Release Notes for Cisco MPLS Tunnel Builder Version 2.1

December 6, 2002

These release notes contain platform and system requirements and instructions for installing and setting up Version 2.1 of the Cisco MPLS Tunnel Builder.

Cisco MPLS Tunnel Builder is a web-based graphical application for configuring and visualizing Multiprotocol Label Switching (MPLS) tunnels as well as viewing performance statistics using the Service Assurance Agent (SAA) on supported Cisco IOS platforms.

Contents

These release notes contain the following sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

Cisco MPLS Tunnel Builder displays a Traffic Engineering (TE) topology map on the right of the browser window and a series of tabs on the left side. A status message window is provided on the right side at the bottom that displays server and device information messages. The user may interact with the network map using the mouse as well as view information about the nodes, links, and tunnels on the network map using the tabs.

The left side of the browser window consists of the following tabs:

- Setup—Use this tab for specifying a “seed” router, the device from which you want to view information. You can also choose a mapping style from the Setup tab:
  - Symmetric—The distance between the nodes is minimized.
  - Hierarchical—The network hierarchy is emphasized.
  - Circular—Nodes are placed in clusters where possible.
  - Orthogonal—Style is similar in appearance to a schematic diagram.
- Nodes—Use this tab for setting selected node values and displaying information about the nodes on the network map.
- Links—Use this tab for setting selected link values and displaying information about the links on the network map.
- Tunnels—Use this tab for adding, modifying, or deleting MPLS tunnels on the network map. The Tunnel Builder application propagates the changes to the network in real time.
- Delay/Jitter—Use this tab for measuring performance characteristics between devices.
- Views—Use this tab for selecting an MPLS topology, Tunnels only, or CDP topology view and for monitoring link and tunnel traps. Links and tunnels can be highlighted on the network map based on the selected metric.

System Requirements

This section describes the following:

Hardware Supported

Cisco MPLS Tunnel Builder can be used on any hardware platform that supports MPLS Traffic Engineering (TE). For Version 2.1, these platforms include the following:

- Cisco 7200 Series routers
- Cisco 7500 Series routers
- Cisco 12000 Series routers

Disk Space Requirements

The installation of the Cisco MPLS Tunnel Builder Version 2.1 requires that you have at least 90 MB of free disk space.

Disk space requirements for the operation of Tunnel Builder depend on the network size.

Operating Systems Supported

Cisco MPLS Tunnel Builder Server

The Tunnel Builder server must be running on a web server that can handle Java and provide the Cisco MPLS Tunnel Builder Java applet to a web browser. For Tunnel Builder Version 2.1, the Tunnel Builder server can run on the following:

- Solaris, Version 2.8
- Microsoft Windows NT
- Microsoft Windows 2000

Cisco MPLS Tunnel Builder Client

For Cisco MPLS Tunnel Builder Version 2.1, the Tunnel Builder client can run on the following:

- Solaris, Version 2.8
- Microsoft Windows NT
- Microsoft Windows 2000

Web Browsers Supported

Cisco MPLS Tunnel Builder Version 2.1 requires one of the following web browsers and the Java Plug-in specified below:

- Internet Explorer, Version 5.0 or later
- Netscape Navigator, Version 4.5 or later

Windows 2000 and Windows NT—If you are using Netscape Version 4.7, you need to install the Java Plug-in Version 1.3 before running Tunnel Builder.

Solaris—If you run the Solaris Version 2.8 client, use the Netscape browser Version 4.79 with the Java Plug-in Version 1.3.1.01. In the .cshrc file, set the plugin path. For example:

- For C shell users:

```
setenv NPX_PLUGIN_PATH=~java/j2rel_3_1_01/plugin/sparc/ns4
```

- For K shell users:

```
export NPX_PLUGIN_PATH=~java/j2rel_3_1_01/plugin/sparc/ns4
```

Cisco IOS Releases Supported

The Tunnel Builder application supports devices running Cisco IOS Release 12.0(22)S or later with MPLS TE enabled.

Downloading the Cisco MPLS Tunnel Builder Kit

Note Before you download theTunnel Builder kit, make sure you have your license key and *Right to Use* document from your Cisco representative or product manager.

Note If you are interested in evaluation software, make sure that you have an evaluation license key from your Cisco representative or product manager before you download the files.

To download the Tunnel Builder images and readme file, perform the following steps:

Step 1 Enter the following URL:

`http://www.cisco.com/cgi-bin/tablebuild.pl/tb`

Step 2 Select a file. On the next screen, read the Software License agreement and download the file.

For the Tunnel Builder product or evaluation kit, download the following files, one at a time, where the *x* represents the version build number:

- tb-2.1.1-kit-sol.tar
- tb-2.1.1-readme.txt
- tb-2.1.1-setup-sol.sh or tb-2.1.1-kit-win32.zip depending on the your system

Now you ready to copy your files to the web server doc directory.

Installing and Starting Cisco MPLS Tunnel Builder

This section includes the following topics:

Installation for Solaris

To install and start the Tunnel Builder application on Solaris systems, perform the following steps.

Note Default values are in brackets.

Step 1 Copy the tb-2.1.1-kit-sol.tar and tb-1.1-setup-sol.sh files to a temporary directory or a directory under your web server doc directory in which you plan to install the application. For example, **/scratch/suitespot/docs/TunnelBuilder**

Step 2 Make sure that you can execute the tb-2.1.1 setup-sol.sh script:

```
chmod 755 tb-2.1.1-setup-sol.sh
```

Step 3 Log in as root.

```
$ su root
password: password
```

Step 4 Run the tb-2.1.1-setup-sol.sh file.

```
web-server-doc-dir% ./tb-2.1.1-setup-sol.sh
```

The setup file, tb-2.1.1-setup-sol.sh, runs a script that asks you where you want to locate the Cisco MPLS Tunnel Builder files. Enter the full path of your web server doc directory.

```
Where (in what directory) would you like the Tunnel Builder client and server to be
installed?

/scratch/suitespot/docs/TunnelBuilder
```

After the Cisco MPLS Tunnel Builder files are copied and installed, you are asked to enter the Cisco license key and configure several options, as follows:

```
Please enter the Cisco license key
license-key
```

Note Enter **none** in response to the following prompt.

```
Please enter (eval) for evaluation version of BRG, (perm) for permanent version of BRG, or
(none) for Non-BRG version.
None

What port would you like to use for the Tunnel Builder client and server communication?
[7271]

Do you want the TunnelBuilder server to use telnet or ssh to access the routers? [telnet]
```

All routers will be accessed during the method that you selected.

```
Would you like to receive SNMP trap notification of links and tunnels changing status?
[no]

What port would you like to use for receiving UDP datagrams? [162]
```

Note If port 162 conflicts with other network management options, then enter another port number. Port 162 is the standard port for UDP communication.

```
What SNMP community string would you like to use? [public]

Would you like to run the Tunnel Builder server in debug mode? [no]

Would you like to enable logging of Tunnel Builder commands and logging of commands sent
to the router? [no]
```

Step 5 When the installation script is complete, you are asked if you want to run the server automatically.

To start the server manually, execute a **startTopoServer** command from your web server doc directory.

```
cd /scratch/suitespot/docs/TunnelBuilder/serverkit
web-server-doc-dir% ./startTopoServer
```

Step 6 To start the Tunnel Builder application, use your web browser to find and select the ServerControl.html file, for example, http://<*server-host-name*>/TunnelBuilder/clientkit/ServerControl.html.

To access the Tunnel Builder application from your laptop, use your web browser to find and select the ServerControlLaptop.html file. For example:

http://*server-host-name*/TunnelBuilder/clientkit/ServerControlLaptop.html.

Note If you have not previously downloaded and installed the Java Plug-in Version 1.3.1, you may be prompted to do so at this point.

The Tunnel Builder application is displayed in your browser window.

Installation on Microsoft Windows NT and Windows 2000

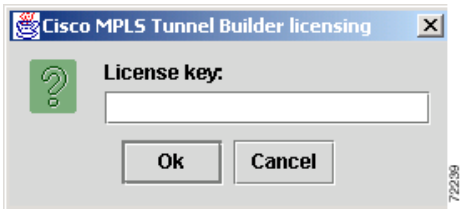
To install and start the Tunnel Builder application on Microsoft Windows NT or Windows 2000 systems, perform the following steps:

Step 1 Copy the tb-2.1.1-kit-win32.zip file to a directory on your Windows NT or Windows 2000 system. Use WinZip to extract all the files.

Note If you are not running the browser and the Tunnel Builder server on the same machine, then install Tunnel Builder in your web server's document directory.

Step 2 To start the Tunnel Builder server, access the serverkit directory where Tunnel Builder was installed and double-click the startsrv-nt.bat file. The Cisco MPLS Tunnel Builder licensing dialog box appears (see Figure 1).

Figure 1 Cisco MPLS Tunnel Builder Licensing Dialog Box



Step 3 Enter your License key and click **OK**. The Cisco MPLS Tunnel Builder Server configuration dialog box appears.

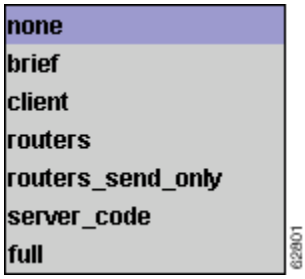
Step 4 In the Cisco MPLS Tunnel Builder Server configuration dialog box, do the following:

- Enter a port number in the **Port for Client/Server communication** field. The default is 7271.
- To select the access mode you want the Tunnel Builder Server to use for accessing the routers, click the drop-down arrow in the **Router access** field. Click **telnet** or **ssh**.
- In the Link and Tunnel Traps area, do the following:
  - To activate SNMP traps notification, check the **Enable SNMP Trap Notification** check box. The default is disabled.
  - Enter a port number in the **Port for UDP datagrams** field. The default value is 162.

Note If port 162 conflicts with other network management options, then enter another port number. Port 162 is the standard port for UDP communication.

  - Enter a community name in the **SNMP community** field. The default is public.
- To generate a log file, check the **Turn on Logging** check box. The default is to not generate a log file.
- Enter a number in the **Read timeout value (secs)** field. The default value is 30 seconds.
- To view the debug modes, click the drop-down arrow in the **Debug mode** field. Click the debug mode option (see Figure 2) that you want to track. The default option is none.

Figure 2 Debug Mode Options



After making your choices, click **OK**. The installation creates a TBconfig.txt file that contains your choices. An HTML file that sets up communication between the Cisco MPLS Tunnel Builder server and client is also updated with the port numbers to use for communications.

Step 5 To start the Tunnel Builder application, do one of the following:

- To start Tunnel Builder in your browser window, access the clientkit directory in which Tunnel Builder was installed and double-click the ServerControl.html file.
- If you installed Tunnel Builder in a web server on your Windows machine, refer to the instructions in the "Installation for Solaris" section on page 5.

Reinstallation Requirements for Upgrading

You need to reinstall the Cisco MPLS Tunnel Builder software to do any of the following upgrades:

- To Cisco MPLS Tunnel Builder Version 2.1 from Cisco MPLS Tunnel Builder Version 1.0
- To Cisco MPLS Tunnel Builder Version 2.1 from Cisco MPLS Tunnel Builder Version 2.0
- To the next license level from your current license level

Cisco MPLS Tunnel Builder Features

This section describes the features for Cisco MPLS Tunnel Builder Version 2.1. The Tunnel Builder application includes a network map and features for managing tunnels as well as for managing links and devices. Specific features are described in the following sections:

Network Map

The network map includes topologies based on Multiprotocol Label Switching (MPLS). The network map also contains tunnel information obtained directly from each device through MPLS. When a network map is generated, the Tunnel Builder application obtains all traffic engineering (TE) information and device configuration by directly accessing the devices. Cached data for this information can also be accessed from the server.

Seed Routers

The Tunnel Builder application references network maps based on a seed router. The seed router provides the MPLS-based topology information. The Tunnel Builder application maintains a list of known seed routers. You can add or delete seed routers from the Seed Routers List.

MPLS-Based Topology

The Tunnel Builder application generates a list of network nodes and links based on the MPLS topology read from the seed router. Based on the generated list, the Tunnel Builder application accesses each device to read device configuration information. Using the gathered information, the Tunnel Builder application can manage the devices, links, and MPLS TE tunnels that make up the network map.

Mapping Choices

You can view these subsets of the network topology:

- Nodes and links that are part of the MPLS-based network topology
- Tunnels existing in the network topology

Maintaining Network Map Information

The network topology is read any time that a new seed router is specified and you request a map. You can also request an update to the map for a given seed router. You can update the map with the present seed router by clicking **Fetch from Network**. After specifying a new seed router, you can update the map by clicking either Fetch button.

Device Management

Most of Tunnel Builder features described in the following section relate to the configuration of a single device. However, the Tunnel Builder application provides as much information as it can about all devices in the network map. The following features allow you to manage devices.

Viewing Device Configuration Information

The Tunnel Builder application gathers and displays the following configuration information about each device in the network map:

- Interfaces on the device (IP address, interface name, TE status, and global and subpool bandwidth settings)
- MPLS TE device ID

MPLS Tunnels Headed by Device

The Tunnel Builder application provides you with a list of MPLS tunnels headed by a specific device.

Committing Changes to Device Configurations

The Tunnel Builder application allows you to save changes to the configuration information of the device and write the current running configuration into nonvolatile memory. You accomplish this by clicking “Commit changes” in the **Setup** tab.

Link Management

The following features of the Tunnel Builder application allow you to monitor links.

Viewing Link Configuration Information

The Tunnel Builder application gathers and displays the following information about the interfaces for each link in the network map:

- Maximum bandwidth
- Maximum reservable global pool bandwidth
- Maximum reservable subpool bandwidth
- Bandwidth allocated and reservable per priority (0 to 7)
  - Total allocated bandwidth
  - Global pool reservable bandwidth
  - Subpool reservable bandwidth
- Attribute bit settings
- TE metric

Link Up/Down Event Notification

The Tunnel Builder application provides timely notification to the user of interface up or interface down events that affect any of the links in a network map.

Updating Link Bandwidth Information

The Tunnel Builder application supplies bandwidth information (allocated, global pool, and subpool numbers) on a per-priority basis for every link in the network. The application reads this information from the output of the **show mpls traffic topology** command. The bandwidth information is accurate as of the last Interior Gateway Protocol (IGP) update that occurred on the network.

The IGP update process is completely separate from the Tunnel Builder application and any Tunnel Builder map updates that occurs. The time between IGP updates is determined by a router configuration setting and by a router threshold that is triggered when a tunnel tries to come up, but does not have the bandwidth.

The Tunnel Builder application provides an update button that causes the Tunnel Builder server to go out to the seed router, get the MPLS topology, and update the bandwidth information for every link in the map. This button allows you to get bandwidth information that is accurate as of the last IGP update.

Tunnel Management

The following features of the Tunnel Builder application allow you to manage tunnels.

Viewing and Monitoring Tunnels

The Tunnel Builder application gathers and displays the following configuration information about the MPLS tunnels found in a network map:

- Tunnel name and number
- Tunnel type: MPLS (primary tunnel), FRR (primary tunnel), or backup
- Tunnel status
  - Operating status (up or down)
  - Administrative status (up or down)
  - Path status (valid or not valid)
  - Signaling status (connected or not connected)
- Bandwidth specified for the tunnel
- Priority of tunnel
- Affinity bit settings
- Head and destination
- Explicit route (LSP) used by the tunnel
- Traffic sent and received statistics for the tunnel
- Autoroute setting for the tunnel
- Autobandwidth settings for the tunnel
- Path options assigned to tunnel

Tunnel Up/Down Event Notification

The Tunnel Builder application provides you with timely notification of a link up or link down event that affects any tunnels in a network map.

Creating a Primary Tunnel

You can create MPLS tunnels with a wide variety of configurations with the Tunnel Builder application. You must use the following configuration parameters:

- Source device (the head of the tunnel)
- Destination device (required if a dynamic path option is selected)
- At least one path option

Using the parameters described below, you can create one or more identically configured tunnels.

Note The maximum number of tunnels that you can create in a batch depends upon Cisco IOS support for the platform as a tunnel head or midpoint. For details, see *MPLS Traffic Engineering (TE)—Scalability Enhancements*.

Path Options

A tunnel may have more than one path option. Path options are numbered. The lowest numbered option is used first, if available.You can specify the following types of path options with the Tunnel Builder application:

- A new explicit path—You select the head device and a sequence of links that form the new explicit path for use by the tunnel.
- An existing explicit path—You select an existing explicit path on the head device.
- A dynamic path—You select the head device and the tail device.

Optional MPLS Tunnel Parameters

The settings for the following MPLS tunnel parameters are optional. If you do not specify a value for these parameters, the default values are used.

- Bandwidth required for the MPLS tunnel in kilobytes/second. The default is 0.
- Affinity bits, attribute values required for links carrying this tunnel, specified as a value/mask pair. The default is 0x00000000/0x0000FFFF.
- Priority used when signaling an LSP for this tunnel, with allowed values 0 to 7; 0 is the highest priority; 7 is the lowest. The default is 7. Setup priority and hold priority are typically configured to be equal. Setup priority cannot be better (numerically smaller) than the hold priority.
- Tunnel name, or tunnel description. The default is *router_t#*, where *router* is the device's host name and # is the tunnel number.
- Autoroute, specifies that the IGP should use the tunnel in its enhanced shortest path first (SPF) calculations. The default is to set no autoroute.
- Autoroute metric, specifies the MPLS traffic engineering tunnel metric (absolute or relative) value.
- Autobandwidth (can be configured for tunnels on devices that support the autobandwidth feature).
- Enable Fast ReRoute indicates whether this tunnel is a fast reroutable primary tunnel.

Directing Traffic into an MPLS Tunnel

To direct traffic into an MPLS tunnel with the Tunnel Builder application, you create a tunnel with autoroute enabled. Traffic can also be directed into an MPLS tunnel by defining a static route on the head device. You can create and delete static routes from the Nodes tab.

Creating a Backup Tunnel

You can create backup tunnels with a wide variety of configurations with the Tunnel Builder application. You must use the following configuration parameters:

- Source device (the head of the backup tunnel)
- Element(s) you want this backup tunnel to protect
- At least one path option

Path Options

A tunnel may have more than one path option. Path options are numbered. The lowest numbered option is used first, if available.You can specify the following types of path options with the Tunnel Builder application:

- A new explicit path—You select the head device and a sequence of links that form the new explicit path for use by the tunnel.
- An existing explicit path—You select an existing explicit path on the head device.

Optional Backup Tunnel Parameters

The settings for the following backup tunnel parameters are optional.

- Bandwidth limit for the backup tunnel in kilobytes per second.
- Pool that the backup tunnel will protect.
- Affinity bits, attribute values required for links carrying this tunnel, specified as a value/mask pair. The default is 0x00000000/0x0000FFFF.
- Priority used when signaling an LSP for this tunnel, with allowed values 0 to 7; 0 is the highest priority; 7 is the lowest. The default is 7. Setup priority and hold priority are typically configured to be equal. Setup priority cannot be better (numerically smaller) than the hold priority.
- Tunnel name, or tunnel description. The default is *router_t#*, where *router* is the device's host name and # is the tunnel number.

Modifying or Deleting a Tunnel

You can modify the following parameters for a specified MPLS primary tunnel using the Tunnel Builder application:

- Bandwidth
- Affinity bits
- Priority
- Autoroute
- Autoroute metric
- Autobandwidth (modifiable on devices that support this feature)
- FRR

You can use the Tunnel Builder application to delete an existing tunnel based on the head device and tunnel number. You can select multiple tunnels for deletion in a single operation.

Note When a tunnel is deleted that uses an explicit path, the explicit path is not automatically removed. When a tunnel is deleted that uses a static route, the static route is not automatically removed.

Note Backup tunnels cannot be modified using the Tunnel Builder application.

Creating and Deleting Explicit Paths

You can define an explicit path on a specified device using the Tunnel Builder application. You can use explicit paths in conjunction with defining the path options of an MPLS tunnel.

To create an explicit path, you must specify the following information:

- Name of the explicit path
- Sequence of links that make up the explicit path

The Tunnel Builder application provides information about the bandwidth available along with an explicit path. The bandwidth available on an explicit path is equal to the bandwidth available on the link within the explicit path that has the least available bandwidth.

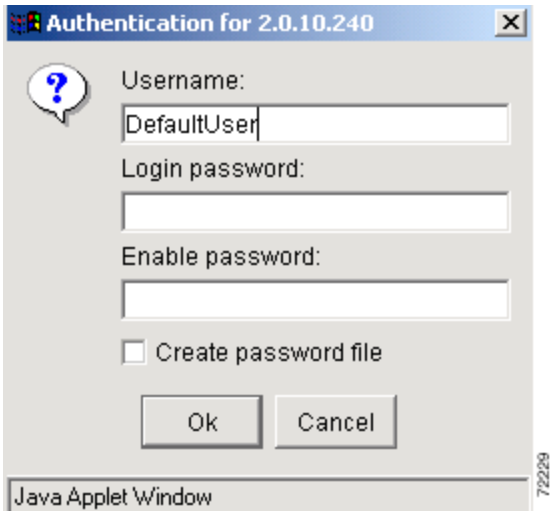
You can delete an existing explicit path on a specified device based on the explicit path name.

Security

The Cisco MPLS Tunnel Builder application provides means to ensure security when accessing routers. The application uses a combination of a user name, login password, and enable password to authenticate a user on a selected seed router (see Figure 3). Tunnel Builder uses the user name, password, and enable password combination that you entered as the default authentication information for all other routers in the network map. All routers are accessed using the same user name. If a router does not require a user name when you log in, then the user name is not sent to the router. However, the server uses the user name for client identification.

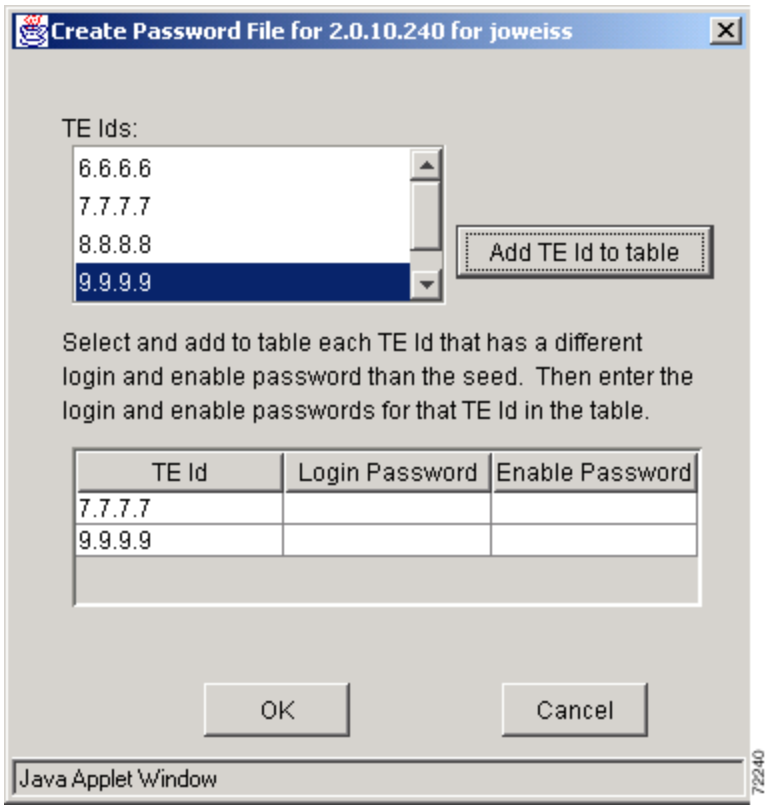
You are allowed to use different login and enable passwords on different routers through the use of a separate password file. This password file contains one line for each router using any passwords that are different from those in the default authentication information. You have the option of creating this password file when you access the Tunnel Builder application. Figure 3 shows the Authentication dialog box for the seed router that contains a Create password file check box.

Figure 3 Authentication Dialog Box



To create a password file, check the **Create password file** check box. The Create Password File dialog box appears for the seed router for the username (see Figure 4).

Figure 4 Create Password File Dialog Box



The routers are defined in the password file using their TE Ids. You can select and add a TE Id and enter its associated login password and enable password in the Create Password File dialog box. The format of the file is as follows:

```
#comment - the passwords for node 2.2.2.2
TEId:2.2.2.2:password:red:enablepw:blue
# the passwords for node 3.3.3.3
TEId:3.3.3.3:password:yellow:enablepw:green
# this router uses the same enable password as the default
TEId:4.4.4.4:password:brown
# if the router requires a null password
TEId:5.5.5.5:password::enablepw:gray
```

The password file uses the filename *username_1_2_3_4.txt*, where *username* is the user name and *1.2.3.4* is the IP address of the seed router.

The Tunnel Builder server performs this authentication process and returns a message to the Tunnel Builder client indicating if the authentication was successful or not. Only users that are successfully authenticated are allowed to fetch the MPLS and CDP topologies to construct a network map.

When you perform a command that changes the configuration of a router, for example, **create tunnel**, **modify tunnel**, **delete tunnel**, **modify link**, and **start rtr**, Tunnel Builder uses your authentication information and the additional passwords found in the password file to make the change. If another user performs a **fetch from server** on the same seed router, they are authenticated and receive the cached network map that was actually read from the network using the first user's authentication information and password file.

You cannot make changes to a router without having valid password information.

Licensing

To install Cisco MPLS Tunnel Builder Version 2,1, you must enter an authorized license key. This license key is specified on your *Right to Use* document included in your product. This license key authorizes a maximum number of traffic engineering (TE)-enabled routers in the TE topology for any single seed router, dependent on your order.

On Windows systems, the first time the server is started after the installation completes, the application displays a Cisco MPLS Tunnel Builder licensing dialog box. After you enter your license key in this dialog box and click **OK**, the application creates a license.dat file. If a license.dat file exists in the server kit directory, you do not get the dialog box to enter the license key.

On Solaris systems, the application prompts you for a license key during setup.

Once you approach the limit of the license, you are notified by a message like the following:

```
Number of TE routers (xxx) in the 1.2.3.4 network exceeds the number allowed by your
Tunnel Builder license (yyy). Please contact your administrator.
```

Where:

- xxx is the number of TE routers in your network
- 1.2.3.4 is the seed router from which you tried to fetch
- yyy is the upper bound of your license

You can choose to upgrade the maximum number of TE-enabled routers supported for any single seed router in Tunnel Builder. You will need a new *Right to Use* document and a new authorized license key(s) for each level through which you upgrade.

Right to Use documents and authorized license keys are available for the following levels:

- Up to 50 MPLS TE-enabled routers
- Up to 100 MPLS TE-enabled routers
- Up to 150 MPLS TE-enabled routers

SSH Support

During installation, you can choose either Secure Shell (SSH) or Telnet as the means to access the routers on your network. The default is Telnet. Once you select SSH or Telnet, the server uses only that method to access all routers.

If you select SSH for router access, all routers on the network must be running a version of Cisco IOS software that supports SSH.

Note The Cisco IOS image that supports SSH will support Data Encryption Standard (DES) encryption or DES and Triple DES (3DES) encryption. In the DES software images, DES is the only encryption algorithm available. In the 3DES software images, both DES and 3DES encryption are available.

If the seed router supports both DES and 3DES data encryption, then all routers on the network must be loaded with an image that supports DES and 3DES data encryption. In this case, by default, the seed router uses 3DES encryption.

If the seed router supports only DES data encryption, then all routers on the network can be loaded with an image that supports DES only or with an image that supports both DES and 3DES data encryption. A router that supports DES and 3DES understands the DES encryption sent by the seed router.

Online Help System

The Tunnel Builder online help system uses your default web browser. Supported browsers are Netscape Navigator (Version 4.5 or later) and Internet Explorer (Version 5 or later).

To access the online help system, click the **Help** button after bringing up the Tunnel Builder application.

Limitations and Restrictions

Netscape Version 4.7 and the Java Plug-in Version 1.3

You must install the Java Plug-in Version 1.3.1 *before* attempting to run the Cisco MPLS Tunnel Builder Version 2.1 client on a Microsoft Windows machine using the Netscape Communicator Version 4.7 browser. Alternatively, you can use the Netscape Version 4.5 browser or Internet Explorer Version 6.0 browser where you are prompted to download Java Plug-in Version 1.3.1, if it is not already installed.

Displaying Larger Numbers of Nodes

Displaying a topology map with a large number of nodes makes the map less readable. You can use the "+" button to zoom in on specific areas of the map for a more readable view.

Caveats

Caveats describe unexpected behavior in Cisco MPLS Tunnel Builder software releases. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only selected severity 3 caveats are included in the caveats document.

This section contains open caveats for the current Cisco MPLS Tunnel Builder release.

Open Caveats—Cisco MPLS Tunnel Builder Version 2.1

This section describes possibly unexpected behavior by Cisco MPLS Tunnel Builder Version 2.1.

- **CSCdv05063—Overwriting SeedRouters.txt during an installation upgrade**

  The ../serverkit/SeedRouters.txt file is overwritten during an upgrade of an existing TunnelVision installation.

  Workaround: Back up the existing SeedRouters.txt file and copy it back into the ../serverkit directory after an installation upgrade is performed.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.