request Operations

From the Service Requests window you can perform the following operations for TE service requests:

- **Create**—See the respective sections in [Chapter 5, “Basic Tunnel Management”](#), [Chapter 6, “Advanced Primary Tunnel Management”](#), or [Chapter 7, “Protection Planning.”](#)
- **Details**—See [Viewing Service Request Details, page B-3](#).
- **Status**—Select **Logs** to access any available logs for a selected service request. For more details, see [Viewing a Task Log, page 10-2](#).
- **Edit**—See [Editing a Service Request, page B-6](#).

- **Deploy**—Only supported for TE Traffic Admission service requests from this location. For TE Resource, TE Tunnel, and TE Protection service requests, see the respective sections in [Chapter 5](#), “Basic Tunnel Management”, [Chapter 6](#), “Advanced Primary Tunnel Management”, or [Chapter 7](#), “Protection Planning.”
- **Decommission**—See [Decommissioning a Service Request \(Only Applies to TE Traffic Admission SRs\)](#), [page B-7](#). Not supported for TE Resource, TE Tunnel, and TE Protection service requests.
- **Purge**—See [Purging a Service Request](#), [page B-9](#).

## Viewing Service Request Details

The service request details include the link endpoints for the service request, the history, and the configlet generated during the service request deployment operation. Use the service request details to help you troubleshoot a problem or error with the service request or to check the commands in the configlet.

This section describes how to view the details of a service request, including the history, link details, and configlets.

To view service request details:

- Step 1** Select **Service Inventory > Inventory and Connection Manager > Service Requests**.
- Step 2** Select the service request and click **Details**. The Service Request Details window appears as shown in [Figure B-2](#).

**Figure B-2** Service Request Details—Attributes

Service Request Details	
Service Request Details for Job ID 8	
Attribute	Value
Type	TE Tunnel
State	DEPLOYED
Operation Type	MODIFY
Service Request ID	21
Last Modification Time	Mon Nov 07 00:33:09 PST 2005
<div>History Audit Configlets OK</div>	

138836

From the Service Request Details page, you can view more information about:

- **Details > History**—Service request history report
- **Details > Audit**—Not supported by ISC TEM.
- **Details > Configlets**—View the ISC generated configlet for the service request

The following sections describe the links, history, and configlet details for a service request.

## History

[Figure B-3](#), [Figure B-4](#), and [Figure B-5](#) show the Service Request History Report window.

**Figure B-3 Service Request History Report (top)**

Service Request State Change Report			
Element Name	State	Create Time	Report
Service element isctmp11:tunnel-te2	LOST	2005-10-31 12:22:15	transitioned from DEPLOYED to LOST state.
Service element isctmp12:tunnel-te212	LOST	2005-10-31 12:22:15	transitioned from DEPLOYED to LOST state.
Service element isctmp1:Tunnel2	LOST	2005-10-31 12:22:15	transitioned from DEPLOYED to LOST state.
Service element isctmp12:tunnel-te1000	LOST	2005-10-31 12:22:15	transitioned from DEPLOYED to LOST state.
Service element isctmp1:Tunnel1000	LOST	2005-10-31 12:22:15	transitioned from DEPLOYED to LOST state.
Service element isctmp1:Tunnel3	LOST	2005-10-31 12:22:15	transitioned from DEPLOYED to LOST state.

138839

**Figure B-4 Service Request History Report (middle)**

Service element isctmp11:tunnel-te1000	LOST	2005-10-31 12:22:15	transitioned from DEPLOYED to LOST state.
Service element isctmp10:tunnel-te2	DEPLOYED	2005-10-31 12:22:15	transitioned from DEPLOYED to DEPLOYED state.
Service element isctmp10:tunnel-te1	DEPLOYED	2005-10-31 12:22:15	transitioned from DEPLOYED to DEPLOYED state.
SR Job ID 8 SR ID 13	LOST	2005-10-31 12:22:15	transitioned from REQUESTED to LOST state.
	REQUESTED	2005-11-02 15:54:39	SR Job ID 8 was subsumed: Old SR ID = 13, New SR ID = 14
	REQUESTED	2005-11-02 15:54:39	SR Job ID 8 transitioned from LOST to REQUESTED state
Service element isctmp11:tunnel-te2	PENDING	2005-11-06 16:02:32	transitioned from LOST to PENDING state.
Service element isctmp12:tunnel-	PENDING	2005-11-06 16:02:32	transitioned from LOST to PENDING state.

138840

**Figure B-5 Service Request History Report (bottom)**

Service element isctmp1:Tunnel300	DEPLOYED	2005-11-07 00:33:09	transitioned from DEPLOYED to DEPLOYED state.
Service element isctmp10:tunnel-te1002	DEPLOYED	2005-11-07 00:33:09	transitioned from DEPLOYED to DEPLOYED state.
Service element isctmp1:Tunnel138	DEPLOYED	2005-11-07 00:33:09	transitioned from DEPLOYED to DEPLOYED state.
Service element isctmp10:tunnel-te1	DEPLOYED	2005-11-07 00:33:09	transitioned from DEPLOYED to DEPLOYED state.
Service element isctmp11:tunnel-te1007	DEPLOYED	2005-11-07 00:33:09	transitioned from DEPLOYED to DEPLOYED state.
SR Job ID 8 SR ID 21	DEPLOYED	2005-11-07 00:33:09	transitioned from PENDING to DEPLOYED state.

OK

138841

The history report shows the following information about the service request:

- **Element name**—The device, interface, and subinterfaces participating in this service request.
- **State**—The transition states the element has gone through.
- **Create Time**—The time the element was created for this service request.
- **Report**—The action taken by ISC for the element in this service request.

## Configlets

To view configlets:

- Step 1** Click **Configlets** on the Service Request Details window. The Service Request Configlets window appears (Figure B-6).

**Figure B-6** Service Request Configlets

The screenshot shows a window titled "Service Request Configlets". Inside, there's a header "Configlets for Service Request Job ID 8" and a sub-header "Showing 1 - 7 of 7 records". Below this is a table with a single column labeled "Device". The table contains seven rows, each with a radio button and a device name: 1. isctmp1 (selected), 2. isctmp10, 3. isctmp11, 4. isctmp12, 5. isctmp5, 6. isctmp6, and 7. isctmp8. At the bottom of the table, there's a "Rows per page:" dropdown set to "10". To the right of the table, there's a pagination control: "Go to page: 1 of 1" with a "Go" button. At the bottom right of the window, there are two buttons: "View Configlet" and "OK".

#	Device
1.	<input checked="" type="radio"/> isctmp1
2.	<input type="radio"/> isctmp10
3.	<input type="radio"/> isctmp11
4.	<input type="radio"/> isctmp12
5.	<input type="radio"/> isctmp5
6.	<input type="radio"/> isctmp6
7.	<input type="radio"/> isctmp8

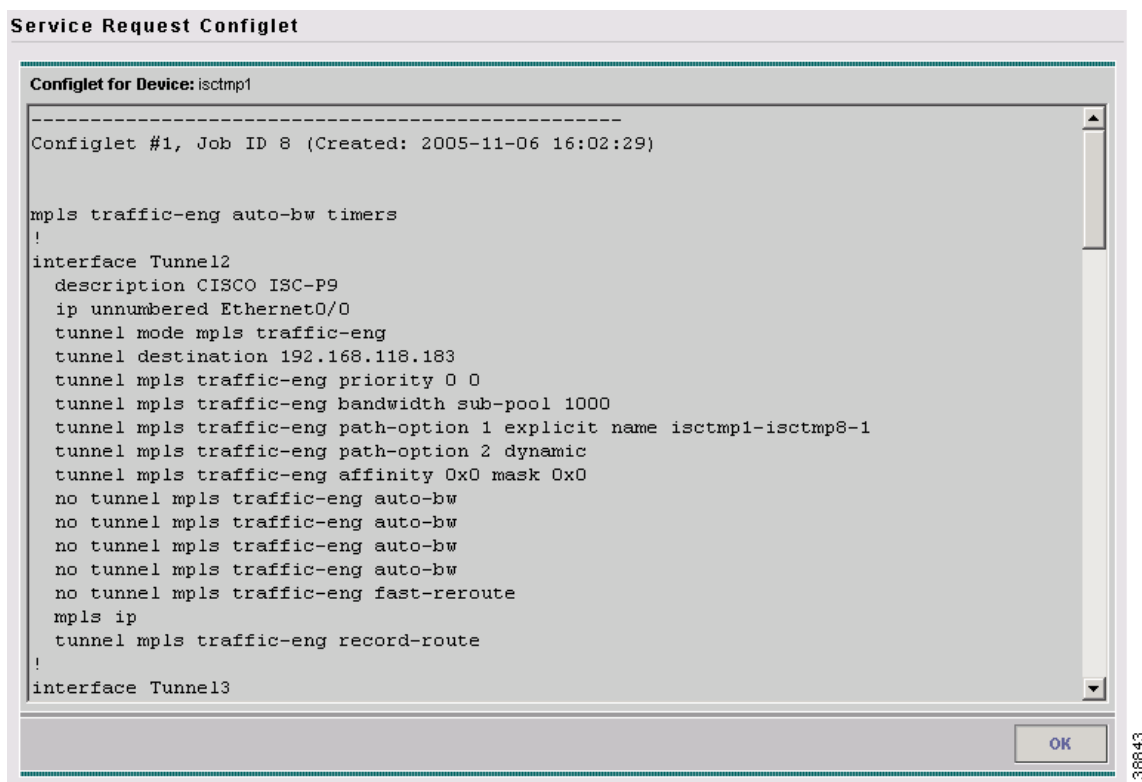
Rows per page: 10

Go to page: 1 of 1 Go

View Configlet OK

This window shows all devices whose configuration is affected by the service request.

- Step 2** Select the device to view the configlet.
- Step 3** Click **View Configlet**. The Service Request Configlet window appears (Figure B-7).

**Figure B-7** Configlet Example

The device configlet shows all commands downloaded to the device configuration during the service request deployment operation.

- Step 4** Click **OK** to exit.

## Editing a Service Request

The TE Resource, TE Tunnel and TE Protection service requests can be edited from the main Traffic Engineering Management Services window as described in chapters 4, 5, 6, and 7. This is the recommended method. Alternatively, the edit operation can be initiated from the Service Request window for these service requests.

The TE Admission service request, however, can only be initiated from the Service Requests window. We will focus on TE Admission service requests in the following procedure.

To edit a service request, use the following steps:

- Step 1** Select **Service Inventory > Inventory and Connection Manager > Service Requests**.
- Step 2** Select the service request you want to modify and click **Edit**. The TE Traffic Admission SR window in [Figure 8-2](#) appears.
- Step 3** Make the desired changes in the editor and click **Save**.



The Service Requests window reappears with the corresponding State set to **REQUESTED** and the Operation Type changed to **MODIFY** as shown in [Figure B-8](#).

**Figure B-8** Service Requests - **MODIFY REQUESTED** state

Service Requests

Show Services with  matching  of Type

Showing 6 - 10 of 16 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
6.	6	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy1	10/19/05 3:29 PM	
7.	7	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy2	10/19/05 3:29 PM	
8.	8	DEPLOYED	TE Tunnel	MODIFY	admin			11/7/05 12:33 AM	
9.	9	DEPLOYED	TE Protection	MODIFY	admin			11/2/05 3:54 PM	
10.	10	REQUESTED	TE Admission	MODIFY	admin			11/30/05 1:20 PM	tunnel-te1 : CISCO ISC-P55

Rows per page:  Go to page:  of 4

Auto Refresh: ☒

- Step 4** Deploy the service request by selecting it and clicking **Deploy > Deploy**. This is necessary for the changes to be provisioned to the network.
- Step 5** In the Deploy Service Request window, select the time at which the deployment should take place (default is immediately), and click **Save**.
- Step 6** After deployment, look for the service request state to go to DEPLOYED to indicate a successful deployment.

## Decommissioning a Service Request (Only Applies to TE Traffic Admission SRs)

To decommission a TE Admission service request, use the following steps:

- Step 1** Select **Service Inventory > Inventory and Connection Manager > Service Requests**.
- Step 2** Select the service request you want to decommission and click **Decommission**. The Confirm Request window in [Figure 8-2](#) appears.

**Figure B-9 Confirm Request - Decommissioning a TE Traffic Admission SR**


**Confirm Request**

**Confirm Decommission Service Request(s)**

Showing 1-2 of 2 records

#	Job ID	State	Operation Type	Customer Name
1.	10	REQUESTED	ADD	
2.	12	DEPLOYED	ADD	

Rows per page: 5 Go to page: 1 of 1 **Go**

Warning: 

If the service request(s) has template(s) associated with it, you should remove the template commands first before decommission the service request(s).

**OK** **Cancel**

138795

Mouse over any yellow warning symbol to see the warning message.

- Step 3** Click **OK** to confirm the decommissioning of the service request.

The Service Requests window reappears with the corresponding Operation Type changed to **DELETE** as shown in [Figure B-10](#).

**Figure B-10 Service Requests - Decommissioning a TE Traffic Admission SR**

**Service Requests**

Show Services with Job ID matching \* of Type All **Find**

Showing 11 - 15 of 16 records

#	<input type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
11.	<input type="checkbox"/>	11	DEPLOYED	TE Admission	ADD	admin			10/20/05 6:01 PM	Tunnel2 : CISCO ISC-P64
12.	<input type="checkbox"/>	12	REQUESTED	TE Admission	DELETE	admin			11/30/05 1:43 PM	Tunnel1000 : CISCO ISC-P70
13.	<input type="checkbox"/>	16	DEPLOYED	TE Admission	ADD	admin			11/2/05 3:54 PM	tunnel-te1000 : tunnel-te1000
14.	<input type="checkbox"/>	17	DEPLOYED	TE Admission	ADD	admin			11/2/05 3:54 PM	tunnel-te1004 : CISCO ISC-P136
15.	<input type="checkbox"/>	18	DEPLOYED	TE Admission	ADD	admin			11/2/05 3:55 PM	tunnel-te1006 : tunnel-te1006

Rows per page: 5 Go to page: 3 of 4 **Go**

**Auto Refresh:** ☒ **Create** **Details** **Status** **Edit** **Deploy** **Decommission** **Purge**

138796

- Step 4** Deploy the service request by selecting it and clicking **Deploy > Deploy**. This is necessary for the changes to be provisioned to the network.
- Step 5** In the Deploy Service Request window, select the time at which the deployment should take place (default is immediately), and click **Save**.
- Step 6** After deployment, look for the service request state to go to DEPLOYED to indicate a successful deployment.

## Purging a Service Request

The Purge operation is designed to remove a service request from the repository without affecting the network.

The **Purge** button has 2 options:

- **Purge**—The regular purge can only be used on the service request in **CLOSED** state. Therefore, it cannot be used on TE Resource, TE Tunnel, or TE Protection service requests since these cannot be decommissioned. These three types of service requests can only be force purged.
- **Force Purge**—During force purge, the repository checks the necessary dependency on the service request before it can be purged, so if a service request cannot be purged, there will be an error message.

## Verifying Service Requests

After you deploy a service request, you should verify that there were no errors.

You can verify a service request through the following:

- **Transition state**—The transition state of a service request is listed on the Service Requests window in the State column. See [Service Request States, page B-9](#) for more information.
- **View service request details**—From the Service Requests Details window, you can view the link endpoints and the configlets for this service request.
- **Task Logs**—Access the task logs either from the **Monitoring > Task Manager** or from **Service Inventory > Inventory and Connection Manager > Service Requests (Status button)** to help you troubleshoot a failed service request or to view more details about a service request. See [TE Task Logs, page 10-1](#) for more information.

## Service Request States

A service request transition state describes the different stages a service request enters during the provisioning process.

For example, when you deploy a service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet for each device. When the configlets are generated and downloaded to the devices, the service request enters the *Pending* state. When the devices are audited, the service request enters the *Deployed* state.

[Table B-1](#) describes the transition states for an ISC service request.

Table B-1 Cisco IP Solution Center Service Request States

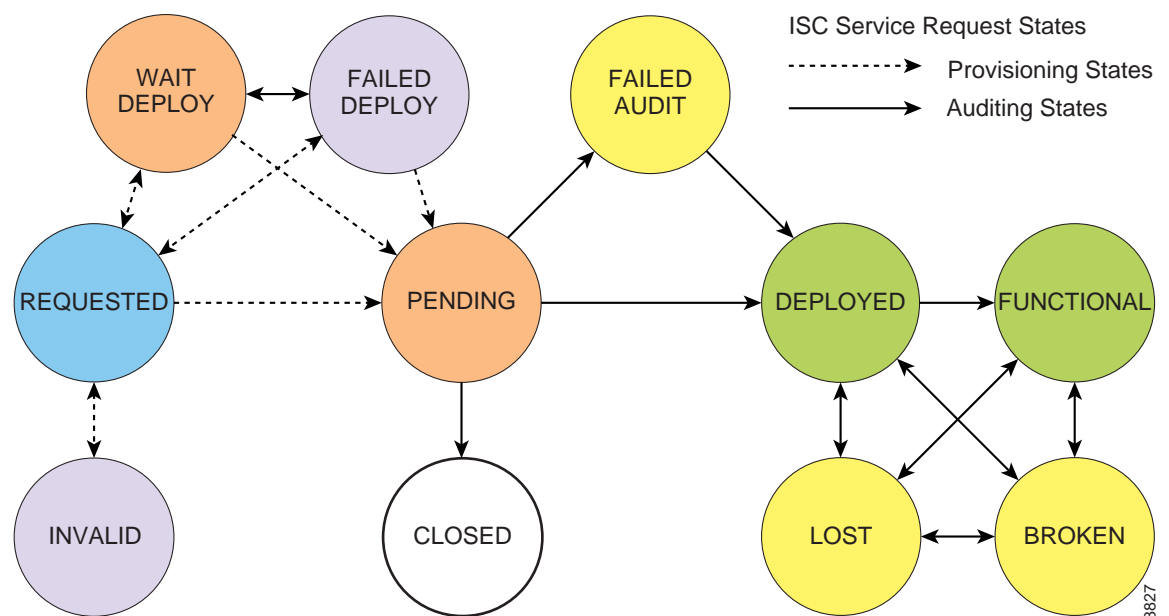
Service Request Type	Description
<b>Broken</b>	A Functional Audit has been run against the TE Tunnel SR or TE Protection SR and this audit has found that one or more tunnels are not using their first path option.
<b>Closed</b>	A service request moves to <b>Closed</b> if the service request should no longer be used during the provisioning or auditing process. A service request moves to the <b>Closed</b> state only upon successful audit of a decommission service request. ISC does not remove a service request from the database to allow for extended auditing. Only a specific administrator purge action results in service requests being removed.
<b>Deployed</b>	A service request moves to <b>Deployed</b> if the intention of the service request is found in the router configuration file. <b>Deployed</b> indicates that the configuration file has been downloaded to the router, and the intent of the request has been verified at the configuration level. That is, ISC downloaded the configlets to the routers and the service request passed the audit process.
<b>Failed Audit</b>	This state indicates that ISC downloaded the configlet to the router successfully, but the service request did not pass the audit. Therefore, the service did not move to the <b>Deployed</b> state. The <b>Failed Audit</b> state is initiated from the <b>Pending</b> state. After a service request is deployed successfully, it cannot re-enter the <b>Failed Audit</b> state (except if the service request is redeployed).
<b>Failed Deploy</b>	The cause for a <b>Failed Deploy</b> status is that DCS reports that either the upload of the initial configuration file from the routers failed or the download of the configuration update to the routers failed (due to lost connection, faulty password, and so on).
<b>Functional</b>	A Functional Audit has been successfully run against the TE Tunnel SR or TE Protection SR, meaning that all tunnels have been found to be using their first path option.
<b>Invalid</b>	<b>Invalid</b> indicates that the service request information is incorrect in some way. A service request moves to <b>Invalid</b> if the request was either internally inconsistent or not consistent with the rest of the existing network/router configurations (for example, no more interfaces were available on the router). The Provisioning Driver cannot generate configuration updates to service this request.
<b>Lost</b>	A service request moves to <b>Lost</b> when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was in the <b>Deployed</b> state, but now some or all router configuration information is missing. A service request can move to the <b>Lost</b> state <i>only</i> when the service request had been <b>Deployed</b> .
<b>Pending</b>	The provisioning engine has successfully deployed the requested changes to the network, but the config audit has not yet completed its checking that the network configuration agrees with the expected configuration stored in the repository.

Table B-1 Cisco IP Solution Center Service Request States (continued)

Service Request Type	Description
<b>Requested</b>	If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains <b>Requested</b> , the service is in an error state.
<b>Wait Deploy</b>	This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. <b>Wait Deploy</b> indicates that the configlet has been generated, but it has not been downloaded to the Cisco CNS-CE server because the device is not currently online. The configlet is staged in the repository until such time as the Cisco CNS-CE server notifies ISC that it is up. Configlets in the <b>Wait Deploy</b> state are then downloaded to the Cisco CNS-CE server.

Figure B-11 illustrates which service request states relate to the configuration auditing process, and which states relate to the provisioning process.

Figure B-11 Service Requests States



93827





## Warnings and Violations

---

This appendix lists warnings and violations that might be invoked when using the planning tools in Cisco IP Solution Center Traffic Engineering Management (ISC TEM) (computation engine).

This appendix contains the following sections:

- [Overview, page C-1](#)
- [Warnings, page C-2](#)
- [Violations, page C-3](#)

### Overview

Warnings and violations are tied in with the planning tools (see the [“Planning Tools” section on page 1-5](#)). They are issued under the following circumstances:

- During an attempt to audit, place, repair, or groom a primary managed tunnel.
- During an attempt to protect selected network elements (links, routers, or SRLGs). Here, they help determine the cause of the failed protection (see [Chapter 7, “Protection Planning”](#)).

When the off-line backup route generation is called to determine if certain elements can be protected, the backup route generator responds for each element with either a set of tunnels that protect the element or a set of violations and warnings that help determine why the element could not be protected.



**Note**

---

In the following, the term DirectedLink refers to a router interface.

---

# Warnings

This class is characterized by all reports that are warnings. They are considered less severe than violations in the sense that they don't prevent the computation of a protection path.

## Protection Computation Warnings

### **WarningFixVetoed**

A fix of this element would have caused a neighbouring element to become unprotected. This fix is vetoed and no changes are proposed.

### **WarningRouterNotConformant**

This element or any adjacent routers is/are not Protocol Conformant. It cannot therefore be protected.

Fields:

- Report Type—Name of report type.
- Description—Description of the problem signaled by the violation.
- Non-conformant router—Router that does not support traffic engineering.

### **WarningTunnelBandwidthQuotaTooSmall**

The bandwidth of a backup tunnel that protects this element is below the minimum allowed bandwidth capacity.

Fields:

- Minimum allowed bandwidth quota—Minimum bandwidth allowed to protect the element in question.
- Actual tunnel bandwidth quota—Actual bandwidth of the backup tunnel.

### **WarningTunnelNumberTooLarge**

There are too many backup tunnels for a flow through this element.

Fields:

- Maximum tunnel number allowed—Maximum number of tunnels allowed for a given network element.
- Actual Tunnel Count—Actual number of tunnels imposed on this network element.
- Flow:
  - Maximum Bandwidth—Maximum bandwidth for the traffic flow that needs to be protected.
  - Head Links—Protected interface for this flow.
  - Through Router —Protected device through which the regular traffic flow passes. If the protected element is a link, the Through Router field will not appear.
  - Tail Router—Host name of destination (tail) router.
  - Type (NHop, NNHop)—Next hop type: NHOP for link (no through router) and NNHOP for node.

### **WarningZeroProtectedFlow**

A flow through this element is protected by a backup tunnel, but has a maximum flow of zero.



Fields:

- Flow:
  - Maximum Bandwidth—Maximum available bandwidth on the element.
  - Head Links—Protected interface for this flow.
  - Through Router —Protected device through which the regular traffic flow passes. If the protected element is a link, the Through Router field will not appear.
  - Tail Router—Host name of destination (tail) router.
  - Type (NHop, NNHop)—Next hop type: NHOP for link (no through router) and NNHOP for node.

## Violations

This class is specialized by all reports that are violations. They are considered more "severe" than warnings because unlike warnings, they will prevent the computation of a protection path.

### Primary Placement Computation Violations

#### ViolationFrrProtectionInadequate

The FRR protection for a tunnel does not meet the specified protection level.

Fields:

- Report Type—Name of report type.
- Description—Description of the problem signaled by the violation.
- Required FRR Protection Level—Used to enable an MPLS traffic engineering tunnel to use a backup tunnel in the event of a link failure if a backup tunnel exists. Possible levels are **None**, **Best Effort**, **Link and SRLG**, and **Link, SRLG and Node**.
- Primary Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
- Path—Tunnel Path
  - Node—Device host name. Is only displayed if the protection level is "Link, SRLG & Node".
  - Protected (Node)—Indicates whether each node is protected (Yes) or not (No). Is only displayed if the protection level is "Link, SRLG & Node".
  - Link Label—IP addresses of the interfaces on the link.
  - Protected (Link)—Indicates whether each link is protected (Yes) or not (No).

#### ViolationInconsistentResourceAttributeChanges

A Topology-change attempts to modify one or more attributes on a resource causing a pair of its attributes to become inconsistent.

Fields:

- Report Type—Quality report, warning report, or violation report.

- Description—Description of the problem signaled by the violation.
- Resource—
  - Id—Id for head device or head interface representing the network resource.
  - Type—Resource device or interface.
- Attributes:
  - Attribute—Names of inconsistent attributes.
  - New Value—New attribute value proposed by user.

#### **ViolationInconsistentTunnelAttributeChanges**

A Tunnel-change attempts to modify one or more attributes on a tunnel causing a pair of its attributes to become inconsistent.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
- Attributes:
  - Attribute—Names of inconsistent attributes.
  - New Value—New attribute value proposed by user.

#### **ViolationLinkAffinityMismatch**

A least one directed link in the path of a Primary Tunnel does not have attribute flags that match the affinity bits and mask of the Tunnel.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Primary Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
  - Affinity Bits/Mask—Affinity bits and mask of the tunnel.
- Path—Name of tunnel path.
  - Outgoing Interface—Host name/IP address of outgoing interface.
  - Attribute Flags—Links attributes to be compared to the tunnel's affinity bits. All have to be identical to have a valid path. The violation is triggered when at least one is different.

#### **ViolationLinkPoolOversubscribed**

The specified bandwidth pool for a directed link is over-subscribed by Primary Tunnels that pass through it.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Directed Link:
  - Head Device/Interface—Host name for the head device and IP address of interface.
  - Tail Device/Interface—Host name for the destination (tail) device or interface.
  - Pool—Global pool or sub pool.
  - Pool Bandwidth—The allocated global pool or sub pool bandwidth on the link.
- Primary Tunnel (table)—Specifies how many tunnels are using the link resource.
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
  - Bandwidth—Total bandwidth of the tunnel.
  - Pool—Global pool or sub pool.
  - Path—Name of tunnel path.

#### **ViolationMaxReRoutesExceeded**

This number of Primary Tunnel re-routes in this solution exceeds the specified maximum.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Number of re-routes in solution—Number of re-routes proposed by the computation engine.
- Specified maximum number of re-routes—Maximum number of re-routes allowed.

#### **ViolationNoPathInLayout**

In the presence of other Primary Tunnels that have already been placed on the topology, no legitimate path is possible for a requested Primary Tunnel. Note: If a user requested path was specified this only means that the Primary Tunnel could not be placed on that requested path in the presence of other Primary Tunnels.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Requested Primary Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
  - Bandwidth—Total bandwidth of the tunnel.
  - Requested Path—User-specified path for the tunnel.
  - Pool—Global pool or sub pool.

- FrrProtection—Possible protection levels are **None**, **Best Effort**, **Link and SRLG**, and **Link, SRLG and Node**.
- Propagation Delay—The time it takes for traffic to travel along a link from the head interface to the tail interface.
- AffinityBits/Mask—Affinity bits and mask of the tunnel.

#### ViolationNoPathInTopology

Irrespective of other Primary Tunnels placed upon the topology, no valid path is possible for a requested Primary Tunnel. Note: If a user requested path was specified this only means that the Primary Tunnel could not be placed on that requested path irrespective of other tunnels.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Requested Primary Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of (destination) tail router.
  - Bandwidth—Total bandwidth of the tunnel.
  - Requested Path—User-specified path for the tunnel.
  - Pool—Global pool or sub pool.
  - FrrProtection—Possible protection levels are **None**, **Best Effort**, **Link and SRLG**, and **Link, SRLG and Node**.
  - Propagation Delay (optional)—The maximum time allowed for traffic to travel along the requested path..
  - AffinityBits/Mask—Affinity bits and mask of the tunnel.

#### ViolationNoTunnelForDemand

No path implements a requested PrimaryTunnel, even though there exists a valid path in the network that this tunnel could take.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Requested Primary Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
  - Bandwidth—Total bandwidth of the tunnel.
  - Requested Path—User-specified path for the tunnel.
  - Pool—Global pool or sub pool.
  - FrrProtection—Possible protection levels are **None**, **Best Effort**, **Link and SRLG**, and **Link, SRLG and Node**.

- Propagation Delay (optional)—The maximum time allowed for traffic to travel along the requested path.
- AffinityBits/Mask—Affinity bits and mask of the tunnel.

**ViolationPathMismatch**

A Primary Tunnel has a different path to that specified for it in the User Specified Path.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Primary Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
  - Actual Path—Actual path of the tunnel associated with the violation.
  - Requested Path—User-specified path for the tunnel.

**ViolationPathNotConnected**

The path of a Primary Tunnel is not “connected”, that is. it does not form a connected sequence of admin-up links between the tunnel head and tail, or it contains loops.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Primary Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
  - Path—Name of tunnel path.

**ViolationPathUsesMissingLinks**

A Tunnel-change attempts to create or modify a Tunnel so that its path or “User Requested Path” uses one or more directed links that do not exist in this topology.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Primary Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
  - Change Type—Add Tunnel/Modify Tunnel.
  - Path Type—Requested/Actual.

- Path—Name of tunnel path.
- Outgoing Interface—Yes or No depending on whether a link is missing.
- Incoming Interface—Yes or No depending on whether a link is missing.

**ViolationPrimaryTunnelDelayTooLong**

A Primary Tunnel has a propagation delay that is larger than the Maximum Propagation Delay specified for it.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Required Max Propagation Delay—The maximum time allowed for traffic to travel along the requested path.
- Primary Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.
  - Path—Name of tunnel path.
  - Actual Propagation Delay (table)—The time it takes for traffic to travel along each link in the entire path.
    - Link—Link segments in path.
    - Propagation Delay—Travel time for the traffic for each link segment.

**ViolationResourceIdUnknown**

A change attempts to remove or modify a resource (link, router or SRLG) with an Id, when no resource with that Id exists.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Resource to be removed:
  - Id—Id for head device or head interface representing the network resource.
  - Type—Resource device or interface.

**ViolationTunnelIdInUse**

A change attempts to add a Primary Tunnel with an Id that already exists.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Tunnel to Add:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.

- Existing Tunnel:
  - Name—Tunnel identifier composed of a name and a tunnel number.
  - Head—Host name of head router.
  - Tail—Host name of destination (tail) router.

**ViolationTunnelIdUnknown**

A change attempts to remove or modify a Primary Tunnel with an Id when no tunnel with that Id exists.

Fields:

- Report Type—Quality report, warning report, or violation report.
- Description—Description of the problem signaled by the violation.
- Tunnel to Remove:
  - Id—Unique tunnel identifier used within ISC TEM.

## Protection Computation Violations

**ViolationAggregateBandwidthOnLink**

The bandwidth of backup tunnels for this element, which pass through the link, have a maximum bandwidth quota that exceeds the backup bandwidth of the link.

Fields:

- Required Bandwidth (due to tunnels)—Required bandwidth for the tunnels on the link.
- Link:
  - Backup Bandwidth—Total available bandwidth of the link.
  - Head Router—Host name of the head router.
  - Head Interface—IP address of the head interface.
  - Tail Router—Host name of destination (tail) router.
  - Tail Interface—IP address of the destination (tail) interface.
  - Label—IP addresses of the interfaces on the link.
  - Admin Status—Indicates whether the link is **Up** or **Down**.

**ViolationBadBackupTunnel**

The tunnel does not protect a flow over this element.

**ViolationBandwidthProtectionMismatch**

The tunnel backup bandwidth quotas of all the tunnels protecting a flow do not add up exactly to the maximum bandwidth of that flow.

Fields:

- Protected bandwidth—The protectable bandwidth of the protection path.
- Flow:
  - Maximum Bandwidth—Maximum available bandwidth on the element.
  - Head Links—Protected interface for this flow.

- Through Router —Protected device through which the regular traffic flow passes. If the protected element is a link, the Through Router field will not appear.
- Tail Router—Host name of destination (tail) router.
- Type (NHop, NNHop)—Next hop type: NHOP for link (no through router) and NNHOP for node.

#### **ViolationLinkLevelTunnelDelayTooLarge**

The delay of the backup tunnel is greater than that allowed.

Fields:

- Maximum allowed delay—Maximum delay allowed on the backup tunnel.
- Actual delay of tunnel—Actual delay of the backup tunnel.

#### **ViolationNoBackupTunnels**

There are no backup tunnels protecting this flow through the element.

Fields:

- Flow:
  - Maximum Bandwidth—Maximum available bandwidth on the element.
  - Head Links—Protected interface for this flow.
  - Through Router —Protected device through which the regular traffic flow passes. If the protected element is a link, the Through Router field will not appear.
  - Tail Router—Host name of destination (tail) router.
  - Type (NHop, NNHop)—Next hop type: NHOP for link (no through router) and NNHOP for node.

#### **ViolationPassesThroughSRLG**

A backup tunnel is protecting a flow over this element that starts at a link within an Shared risk link group(SRLG). However that tunnel also passes through another link in the same SRLG.

Fields:

- Link:
  - Backup Bandwidth—Total available bandwidth of the link.
  - Head Router—Host name of the head router.
  - Head Interface—IP address of the head interface.
  - Tail Router—Host name of destination (tail) router.
  - Tail Interface—IP address of the destination (tail) interface.
  - Label—IP addresses of the interfaces on the link.
  - Admin Status—Indicates whether the link is **Up** or **Down**.
- SRLG—User-defined SRLG name.
- Flow:
  - Maximum Bandwidth—Maximum available bandwidth on the element.
  - Head Links—Protected interface for this flow.



- Through Router —Protected device through which the regular traffic flow passes. If the protected element is a link, the Through Router field will not appear.
- Tail Router—Host name of destination (tail) router.
- Type (NHop, NNHop)—Next hop type: NHOP for link (no through router) and NNHOP for node.

**ViolationUsesFailedElement**

A backup tunnel that protects this element also uses it.





## Document Type Definition (DTD) File

The Document Type Definition (DTD) file provides the rules required by the XML import file for importing bulk data into ISC TEM.

For instructions on how to import tunnels into ISC TEM, see the [“Import Primary Tunnel” section on page 6-8](#).

This chapter includes the following sections:

- [DTD File, page D-1](#)
- [Example, page D-4](#)

### DTD File

This is the DTD file provided with ISC TEM.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Data Definition for file based tunnel import -->

<!-- Import File Structure -->
<!ELEMENT IMPORT_DATA (TUN_ADD|TUN_CHANGE|TUN_DELETE|TUN_MIGRATE)+ >

<!-- Notes on attributes:
    importId: must be unique within the file,
             it is alphanumeric, must begin with alpha character,
             and no special character
    head, tail: hostname of valid TE enabled device
    policy: name of existing managed tunnel policy
    bw: must be numeric and values between 0-2147483647
    tnum: is the number portion of a tunnel interface
         E.g. for "interface tunnel3", use tnum="3"
         must be numeric and values between 0-65535
-->

<!-- Tunnel Add

- #IMPLIED attributes are optional, if not specified, defaults to null
- If tnum is not specified, system will generate tunnel number
- To enable auto bandwidth, specify AUTOBW element
- bw is required if autobw is not enabled
- By default, tunnel will be created with a system path and a dynamic path
```

```
-->

<!ELEMENT TUN_ADD (AUTOBW?)>
<!ATTLIST TUN_ADD
    importId ID #REQUIRED
    head CDATA #REQUIRED
    tail CDATA #REQUIRED
    policy CDATA #REQUIRED
    bw CDATA #IMPLIED
    tnum CDATA #IMPLIED>

<!-- Tunnel Change

    - #IMPLIED attributes are optional, if not specified, value on existing
      tunnel is kept
    - To enable auto-bw, or to change auto-bw parameters, specify AUTOBW element
    - To disable auto-bw, set disableAutoBw="yes" and do not specify AUTOBW element
    - Existing tunnel path cannot be changed directly, setting reroutable="true"
      will enable system to reroute the tunnel if necessary

-->

<!ELEMENT TUN_CHANGE (AUTOBW?)>
<!ATTLIST TUN_CHANGE
    importId ID #REQUIRED
    head CDATA #REQUIRED
    tnum CDATA #REQUIRED
    policy CDATA #IMPLIED
    bw CDATA #IMPLIED
    disableAutoBw (yes) #IMPLIED
    reroutable (true|false) #IMPLIED>

<!-- Tunnel Delete

    - all attributes are required to identify tunnel to be deleted

-->

<!ELEMENT TUN_DELETE EMPTY>
<!ATTLIST TUN_DELETE
    importId ID #REQUIRED
    head CDATA #REQUIRED
    tnum CDATA #REQUIRED>

<!-- Tunnel Migrate

    - #IMPLIED attributes are optional, if not specified, value on existing
      tunnel is kept
    - All comments under Tunnel Change (above) applies to Tunnel Migrate
    - only unmanaged primary tunnel can be migrated
    - for tunnels with unmanaged tunnel policy, must specify a managed policy
    - for tunnels that was non-conformant:
      . if bw was zero, specify a new bw or enable auto-bw
      . if path was dynamic or non-conformant, the path options will be
        replaced with a system path and a dynamic path, and reroutable will
        be set to true.
    - reroutable attribute applicable only for tunnel that had a conformant first
      explicit path (i.e. explicit path with no loopback)

-->
```

```

<!ELEMENT TUN_MIGRATE (AUTOBW?)>
<!-- ATTLIST TUN_MIGRATE
importId ID #REQUIRED
head CDATA #REQUIRED
tnum CDATA #REQUIRED
policy CDATA #IMPLIED
bw CDATA #IMPLIED
disableAutoBw (yes) #IMPLIED
reroutable (true|false) #IMPLIED-->

<!-- Auto Bandwidth

- #IMPLIED attributes are optional, if not specified, value is set to null
  for TUN_ADD and existing value is kept TUN_CHANGE
- maxBw is required when used in TUN_ADD or if existing tunnel is not auto-bw
  enabled
- minBw and maxBw must be numeric and values between 0-2147483647
- maxBw must be greater than minBw if specified
- freq must be numeric and values between 300-604800

-->

<!ELEMENT AUTOBW EMPTY>
<!-- ATTLIST AUTOBW
freq CDATA #IMPLIED
minBw CDATA #IMPLIED
maxBw CDATA #IMPLIED-->
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORT_DATA SYSTEM "TeImport.dtd">

<IMPORT_DATA>

<!-- Add New Managed Tunnel -->
<TUN_ADD importId="a1" head="isctmp3" tail="isctmp1" policy="mgdPolicy" bw="400" />
<TUN_ADD importId="a2" head="isctmp2" tail="isctmp9" policy="mgdPolicy" >
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_ADD>

<!-- Modify Existing Tunnel -->
<TUN_CHANGE importId="c1" head="isctmp2" tnum="200" bw="30" />
<TUN_CHANGE importId="c2" head="isctmp4" tnum="2" policy="mgdPolicy" reroutable="true"/>
<TUN_CHANGE importId="c3" head="isctmp5" tnum="46">
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_CHANGE>
<TUN_CHANGE importId="c4" head="isctmp2" tnum="200" bw="30" disableAutoBw="yes"/>

<!-- Delete Existing Tunnel -->
<TUN_DELETE importId="d1" head="isctmp3" tnum="45"/>

<!-- Migrate Tunnel -->
<TUN_MIGRATE importId="m1" head="isctmp2" tnum="3" policy="mgdPolicy"/>
<TUN_MIGRATE importId="m2" head="isctmp5" tnum="1" policy="mgdPolicy"/>

</IMPORT_DATA>

```

# Example

The following is an example of a tunnel import XML file conforming to the DTD file specified in [DTD File, page D-1](#). It consists of a sample block for each of the Add, Change, Delete, and Migrate operations

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORT_DATA SYSTEM "TeImport.dtd">

<IMPORT_DATA>

<!-- Add New Managed Tunnel -->
<TUN_ADD importId="a1" head="isctmp3" tail="isctmp1" policy="mgdPolicy" bw="400" />
<TUN_ADD importId="a2" head="isctmp2" tail="isctmp9" policy="mgdPolicy" >
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_ADD>

<!-- Modify Existing Tunnel -->
<TUN_CHANGE importId="c1" head="isctmp2" tnum="200" bw="30" />
<TUN_CHANGE importId="c2" head="isctmp4" tnum="2" policy="mgdPolicy" reroutable="true"/>
<TUN_CHANGE importId="c3" head="isctmp5" tnum="46">
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_CHANGE>
<TUN_CHANGE importId="c4" head="isctmp2" tnum="200" bw="30" disableAutoBw="yes"/>

<!-- Delete Existing Tunnel -->
<TUN_DELETE importId="d1" head="isctmp3" tnum="45"/>

<!-- Migrate Tunnel -->
<TUN_MIGRATE importId="m1" head="isctmp2" tnum="3" policy="mgdPolicy"/>
<TUN_MIGRATE importId="m2" head="isctmp5" tnum="1" policy="mgdPolicy"/>

</IMPORT_DATA>
```



---

## A

About This Guide [xi](#)

administration

- GUI [A-67](#)

administrative features [9-1](#)

admin status [A-25](#)

affinity [9-4, A-48, A-63](#)

affinity bits [A-28](#)

affinity mask [9-4, A-48, A-63](#)

algorithm

- Randomize [11-10, A-12](#)
- Spring [11-10, A-12](#)
- using [11-10](#)

antialiasing [11-9, A-11](#)

Assign TE Resources

- in GUI [A-40](#)

attribute bits, resource modification [A-28](#)

audience [xi](#)

Audit SR

- from TE Protection SR [7-11](#)

auto-gen

- creating multicast tunnels [A-46](#)

Auto Refresh

- discovery [3-8](#)

autoroute announce [8-3, A-66](#)

autoroute metric [8-3, A-66](#)

---

## B

backing store [11-9, A-11](#)

backup tunnel

- create [5-20, A-59](#)

creation [5-2](#)

deployment logs [10-1](#)

field definitions [A-60, A-62](#)

GUI [A-59](#)

introduction [5-2](#)

bandwidth

- auto [1-4](#)
- calculating utilization [1-2, 9-11](#)
- global pool [A-25](#)
- guarantees [1-4, 1-5](#)
- limit [A-62](#)
- max global (BC0) reservable [A-28](#)
- max sub pool (BC1) [A-28](#)
- non-zero [1-4](#)
- pool type [9-4, A-48](#)
- sub pool [A-25](#)
- total allocated [A-25](#)

Broken state [B-10](#)

browsers

- limitation on multiple [2-2](#)

---

## C

Cisco IOS

- commands [B-3](#)

Class-of-Service (CoS) [5-2, 8-1](#)

closed state [B-10](#)

Command Line Validation Tool

- overview [6-9](#)

commands

- downloaded to device [B-6](#)

concurrency

- limitation [2-2](#)

ConfigAudit log [10-1](#)

configlet

viewing [B-5](#)

configlets [9-17](#)

managing service requests [B-5](#)

conformant/non-conformant tunnels [1-4](#)

Conformant tunnels

definition [1-4](#)

conventions and terminology [xviii](#)

coordinates

set [11-4](#)

customer

select [2-9](#)

---

## D

Data persistence [1-3](#)

decommissioning a service request [B-7](#)

delay constraint [A-48](#)

deploy

force deploy [5-24, A-43, A-56, A-61](#)

tunnel [5-15, 5-17, 5-19, 5-26, 5-27, 7-11](#)

deployed state [B-9, B-10](#)

deployment

force deploy [8-5, A-30](#)

queue [A-56, A-61](#)

status, traffic admission [8-2](#)

task logs [10-1](#)

difference between managed and unmanaged [A-59](#)

DirectedLink [C-1](#)

documentation [xii](#)

conventions and terminology [xviii](#)

Document Type Definition

see DTD file [D-1](#)

double buffer [11-9, A-11](#)

downloaded commands [B-6](#)

DTD file

contents [D-1](#)

overview [D-1](#)

using to import tunnels [6-9](#)

---

## E

edge length

automatic [A-13](#)

constant [A-13](#)

epsilon, algorithm constant [A-13](#)

explicit path

accessing in GUI [A-30, A-33, A-35](#)

create [A-34](#)

edit [5-3, 5-5, A-34](#)

editor [5-6](#)

fields in GUI [A-33](#)

select [5-4, 5-13, 5-23, A-49, A-64](#)

viewer [5-14, A-50](#)

---

## F

failed audit state [B-10](#)

failed deploy state [B-10](#)

failed service request [B-9](#)

features in ISC TM [1-2](#)

FRR protection level [9-4, A-48](#)

Functional state [B-10](#)

---

## G

grid

color [A-15](#)

in Topology Display [A-14](#)

spacing [A-15](#)

GUI

accessing [A-1](#)

administration [A-67](#)

Assign TE Resources [A-40](#)

backup tunnel [A-59](#)

Create Managed TE Tunnel [A-41](#)



Create Unmanaged TE Tunnel [A-59](#)  
 field descriptions [A-1](#)  
 layout graph [11-4](#)  
 monitoring [A-67](#)  
 overview [A-1](#)  
 resource modification [A-28](#)  
 Save Graph Layout [11-4](#)  
 task runtime actions [3-7](#)  
 TE Explicit Path [A-33](#)  
 TE links [A-21](#)  
 TE nodes [A-18](#)  
 TE Providers [A-3](#)  
 TE Topology [A-5](#)  
 TE Traffic Admission [A-64](#)  
 Traffic Management Services [A-1](#)

---

## H

hold priority [1-4, 5-2, 5-4, 9-4, A-48](#)

---

## I

import file  
   description [6-9](#)  
 interface  
   calculating bandwidth utilization [1-2, 9-11](#)  
   non-TE [5-4, 5-7](#)  
   TE [5-7](#)  
 invalid state [B-10](#)  
 IOS-XR  
   limitation with non-POS interfaces [2-2](#)  
 ISC TM  
   overview [1-1](#)  
   prerequisites and limitations [2-2](#)

---

## J

JRE version

support [2-2](#)

---

## L

latitude range  
   topology map [A-10](#)  
 license  
   install license keys [2-4](#)  
 link  
   add [5-7](#)  
   status [A-25](#)  
 link speed factor  
   resource modification [A-29](#)  
 logs  
   deployment log [5-16, 5-24, 6-7, 7-12, 8-5](#)  
   TE Discovery, examples [3-8](#)  
 longitude range  
   topology map [A-10](#)  
 lost state [B-10](#)

---

## M

managed and unmanaged tunnels [1-3](#)  
 manage lock  
   in GUI [A-3](#)  
 map  
   add new [11-7](#)  
   clear [11-8](#)  
   load [11-5](#)  
   projection [11-6](#)  
   supported format [11-5](#)  
   using [11-5](#)  
 max delay increase  
   resource modification [A-28](#)  
 monitoring  
   field descriptions [A-67](#)  
   GUI [A-67](#)  
 MPLS TE tunnels [1-1](#)

multicast  
     creating tunnels with auto-gen [A-46](#)

---

## N

next hop  
     list [5-7](#)  
     select [5-7](#)  
 non-Cisco devices  
     support for [2-2](#)  
 Non-conformant tunnels  
     definition [1-4](#)  
     managing [1-5](#)  
 Non-POS interfaces  
     limitation with IOS-XR [2-2](#)

---

## O

objective [xi, 2-2](#)  
 optimize links [A-12](#)  
     Topology Display [11-10](#)

---

## P

pathing constraints [5-2](#)  
 pending state [B-9, B-10](#)  
 performance reports  
     see TE Performance Reports [10-4](#)  
 planning  
     concurrent [9-17](#)  
 Planning tools  
     introduction [1-5](#)  
 point-to-point links  
     ISC TEM support [2-2](#)  
 policy  
     create [5-2](#)  
     managed [5-2](#)  
     overview [9-2](#)

    TE tunnel [5-13, 6-6](#)  
     unmanaged [5-2](#)  
 policy editor [9-3](#)  
 preconfiguration process  
     [2-3](#)  
 preferential treatment of traffic [8-2](#)  
 primary tunnel  
     create [5-8, 5-11, 6-4, A-44, A-59](#)  
     deployment logs [10-1](#)  
     edit [A-52](#)  
     GUI [A-41, A-59](#)  
     introduction [5-1, 5-2, 6-1](#)  
     managed [5-8, A-41, A-44](#)  
     types of [5-8](#)  
     unmanaged [5-8, A-59](#)  
     view details [A-43](#)  
 prioritization  
     path selection [5-2](#)  
 projection  
     topology map [A-10](#)  
 propagation delay  
     resource modification [A-28](#)  
 protected interface [A-62](#)  
 provision preference [5-8, A-34](#)  
 purging a service request [B-9](#)

---

## R

Randomize algorithm [A-12](#)  
 related documentation [xii](#)  
 repaint period [A-13](#)  
 repository  
     loading into topology GUI [A-7](#)  
     populate [3-2](#)  
 repository, ISC [B-1](#)  
 requested state [B-11](#)  
 resource management  
     GUI [4-1](#)  
     modifying network resources [4-1](#)

- overview [4-1](#)
- resource modification
  - attribute bits [A-28](#)
  - GUI [A-28](#)
  - link speed factor [A-29](#)
  - max delay increase [A-28](#)
  - propagation delay [A-28](#)
  - Resource Modification SR [A-30](#)
  - TE Metric [A-28](#)
- role
  - admin [2-5](#)
  - TERole [2-5](#)
  - TEServiceOpRole [2-5](#)
- Role-Based Access Control (RBAC) [1-3](#)

---

## S

- schedules [9-15](#)
- seed router
  - communicating via SSH [2-4](#)
  - communicating via Telnet [2-4](#)
- Service auditing [1-3](#)
- service request
  - transition states [B-9](#)
  - verifying [B-9](#)
- service request (SR)
  - history [9-17](#)
  - state [5-15, 5-18, 5-20, 5-24, 5-26, 5-27, 6-7, 6-17, 6-22, 6-26, 6-30, 7-11, 8-5](#)
- service requests
  - configlets [B-5](#)
  - decommissioning [B-7](#)
  - history [B-3](#)
  - operations [B-2](#)
  - overview [B-1](#)
  - purging [B-9](#)
  - states [B-9](#)
  - verifying [B-9](#)
  - viewing details [B-3](#)

- Service state management [1-3](#)
- setup priority [1-4, 5-2, 5-4, 9-4, A-48, A-63](#)
- SLA
  - guarantees [1-1](#)
  - violating with non-conformant tunnels [1-5](#)
- SNMP [1-2, 9-11](#)
- spacing
  - automatic [A-13](#)
  - horizontal [A-13](#)
  - vertical [A-13](#)
- Spring
  - settings in Topology Display [11-10](#)
- Spring algorithm [A-12](#)
- SSH
  - communicating with seed router [2-4](#)
- state
  - Broken [B-10](#)
  - closed [B-10](#)
  - deployed [B-10](#)
  - failed audit [B-10](#)
  - failed deploy [B-10](#)
  - Functional [B-10](#)
  - invalid [B-10](#)
  - lost [B-10](#)
  - pending [B-10](#)
  - requested [B-11](#)
  - Wait Deployed [B-11](#)
- states of service requests [B-10](#)
- static route
  - add [8-3](#)

---

## T

- task
  - create [9-6](#)
  - introduction [9-5](#)
  - multiple instances [10-3](#)
  - schedule [9-9, 9-10, 9-15, 9-16](#)
  - summary [9-10](#)

- TE Discovery [9-5](#)
- TE Functional Audit [9-5](#)
- TE Interface Performance [9-5](#)
- types of TE tasks [9-5](#)
- task logs [B-9](#)
  - accessing [A-67](#)
  - deployment [10-1](#)
  - field definitions [A-67](#)
  - overview [3-7, 10-1](#)
- Task Manager
  - logs created from [10-2](#)
- task runtime actions
  - viewing logs [10-2](#)
- TE Discovery
  - create task [3-3, 9-5](#)
  - overview [3-2](#)
  - prerequisites [3-2](#)
  - schedule task [3-5, 3-6](#)
  - view task log [3-7](#)
- TE Explicit Path
  - see explicit path [A-33](#)
- TE Functional Audit task
  - create [9-6](#)
- TE Interface Performance
  - select tunnel [9-14](#)
- TE Interface Performance task
  - create [9-11](#)
  - scheduling collection [9-13](#)
- TE Link
  - view details [A-23](#)
- TE Links
  - accessing [A-21](#)
- TE links
  - display [A-23](#)
  - fields in GUI [A-21](#)
  - view details [A-24](#)
- Telnet
  - communicating with seed router [2-4](#)
- TE Metric
  - resource modification [A-28](#)
- TE Nodes
  - accessing [A-18](#)
- TE nodes
  - display [A-19](#)
  - fields in GUI [A-18](#)
  - view details [A-20](#)
- TE Performance Reports
  - accessing [10-4, A-69](#)
  - GUI [A-69](#)
  - introduction [10-4](#)
- TE Policy Editor [5-3](#)
  - see policy editor [9-3](#)
- TE provider
  - create [2-6, A-3](#)
  - edit [A-3](#)
  - select [3-4](#)
- TE Topology
  - accessing [11-2](#)
  - GUI [A-5](#)
  - overview [11-1](#)
- TE Topology Interface Applet [11-1](#)
  - short description [A-5](#)
- Topology Applet
  - using [11-2](#)
- Topology Display
  - add/modify attributes [11-9](#)
  - algorithms [A-12](#)
  - applet [11-3](#)
  - clear highlighting [11-9](#)
  - clear map [A-8](#)
  - display layers [A-17](#)
  - draw elements from repository [A-7](#)
  - GUI elements [A-5](#)
  - load map [A-8](#)
  - magnetic grid [A-14](#)
  - manage and manipulate graphs [A-10](#)
  - optimize links [11-10](#)
  - print [A-8](#)

- Spring settings [11-10](#)
- tools [A-14](#)
- tunnels [A-11](#)
- view [A-14](#)
- zoom [A-14](#)
- traffic admission
  - accessing [A-64](#)
  - field definitions [A-65](#)
  - GUI [A-64](#)
  - introduction [8-1](#)
- Traffic Admission SR
  - create [8-2](#)
  - deploy [8-4](#)
- transition states [B-9](#)
- troubleshooting [B-9](#)
- tunnel
  - admission [8-1](#)
  - backup [5-2](#)
  - calculating bandwidth utilization [1-2, 9-11](#)
  - create backup [5-20](#)
  - create primary [5-8](#)
  - deployment [A-61](#)
  - policy [5-13, 6-6](#)
  - primary [5-2](#)
  - save & deploy [5-15, 5-17, 5-19, 5-24, 5-26, 5-27](#)
  - zero priority unmanaged [1-4](#)
- tunnels
  - conformant [1-4](#)
  - managed [1-3, 5-4](#)
  - non-conformant [1-4](#)
  - unmanaged [1-3](#)

---

## U

- unmanaged tunnels
  - see managed and unmanaged tunnels [1-3](#)
- user
  - set up new [2-4](#)
- user roles

- accessing [9-1](#)
- introduction [9-1](#)
- users [xi](#)

---

## V

- verifying service requests [B-9](#)
- viewing QoS configlet [B-5](#)
- violations
  - introduction [C-1](#)
  - messages [C-3](#)

---

## W

- Wait Deployed state [B-11](#)
- warnings
  - introduction [C-1](#)
  - messages [C-2](#)

---

## Z

- zooming
  - Topology Display [A-14](#)