



User Guide for Cisco Voice Services Provisioning Tool

Version 2.6(1)

July, 2005

Americas 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: 408 527-0883

Text Part Number: OL-8097-01

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.

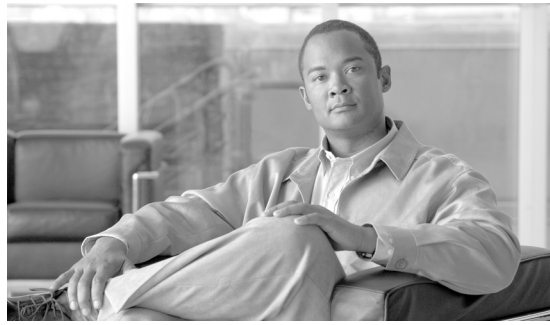
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)

User Guide for Cisco Voice Services Provisioning Tool
Copyright © 2005--2007 Cisco Systems, Inc.
All rights reserved.



CONTENTS

Preface v

| | |
|---|-----|
| Audience | v |
| Conventions | v |
| Product Documentation | vi |
| Related Documentation | vii |
| Document Organization | x |
| Terminology | xi |
| Document Change History | xi |
| Obtaining Documentation, Obtaining Support, and Security Guidelines | xii |

CHAPTER 1

| | |
|---|------|
| Determine the Correct Provisioning Tool Release | 1-1 |
| Installing VSPT Release 2.6(1) | 1-2 |
| Planning and Setting Up for Backup and Restore | 1-5 |
| Specify a Backup User ID During Installation | 1-5 |
| Select a Backup Host | 1-6 |
| Enable TFTP on the Backup Host | 1-6 |
| Installing SSH on VSPT | 1-7 |
| Uninstalling SSH on VSPT | 1-8 |
| Starting VSPT | 1-8 |
| Exiting the VSPT | 1-9 |
| Installing an Earlier Version of VSPT | 1-9 |
| Upgrading VSPT | 1-9 |
| Uninstalling VSPT | 1-10 |

CHAPTER 2

| | |
|------------------------------|-----|
| Provisioning Introduction | 2-2 |
| VSPT Introduction | 2-2 |
| VSPT Basics | 2-3 |
| VSPT Field Definitions | 2-3 |
| VSPT Data Entry Requirements | 2-7 |
| Starting the VSPT | 2-8 |
| Using the VSPT | 2-9 |
| Menus | 2-9 |
| File Menu | 2-9 |

- View Menu 2-10
- Tools Menu 2-11
- Help Menu 2-11
- Configuration Editor Views 2-12
- Defining Users and Permissions 2-12
- Exiting the VSPT 2-13

CHAPTER 3

- Perform an Integrity Check 3-1
 - Integrity Check Dialog Box Options 3-3
 - Check Integrity for MGC Signaling Configuration 3-3
 - Check Traffic Against MGC Configuration 3-4
 - Check Dial Plan Results 3-4
- View Generated Output 3-5
 - View Generated MML Commands 3-5
 - View Generated Cisco MGW Commands 3-6
- Deploy a Configuration 3-6
 - Deploying a New Configuration 3-7
 - Configuring an Incremental Deployment 3-9
- Use Telnet or ssh 3-11
- MGC Viewer 3-12
- State Operation 3-14
- Perform an Audit 3-16
- Back Up and Restore 3-17
 - About the Backup and Restore Process 3-18
 - Schedule a Backup or Restore 3-18
 - Check Status of Backup or Restore 3-20

INDEX



Preface

This document provides information you need to get started using the Cisco Voice Services Provisioning Tool version 2.6(1). You should read the documents supplied with your system before using this guide. A complete list of these documents is included in the *Cisco Media Gateway Controller Software Version 9 Installation and Configuration Guide* that ships with your system.



Note

The Cisco Voice Services Provisioning Tool (VSPT) was previously known as the Cisco Media Gateway Controller (MGC) Node Manager Provisioning Tool (MNM-PT).

This preface describes the objectives, audience, organization, and conventions of this document. It contains the following sections:

- [Audience, page v](#)
- [Conventions, page v](#)
- [Product Documentation, page vi](#)
- [Related Documentation, page vii](#)
- [Document Organization, page x](#)
- [Terminology, page xi](#)
- [Document Change History, page xi](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page xii](#)

Audience

This document is designed for network operators and administrators who have experience with telecommunication networks, protocols, and equipment and who have familiarity with data communication networks, protocols, and equipment. Software and hardware installers and network designers will also find this document useful.

Conventions

This document uses the following conventions:

Table 1 lists the documents available with Cisco Voice Services Provisioning Tool Release 2.6(1).

Table 1 Product Documentation

| Document Title | Available Formats |
|---|---|
| Release Notes for Cisco Voice Services Provisioning Tool Release 2.6(1) | <ul style="list-style-type: none"> Printed document that is included with the product On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps2272/prod_release_notes_list.html |
| User Guide for Cisco Voice Services Provisioning Tool Release 2.6(1) | <ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps2272/products_user_guide_list.html |

Related Documentation

Table 2 describes the additional documentation available

Table 2 Related Documentation

| Document Title | Available Formats |
|---|--|
| Cisco Media Gateway Controller Software Release 9 Provisioning Guide, Chapter 3, “Provisioning with the Voice Services Provisioning Tool“ | <ul style="list-style-type: none"> On Cisco.com at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/provisioning/guide/R9GUI.html |
| Cisco Media Gateway Controller Software Release 9 Dial Plan Guide, Chapter 3, “Provisioning Dial Plans with VSPT” | <ul style="list-style-type: none"> On Cisco.com at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/dial_plan/guide/DP_VSPT.html |
| Cisco Media Gateway Controller Software Installation and Configuration Guide (Releases 9.1 through 9.6) | <ul style="list-style-type: none"> PDF on the product CD-ROM On Cisco.com at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/software/SW2/pre97inst.html |
| Cisco Media Gateway Controller Software Release 9 Provisioning Guide | <ul style="list-style-type: none"> PDF on the product CD-ROM On Cisco.com at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/provisioning/guide/prvgde.html |
| <i>Cisco Media Gateway Controller Software Release 9 Dial Plan Guide</i> | <ul style="list-style-type: none"> PDF on the Product CD-ROM On Cisco.com at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/dial_plan/guide/dplan.html |
| <i>Cisco Media Gateway Controller Software Release 9 MML Command Reference</i> | <ul style="list-style-type: none"> PDF on the Product CD-ROM On Cisco.com at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/command/reference/mmlref_1.html |

Table 2 **Related Documentation (continued)**

| Document Title | Available Formats |
|--|---|
| <i>Cisco Media Gateway Controller Software Release 9 Messages Reference Guide</i> | <ul style="list-style-type: none"> • PDF on the Product CD-ROM • On Cisco.com at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/system/message/errmsg.html |
| <i>Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide</i> | <ul style="list-style-type: none"> • PDF on the Product CD-ROM • On Cisco.com at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/maintenance/guide/omtguide.html |
| <i>Cisco Media Gateway Controller Hardware Installation Guide</i> | <ul style="list-style-type: none"> • PDF on the Product CD-ROM • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re17/hrdwrnst/index.htm |
| <i>Cisco Media Gateway Controller Software Release 9 Billing Interface Guide</i> | <ul style="list-style-type: none"> • PDF on the Product CD-ROM • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/billinf/index.htm |
| <i>Cisco MGC Software Release 9.6(1) Feature Modules</i> | <ul style="list-style-type: none"> • PDF on the Product CD-ROM • On Cisco.com at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/hardware/hrdwrnst.html |
| <i>Cisco Media Gateway Controller Software Release 9 Management Information Base (MIB) Guide</i> | <ul style="list-style-type: none"> • PDF on the Product CD-ROM • On Cisco.com at this URL: http://www.cisco.com/en/US/products/hw/vcallcon/ps2027/prod_technical_reference_list.html |
| <i>Cisco Signaling Link Terminal</i> | <ul style="list-style-type: none"> • PDF on the Product CD-ROM • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/slt/index.htm |
| <i>Cisco Billing and Measurements Server, Release 2 and Cisco Billing and Measurements Server, Release 3.10 and 3.13</i> | <ul style="list-style-type: none"> • PDFs on the Product CD-ROM • On Cisco.com at this URL for Cisco Billing and Measurements Server, Release 2 http://www.cisco.com/univercd/cc/td/doc/product/access/sc/bams2/index.htm • On Cisco.com at this URL for Cisco Billing and Measurement Server, Release 3.10 http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/bams3/index.htm • On Cisco.com at this URL for Cisco Billing and Measurement Server, Release 3.13 http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/bams/3.13/guide/3132ug.html |

Table 2 **Related Documentation (continued)**

| Document Title | Available Formats |
|--|--|
| H.323 Signaling Interface Guide | <ul style="list-style-type: none"> • PDF on the Product CD-ROM • On Cisco.com at this URL: http://www.cisco.com/en/US/products/hw/vcallcon/ps2027/products_user_guide_list.html |
| <i>Voice Services Provisioning Tool Release User's Guides</i> | <ul style="list-style-type: none"> • On Cisco.com at the following URLs: http://www.cisco.com/en/US/products/sw/netmgts/ps2272/products_user_guide_list.html |
| Cisco Media Gateway Controller Software Release 9 Release Notes. | <ul style="list-style-type: none"> • On Cisco.com at the following URL: http://www.cisco.com/en/US/products/hw/vcallcon/ps2027/prod_release_notes_list.html |

**Note**

If you are using Cisco MGC Release 7, you can find documentation at:
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/index.htm>

**Note**

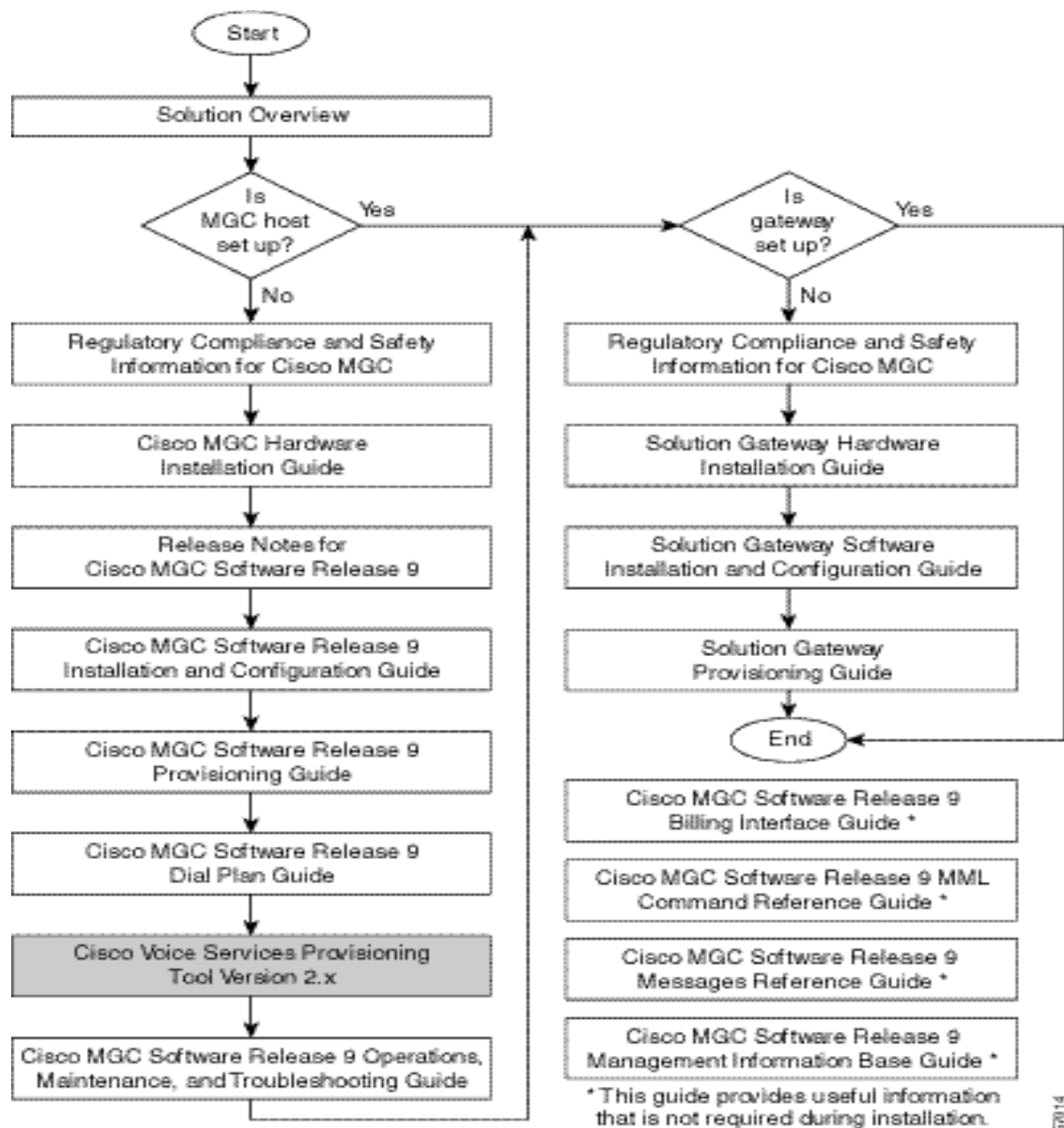
This document uses the term *media gateway controller software* or *MGC application* to mean the Cisco MGC software that runs in the UNIX environment on a server. The term *MGC* refers to the combination of this software and the server. The Cisco MGC communicates with the SS7 network to process and route calls between a traditional time-division multiplexing (TDM) network and a packet data network. This routing takes place through a variety of media gateways, standalone devices that perform the conversion between the TDM and data network formats.

**Note**

The Cisco PGW 2200 Softswitch was formerly known as the Cisco PGW 2200 PSTN Gateway. Older names of this product are the Cisco VSC 3000 and Cisco SC 2200. Some parts of this document may still use the older names.

[Figure 1](#) shows the sequence in which the various manuals documenting Cisco telephony solutions should be read.

Figure 1 Documentation Map



67014

Document Organization

Table 3 describes the major sections of this document.

| | | |
|--|--|--|
| | | |
| | | |
| | | |
| | | |

Terminology

The following terms are used in this document:

Cisco MGC host—A Sun host server running Cisco MGC software. If your product is the Cisco SC2200, this is also known as an SC host. If your product is the Cisco PGW 2200 Softswitch, this is also known as a PSTN Gateway host.

Cisco SC node—The combination of the Cisco SC2200 product and the control signaling network. The SC node consists of all solution components except the media gateway.

Cisco MGC node—The logical grouping of the active and standby MGC hosts, the control signaling network, and the Cisco Signaling Link Terminals (SLTs).

Simplex MGC node—A node that uses a single Cisco MGC host. Typically, nodes of this type are used for solution evaluation tests or for small installations. Any loss of service in the Cisco MGC host disrupts all call traffic. If your product is the Cisco SC2200, this is also called a simplex SC node.

Continuous-service MGC node—A node that uses two Cisco MGC hosts to prevent system downtime that might otherwise result from the failure of a single MGC host. Calls in progress are maintained when one MGC host fails. Continuous-service nodes use SLTs to preprocess SS7 signaling and distribute signaling to both MGC hosts. If a failover occurs, all stable calls are maintained. If your product is the Cisco SC2200, this is also called a continuous-service SC node.

Document Change History

Table 4 **Change History**

| Subject | Document No, Change Date | Change Summary |
|---|---------------------------------|--|
| Updated to document features new in VSPT 2.6(1) | OL-8097-01, July 2005 | Updated to document new features in VSPT Release 2.6(1) |
| Updated to document features new in VSPT 2.5(2) | OL-6449-01, August 2004 | Updated to document to reflect name change and separation from Cisco MGC Node Manager. |

Table 4 **Change History (continued)**

| Subject | Document No, Change Date | Change Summary |
|---|---------------------------------|---|
| Updated to document features new in MNM-PT 2.4(1) | OL-3871-01, June 2003 | Updated to document features new in Cisco MGC software Release 9.4(1) and to reflect name change and tighter integration with Cisco MGC Node Manager. |
| Updated to document features new in VSPT 2.3(2) | OL-3541-01, December 05, 2002 | Updated to document features new in Cisco MGC software Release 9.3(2). |
| Updated to document features new in VSPT 2.3(1) | OL-1910-02, July 30, 2002 | Updated to document HSI adjunct, 6509 LAN Switch, and integrated SLT. |
| Initial release, VSPT 2.2 | OL-1910-01, February 15, 2002 | Initial online release |

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



CHAPTER 1

Installing Cisco VSPT

The Cisco Voice Services Provisioning Tool (VSPT) provides an easy-to-use graphical tool to provision the Cisco PGW 2200 Softswitch running the Cisco MGC software.



Note

In the previous release the VSPT was known as the Cisco MGC Node Manager Provisioning Tool (MNM).

Individual releases of VSPT are designed to be used with specific releases of the Cisco MGC software. VSPT Release 2.6(1) is designed to be used with Cisco MGC Release 9.6(1). If you are using a different release of the Cisco MGC software, see the [“Determine the Correct Provisioning Tool Release”](#) section on page 1-1 to identify the release of VSPT that you need.

- [Installing VSPT Release 2.6\(1\), page 1-2](#)
 - [Planning and Setting Up for Backup and Restore, page 1-5](#)
 - [Installing SSH on VSPT, page 1-7](#)
- [Installing an Earlier Version of VSPT, page 1-9](#)
- [Upgrading VSPT, page 1-9](#)
- [Uninstalling VSPT, page 1-10](#)

Determine the Correct Provisioning Tool Release

You must install the provisioning tool release that is compatible with your Cisco MGC and BAMS software. Select the correct provisioning tool version by referring to [Table 1-1](#). The following versions are included on the Cisco MGC Node Manager CD. Check the applicable Release Notes for possible later patches.

Table 1-1 VSPT & Cisco MGC Software Version Compatibility

| Provisioning Tool Software Version | Cisco MGC Software Release | BAMS Software Release |
|---------------------------------------|----------------------------|------------------------------|
| Provisioning Tool (VSPT) 2.6(1) | Cisco MGC Release 9.6(1) | BAMS Phase 3 (3.13) |
| Provisioning Tool (VSPT) 2.5(2) | Cisco MGC Release 9.5(1) | BAMS Phase 3 (3.13) |
| MNM-Provisioning Tool (MNM-PT) 2.4(1) | Cisco MGC Release 9.4(1) | BAMS Phase 3 (3.12 and 3.13) |

Table 1-1 VSPT & Cisco MGC Software Version Compatibility (continued)

| Provisioning Tool Software Version | Cisco MGC Software Release | BAMS Software Release |
|--|------------------------------|--|
| Provisioning Tool (VSPT) 2.3(2) | Cisco MGC Release 9.3(2) | BAMs Phase 2, BAMS Phase 3 (3.10 and 3.12) |
| Provisioning Tool (VSPT) 2.2(2) and 2.2(2) patch 4 | Cisco MGC Release 9.2(1.5-2) | BAMS Phase 2, BAMS Phase 3 |
| Provisioning Tool (VSPT) 1.6(4) and 1.6(4) patch 3 | Cisco MGC Release 7.4 | BAMS Phase 1 |

Instructions for installing the Provisioning Tool are provided later in this chapter.

Installing VSPT Release 2.6(1)

Before installing VSPT Release 2.6(1), verify the following:

- You want to provision the Cisco PGW 2200 Softswitch running Cisco MGC software Release 9.6(1). If you are provisioning an earlier version, see the “[Determine the Correct Provisioning Tool Release](#)” section on page 1-1.
- You have met the workstation hardware and software requirements. See the “System Requirements” section of the associated release notes.
- You have established network connectivity between your workstation and the network elements.
- The network elements have the correct release of software installed.
- You have identified your desired installation configuration, one of the options described in the “[Determine the Correct Provisioning Tool Release](#)” section on page 1-1.
- You have decided if you are installing SSH for secure communications with SSH-enabled components.



Note

VSPT installation must be carried out from the VSPT server or a machine with X Window capability. Make sure you have root access on your Sun workstation.

Before you begin provisioning, you should have a list of components you want to provision, including the component names, IP addresses, properties, and other parameters. To create this list, use the instructions provided in the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/provisioning/guide/prvgde.html



Tip

In addition, descriptions of the properties and values contained in VSPT are included in Appendix A of the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* and [Table 1-2](#) of this document. Review this information before you begin provisioning, and keep it available for reference during provisioning.

To install VSPT Release 2.6(1), follow this procedure:

-
- Step 1** Verify that the requirements listed in the “[Determine the Correct Provisioning Tool Release](#)” section on [page 1-1](#) have been met.
- Step 2** Open an X terminal window.
- Step 3** If you are not already logged in as root, become the root user by entering the following command:
- ```
>su - root
```
- Step 4** Ensure that the X Windows display is set as follows:
- In csh or tcsh: `setenv DISPLAY <hostname>:0`
  - In sh or ksh: `DISPLAY=<hostname>:0 ; export $DISPLAY`
- Replace the value <hostname> with the hostname of your machine.
- Step 5** Download the VSPT tar file into the directory of your choice. The tar file is available at the following location:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/vspt>
- A valid login to the Cisco website is required for you to download the VSPT tar file from the preceding URL.
- Step 6** Navigate to the downloaded file.
- Step 7** Untar the downloaded file by entering `tar -xvf <filename>`
- Replace the value <filename> with the filename of the tar file.
- Step 8** Enter `./setup` to run the installation script.
- The VSPT InstallShield Wizard opens, displaying the Welcome window.
- Step 9** Click **Next**.
- The ReadMe Information window displays.
- Step 10** Click **Next**.
- The License Agreement window displays.
- Step 11** Accept the license agreement and click **Next**.
- The Destination Folder window displays, indicating the default destination directory.
- Step 12** Click **Next** to accept the default destination directory, or select **Change** to provide a different directory path. If you want to use a directory destination other than the default, enter the appropriate directory path and click **Next**.
- The Query Backup User Panel window displays.
- Step 13** Optional: Enter the Backup User ID (your backup server login ID), and click **Next**.



---

**Note** During installation you are asked to designate a Backup User ID. Only a user logged in with this ID can carry out backup and restore operations. See the “[Specify a Backup User ID During Installation](#)” section on [page 1-5](#) for more information. This is applicable only if you are conducting backup operations. All other features of VSPT function without the entering of a backup user ID.

---

The Ready to Install window displays.

- Step 14** Click **Install Now**.  
VSPT 2.6(1) installation take place and the Installation Summary window displays upon completion.
- Step 15** Click **Exit**.  
The VSPT InstallShield Wizard closes.
- Step 16** If you are using the VSPT Backup and Restore feature, enable TFTP on the backup server. See the [“Planning and Setting Up for Backup and Restore”](#) section on page 1-5.
- Step 17** If you are installing SSH for VSPT, see the [“Installing SSH on VSPT”](#) section on page 1-7.
- Step 18** Go on to the [“Starting VSPT”](#) section on page 1-8.

---

Table 1-2 defines the default VSPT files and directories.

**Table 1-2** *Provisioning Tool Installation Files and Directories*

| File or Directory                          | Description                          |
|--------------------------------------------|--------------------------------------|
| <b>/opt/CSCOvsp26</b>                      |                                      |
| vspt                                       | Provisioning tool application script |
| /classes                                   | Class and property files             |
| /docs                                      |                                      |
| /help                                      | Online help files                    |
| /images                                    | Images or logos used in VSPT         |
| /jre/                                      | Java Runtime Environment             |
| /netscape                                  | Netscape web browser files           |
| /uninstall                                 | Uninstall script directory           |
| /utils                                     | Utilities for VSPT                   |
| /version                                   | Provisioning Tool version            |
| <b>/var/opt/CSCOvsp26 (home directory)</b> |                                      |
| /data                                      | Configuration files                  |
| /logs                                      | Log files                            |
| /etc                                       | XML files                            |



**Note**

The files and directories listed in Table 1-2 are for the most recent version of VSPT. Your directory structure may be different if you are using an older version.

---

## Planning and Setting Up for Backup and Restore

You typically use VSPT Backup to back up the configuration on a supported component, such as a Cisco PGW 2200, onto a different server (the backup host). The configuration can then be restored if needed on the original machine.

For example, if you are backing up a Cisco PGW 2200 host, VSPT logs in to the Cisco PGW 2200 host, copies the configuration, and the Cisco PGW 2200 transfers it to the backup host using TFTP. The backup host must have TFTP enabled.

If you are going to use Backup and Restore, you should do the following:

- [Specify a Backup User ID During Installation, page 1-5](#)
- [Select a Backup Host, page 1-6](#)
- [Enable TFTP on the Backup Host, page 1-6](#)

### Specify a Backup User ID During Installation

During VSPT installation, you are prompted for a Backup ID. The Backup ID is the UNIX ID of a user account authorized to use VSPT to perform configuration backups. Depending on your security policy, this might be the ID of a particular individual, or an ID created specifically for the purpose and usable by one or more individuals authorized to perform backups.

In order for a user to schedule backups or perform immediate backups, VSPT must be started from a UNIX shell with the backup ID, in either of two ways:

- If VSPT is launched from Cisco MGC Node Manager (Cisco MNM), the user must have started the Cisco EMF client with the Backup ID. If the user's normal ID is different from the backup ID, the user must start a new Cisco MNM session with the backup ID.
- From the command line in a UNIX shell opened with the backup ID.

### If You Reinstall VSPT with a Different Backup ID

If you reinstall VSPT and select a different backup ID, you must manually delete two files that are not automatically removed in reinstallation. (This is because the files are read-only and owned by root.)

- 
- Step 1** Log in as root.
- Step 2** Change to this directory:  
`/var/opt/CSCOVsp26/logs/`
- Step 3** Delete these two files:  
`now.log`  
`testValidTFTP`
-

## Select a Backup Host

The backup host to which configurations are copied can be any of the following:

- The same machine where Cisco MGC Node Manager is installed (and typically Cisco VSPT is also installed), referred to as the network management host
- The same machine where Cisco VSPT is installed, if this is different from the Cisco MGC Node Manager machine, and if this is not a Cisco PGW 2200 host
- A separate machine used for backups



### Note

Using a Cisco PGW 2200 host as a backup host is not recommended and is specifically not supported if you are using SSH.

## Enable TFTP on the Backup Host

VSPT uses Trivial File Transfer Protocol (TFTP) as the transfer utility to transfer configuration files from the Cisco PGW (or BAMS) to the backup host. Although UNIX systems include TFTP, by default it is not enabled. To be able to send configuration files to a backup host, you must first enable TFTP on that host.

Before you begin, be sure that you are using a Solaris or Solaris-like TFTP server. Unlike some TFTP servers, the Sun Solaris TFTP server allows a file to be written to the server using TFTP only if the file already exists on the system and is writable by the root user.

TFTP software that has the behavior of the Solaris TFTP software must be used (the file must exist and have write permissions by the root user before the TFTP transfer can be successful). This is because VSPT creates the file with root write permission before attempting to back up the file using TFTP. TFTP server implementations that require the file not to exist before the backup is attempted do not work.

### To Enable TFTP

- 
- Step 1** In the file `/etc/inetd.conf`, uncomment this line:
- ```
# tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```
- Thus:
- ```
tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```
- Step 2** Create the tftp user home directory:
- ```
# mkdir /tftpboot
# chown root /tftpboot
# chmod 777 /tftpboot
```
- Step 3** Restart inetd:
- ```
ps -ef | grep inetd*
kill -HUP <inetd-pid>
```
- Step 4** Verify that TFTP is working:
- ```
# cp /etc/hosts /tftpboot/.
# cd /tmp
```

```
# tftp <machine-name>
tftp> get hosts
```

Installing SSH on VSPT

VSPT 2.6(1) can be installed on both Solaris 8 and Solaris 10.

If you are installing VSPT 2.6(1) on Solaris 10 platform on which SSH is available, check if you have SSH installed. If you already have SSH installed, modify the `sshPath` variable in the configuration file as follows and ignore this section.

```
/opt/CSCOvsp26/classes/com/cisco/transpath/dart/editor/configEditor.properties
sshPath=/usr/bin
```

Where `/usr/bin` is the default location where `ssh` and `sftp` are installed.

If you are installing VSPT 2.6(1) on Solaris 8, the SSH security package used for VSPT is the same CSCOk9000 package used on the Cisco PGW 2200, BAMS, and HSI server. To install this package on VSPT, use the same procedure as for those devices. In addition, you need to modify a variable if the base path of `ssh` and `sftp` is not the default.

Before you begin, VSPT should have software Release 2.6(1) installed.



Note

We recommend installing SSH on VSPT (and Cisco MGC Node Manager) before you install it on the Cisco PGW, so that you can use the element managers to monitor the installation process on the PGW and other managed components.

Step 1 Download the security package, CSCOk9000. You must first secure authorization.



Note

There are U.S. Government restrictions on the exporting of cryptographic technology. The Secure Shell (SSH) program falls under the umbrella of those restrictions. The security package (CSCOk9000) is registered and located in a restricted area from which only authorized customers can download.

Step 2 Stop VSPT.

If VSPT is a co-resident on the Cisco PGW server and CSCOk9000 is already installed, go on to Step 4. If not, go on to Step 3.

Step 3 Install the CSCOk9000 package on the VSPT server machine. For instructions, refer to the steps in *Cisco PGW 2200 Security Enhancements*, “Installing CSCOk9000 on the Cisco PGW 2200 Host.”

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/software/SW2/SecEnh.html

Step 4 If the base path of `ssh` and `sftp` is not the default `/opt/ssh/bin`, modify the `sshPath` variable in the configuration file:

```
/opt/CSCOvsp26/classes/com/cisco/transpath/dart/editor/configEditor.properties
sshPath=/usr/local/bin
```

Where `/usr/local/bin` is the location where `ssh` and `sftp` are installed.

After you install the CSCOk9000 package, both secure and nonsecure utilities are enabled. Users can use Telnet or ssh, FTP or sftp. If you want to disable nonsecure utilities, go on to Step 5.

Step 5 (Optional) To disable nonsecure utilities, use the following toggles:



Note The scripts `toggle_telnet.sh` and `toggle_ftp.sh`, are located in the `/opt/sun_install` directory.

- To disable FTP (making only sftp available):
`/opt/sun_install/toggle_ftp disable`
- To reenables FTP (making both FTP and sftp available):
`/opt/sun_install/toggle_ftp enable`

Uninstalling SSH on VSPT

- If you need to uninstall SSH, use the procedure described in *Cisco PGW 2200 Security Enhancements*, “Fallback Procedures” at http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/software/SW2/SecEnh.html

This reenables FTP and Telnet and uninstalls the CSCOk9000 package.

Starting VSPT

You can start VSPT standalone from the operating system or you can start it from Cisco MGC Node Manager.



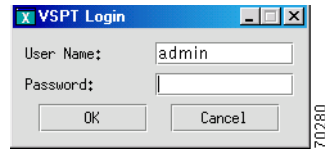
Note See the *Cisco Media Gateway Controller Software Version 9 Installation and Configuration Guide* for information on setting up user privileges and access rights.

Perform the following steps to start the VSPT:

Step 1 Do one of the following:

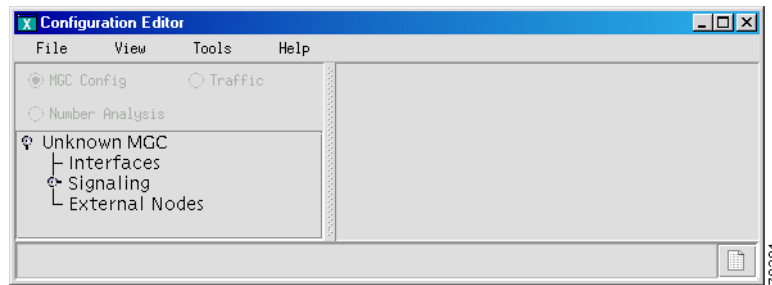
- Start VSPT standalone:
 - Log in to the VSPT server or access it from a machine with X window capability.
 - In a terminal window, change to the default directory, typically:
 - `>cd /opt/CSCOvsp26`
 - Enter the following command to start VSPT:
 - `>./vspt`
- Start VSPT from Cisco MGC Node Manager:
 - Before starting Cisco MGC Node Manager, log in as root.
 - In the Map Viewer, choose **Tools > Provisioning Tool**.

The login screen shown in [Figure 1-1](#) appears.

Figure 1-1 Login Window

Step 2 Enter your user name and password, and click **OK**.

The default user name is admin, and the password is also admin. The Welcome screen is displayed briefly during the login process, and the main window appears (see [Figure 1-2](#)).

Figure 1-2 Main VSPT Window

Exiting the VSPT

You can exit the VSPT at any time by performing one of these actions:

- Click **File > Exit**. Click **OK** at the resulting prompt.
- Click the close box in the upper right of the VSPT window. Click **OK** at the prompt.

Installing an Earlier Version of VSPT

Follow the procedure described in [“Installing VSPT Release 2.6\(1\)”](#) by selecting the version you want to install. You must install the base version before installing a patch.

Upgrading VSPT

To upgrade VSPT, you install the new version as described in the [“Installing VSPT Release 2.6\(1\)”](#) section. Depending on the version you are upgrading from, you may need to take some steps beforehand:

- Because two versions of VSPT (such as VSPT 2.3(2) and 2.6(1)) can exist on the same system, when you are upgrading, the older version is not automatically removed. If you do not want to use both versions, you can manually uninstall the older version. See the [“Uninstalling VSPT”](#) section. (However, keeping the old version is harmless.) Uninstall removes the software, but not the configuration data files.

- If you want to use configuration files created in a previous version, you must copy them. Of course, the configuration will not include components new in the 9.6(1) release.

Uninstalling VSPT

If you upgrade to VSPT Release 2.6(1) and no longer need an earlier version, follow these procedures to uninstall an earlier version.

The uninstallation process removes the `/var/opt/<CSCOvsp2x>` directory (where `2x` is the VSPT release, such as 26 for Release 2.6(1)) created by the installation process. If a directory contains a file that was not created during the installation process, it is not removed and is logged in the `uninstall.log` file. This might occur in the data and logs directories. All application data stored in the `/var/opt/<CSCOvsp2x>` directory is retained.

**Note**

Since the uninstall directory and files are removed during uninstall, *do not* change to the `/opt/CSCOvsp2x` directory to run the uninstall script.

Step 1 Enter the following commands:

```
>su -root
```

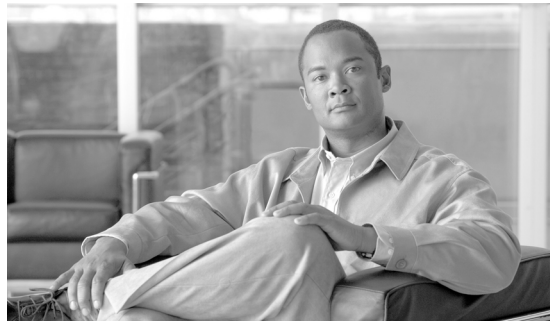
```
>cd /
```

```
>/opt/CSCOvsp2x/uninstall/uninstall
```

Step 2 Proceed with the new VSPT software installation (see the [“Installing VSPT Release 2.6\(1\)”](#) section).

**Note**

If your next installation specifies a different backup ID, you must manually delete certain files. See the [“If You Reinstall VSPT with a Different Backup ID”](#) section on page 1-5.



CHAPTER 2

Cisco Voice Services Provisioning Tool Overview

Cisco Open Packet Telephony (OPT) provides the framework for delivering voice services over packet-based data, voice, and video networks.

OPT encompasses a broad range of hardware platforms and Cisco software, delivering a continuum of voice solutions from core infrastructure to enhanced services over circuit and packet networks. The Cisco Media Gateway Controller (MGC) is at the center of Cisco OPT solutions.

Provisioning a Cisco MGC is preparing it to communicate with an SS7 network, with Cisco media gateways, and with the other components of an OPT solution. The Cisco Voice Services Provisioning Tool (VSPT) provides an easy-to-use graphical tool for provisioning Cisco MGCs.

Individual releases of the VSPT are designed to be used with specific releases of the Cisco MGC software.

VSPT Release 2.6(1) is designed to be used with Cisco MGC Release 9.6(1). If you are using a different release of the Cisco MGC software, use Table 1-1 in the *Installation Guide* to identify the release of VSPT that you need.

This chapter introduces the VSPT and provides directions for obtaining, installing, and using the software. It contains the following sections:

- [Provisioning Introduction, page 2-2](#)
- [VSPT Introduction, page 2-2](#)
- [VSPT Basics, page 2-3](#)
- [Starting the VSPT, page 2-8](#)
- [Using the VSPT, page 2-9](#)
- [Defining Users and Permissions, page 2-12](#)
- [Exiting the VSPT, page 2-13](#)

Provisioning Introduction

All solutions involving the Cisco MGC are configured through the use of one or more Cisco MGC hosts, one or more Signaling System 7 (SS7) network signaling options, and one or more media gateways that control bearer-traffic routing.

**Note**

In this document, a solution is a logical combination of Cisco hardware and software, configured to perform a specific network task.

Before starting a provisioning session, you must understand the network topology for your solution. Create a network drawing, and refer to it while configuring your network.

You should also perform the following tasks before starting a provisioning session:

- Plan your network configuration. Refer to the documentation for your solution for detailed network configuration information.
- Set up your system hardware, and install all required software. For more information, refer to “Prerequisites” in Chapter 1 of the *Installation Guide*, and the *Cisco Media Gateway Controller Software Installation and Configuration Guide (Releases 9.1 through 9.6)* at

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/software/SW2/pre97inst.html

VSPT Introduction

The VSPT allows you to import an existing configuration, modify the configuration, and export it to the same or different devices. The VSPT can also help you to provision individual call parameters. This simplifies the provisioning of a large live network.

Using the VSPT helps avoid common errors that might arise if devices are provisioned independently. It eliminates the need to enter duplicate data, and enables you to import and export configurations.

The VSPT generates configuration files necessary to provision the PGW 2200, including the following provisioning information:

- Signaling
- Trunk groups
- Trunks
- Routes
- Dial plans

During a provisioning session, the VSPT automatically generates the Man Machine Language (MML) or command line interface (CLI) scripts used to configure network elements. It assembles these commands into a batch file and deploys the file to the appropriate network device.

The VSPT allows scheduled backups and restores of configurations on the following devices:

- MGC Host—Active configuration or entire MGC system
- Catalyst 2900XL—Running-config and image in Flash
- Catalyst 5500—For switch module and RSM, configuration and image in Flash
- Catalyst 6509—For switch module and MSFC, configuration and image in Flash

- SLT 2600—Running-config and image in Flash
- BAMS Phase 3—Active configuration
- HSI Adjunct Server—Active configuration

VSPT can be installed with the CSCOk9000 package to support secure communications to SSH-enabled devices, the Cisco MGC host, the BAMS server, or the HSI server.

The following operations can use SSH:

- Provisioning of an SSH-enabled Cisco PGW 2200
- Launching of ssh rather than Telnet for communicating with SSH-enabled network devices through a command-line interface
- Use of SSH to secure X windows communications with the end-user display device
- Use of SSH in place of Telnet for the initial step (logging in to the component to be backed up and getting the configuration) in a backup and restore operation. The configuration is copied to a TFTP server using standard TFTP.

The VSPT can be deployed as an integrated component of the Cisco MGC Node Manager or as a standalone application. If it is installed on the Cisco MGC, call throughput might be affected when the VSPT is active.

VSPT typically runs on a standalone UNIX server that is also running the Cisco MGC Node Manager (Cisco MNM) and supports multiple users and provisioning sessions.

You can launch the VSPT from the managed object icon in the Cisco MNM Map Viewer. For information about Cisco MNM, refer to the *Cisco MGC Node Manager User's Guide* Release 2.6(1) at:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/prod_installation_guides_list.html

This document is designed to help you get started using the VSPT and does not include complete provisioning instructions, which are found in the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* at:

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/provisioning/guide/prvgde.html

Provisioning with the Voice Services Provisioning Tool is at:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps2272/products_user_guide_list.html

Detailed instructions for provisioning dial plans are covered in the *Cisco Media Gateway Controller Software Release 9 Dial Plan Guide* at

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/dial_plan/guide/dplan.html

Provisioning Dial Plans with the VSPT is at

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/dial_plan/guide/DP_VSPT.html

VSPT Basics

This section describes the requirements for entering provisioning data using the VSPT.

VSPT Field Definitions

Table 2-1 lists VSPT field names that correspond to system components in the Cisco MGC, and their definitions. For more information about system components, see the *Cisco Media Gateway Controller Software Version 9 Provisioning Guide*.

This table is not a comprehensive list of provisioning components. It is a description of the major fields displayed in the MGC Config window.

Table 2-1 **Field Name Definitions**

| Field Name | Definition |
|-------------------------------------|--|
| MGCP ¹ Signaling Service | Signaling service between the Cisco MGC and a media gateway. |
| IP Link for MGCP | Link for the MGCP signaling services. |
| MGC Host | Origination point code (OPC) is the address of the Cisco MGC you are provisioning. |
| Interfaces | Hardware card provisioning for the Ethernet cards in the Cisco MGC host. |

Table 2-1 *Field Name Definitions (continued)*

| Field Name | Definition |
|----------------------------------|--|
| Point Codes | |
| Originating Point Code | Originating point code (OPC) is the address for the Cisco MGC. |
| Adjacent Point Code | Address of an STP ² that sends and receives signaling messages to and from the Cisco MGC. |
| Destination Point Code (DPC) | Address of an endpoint, such as a PSTN ³ switch that carries the bearer traffic. |
| Routing Keys | |
| M3UA Route Key | Transpath NE component that represents the M3UA Routing key, a child of an OPC. |
| SUA Route Key | Transpath NE component that represents an SUA Routing key, a child of an OPC. |
| Location Label | Sets up the value for Call Limiting. |
| LinkSet | Set of links from the MGC to an endpoint, such as an adjacent STP. |
| SS7 Subsystem | Logical connection between a pair of mated STPs that allows the Cisco MGC to route through either STP to an endpoint. |
| ISUP Timer Profile | ISDN User Part (ISUP) timer profile provisioned for signaling service. |
| INservice | Intelligent network services table; can be changed at any time and is dynamically reconfigurable. |
| SS7 Path (SS7 Signaling Service) | Connection between the Cisco MGC and a specified point code. |
| SS7 Route | Route for each signaling path from the Cisco MGC to the PSTN switch through the linksets you have created to the STPs. |
| IP Route | Static IP route. |
| M3UA Route | Route for each signaling path from the Cisco MGC to the PSTN switch through the SGNode using M3UA. |
| SUA Route | Route for each signaling path from the Cisco MGC to the PSTN switch through the SGNode using M3UA. |

Table 2-1 Field Name Definitions (continued)

| Field Name | Definition |
|------------------------------|---|
| SS7 Signaling Gateway | |
| SS7 SG Nodes | SS7 signaling gateway nodes. |
| SS7 SG Subsystem | SS7 signaling gateway subsystem. |
| SS7 SG Pairs | SS7 signaling gateway pair. |
| SS7 SG Sigpaths | SS7 service to a signaling gateway. |
| Line Number Translation | Line number translation represents a line number and internal number translation and is dynamically reconfigurable. |
| SIP | SIP (session initiation protocol) service, the connection between an MGC and a SIP server. |
| Auto Congestion Ctrl | |
| Response Category | Auto Congestion Control response categories that may be associated with a trunkgroup (MGC configuration) or a signaling path (SC configuration). |
| MCL Threshold | Definition of onset and abate values of different contributing factors for Machine Congestion Level (MCL). |
| MCL Callreject | The definition of call reject percentage in different MCLs. |
| Advice of Charge | |
| Holiday | Holiday table that allows you to distinguish specific days of the year and charge them differently from the actual day of the week that the holiday falls on. |
| Charge | Charge table that defines the tariff rates (table index key for tariff.dat) and their durations. |
| Tariff | Tariff table that contains the tariff rates and scale factors. Each row is referenced by a tariff ID that call processing obtains by accessing the Charge table. |
| Meter Tariff | Meter Tariff table that is indexed by the tariff identifier retrieved from the charge table. The charge result type from generic analysis indicates which type of tariff table is accessed. |
| Pricharge | Pricharge table that stores the charge information retrieved from the charge table. It is also used to generate AOC charge information for the subscribing user. |
| Pritariff | Pritariff table that stores the tariff information retrieval from tariff table. It is also used to generate AOC charge information for the subscribing user. |
| GTD Parameters | GTD (generic transparency descriptor) that transports ISUP messages and parameters, using a generic format, between the ingress and egress Cisco PGW 2200 Signaling Controllers. |
| External Node | Any object in the network that is connected to the Cisco MGC. For example, media gateways (Cisco MGWs) and associated BSCs ⁴ . |
| ITP | Internet Transfer Point (ITP) is a signaling gateway to the SS7 network. |
| DPNSS | DPNSS ⁵ signaling path that is backhauled over IP to/from a Network Access Server (destination). |

Table 2-1 Field Name Definitions (continued)

| Field Name | Definition |
|-------------|---|
| Association | An SCTP ⁶ association represents the connection between the Cisco MGC and a Cisco access server. |
| SGP | Signaling gateway process. |
| EISUP | EISUP signaling service or signaling path. The signaling path to an externally located MGC (destination). |
| C7 IP Link | Link to the SS7 network (for example, an SSP ⁷ or STP) from the Cisco MGC through a Cisco SLT. |
| Sessionset | A pair of backhaul IP links used on the PGW to communicate with external nodes that support IPFAS or BSMV0. |
| NASPath | Network access server (NAS) signaling path, the Q.931 protocol path between the MGC and the media gateway. |

1. MGCP = Media Gateway Control Protocol.
2. STP = signal transfer point.
3. PSTN = Public Switched Telephone Network.
4. BSC = Broadband Service Card.
5. Digital Private Network Signaling System
6. SCTP = Stream Control Transmission Protocol
7. SSP = service switching point.

VSPT Data Entry Requirements

When you are entering data into the VSPT windows, follow standard MML conventions for names and descriptions. Each MML name must have the following characteristics:

- A maximum of 20 alphanumeric characters, including dashes
- No space, underscore, or special characters
- Must start with an alphabetic character

For example: `name="dpc1"`

MML descriptions can be as many as 128 characters and can include spaces and symbols. You should use a description that helps to identify the component or link that you are provisioning.

For example, for an SS7 route, which indicates the signaling path from the Cisco MGC to a switch through a linkset, you could create a description "SS7 Route to PSTN Switch A through Linkset 1."

For more information about MML, see the *Cisco Media Gateway Controller Software Release 9 MML Command Reference Guide*.

The VSPT GUI enables you to go through the provisioning process in sequence. The sequence of steps is described in the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*.

Starting the VSPT


Note

See the *Cisco Media Gateway Controller Software Version 9 Installation and Configuration Guide* for information on setting up user privileges and access rights.

To start the VSPT, use this procedure:

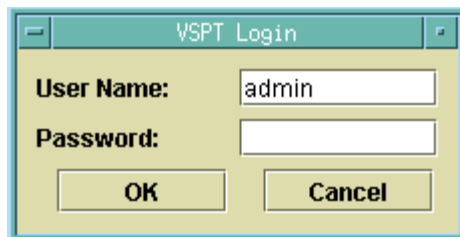
Step 1 Do one of the following to start VSPT standalone:

- Log in to the VSPT server or access it from a machine with X window capability.
- In a terminal window, change to the default directory:
- **>cd /opt/CSCOVsp26**
- Navigate to the appropriate directory if you installed the VSPT in a different location.
- Enter the following command to start the VSPT:

```
>./vspt
```

The login screen shown in [Figure 2-1](#) appears.

Figure 2-1 Login Screen

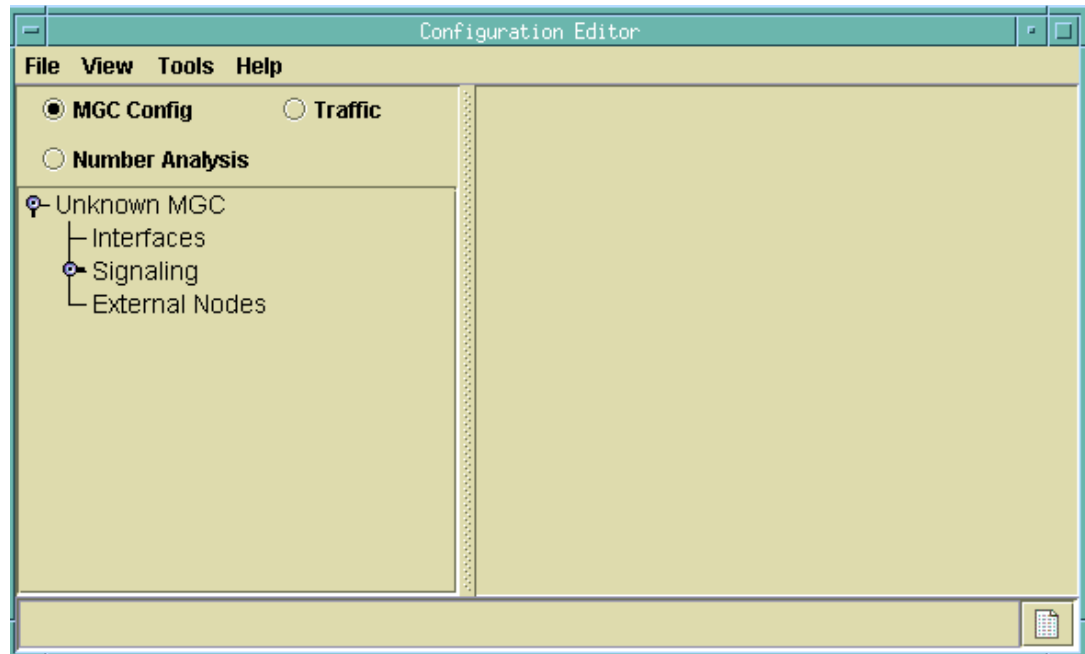


Step 2 Enter your user name and password and click **OK**.

The default user name is admin, and the password is also admin.

The Welcome screen is displayed briefly during the login process, and the Main VSPT window appears (see [Figure 2-2](#)).

Figure 2-2 Main VSPT Window



Using the VSPT

This section describes the VSPT menus and Configuration Editor views and gives instructions for using the tool functions.

Menus

The VSPT menu bar contains these menus:

- File
- View
- Tools
- Help

These menus are described in the following sections.

File Menu

Table 2-2 describes File menu commands.

Table 2-2 File Menu Commands

| Command | Description |
|---------|-----------------------------------|
| New | Begin a new configuration session |
| Open | Open an existing configuration |

Table 2-2 File Menu Commands (continued)

| Command | Description |
|---------|--|
| Import | Import an existing configuration from an MGC, or import trunk group, trunk, routing, or dial plan files into the VSPT |
| Export | Export configuration files from the VSPT to a specified directory |
| Save | <p>Save the current configuration:</p> <ul style="list-style-type: none"> • As Working: Use to save a new configuration, either a configuration imported from the Cisco PGW or a configuration created in VSPT. Use also to save modifications to an existing configuration, overwriting the last version. The configuration is saved in the /var/opt/CSCOvsp26/data/mgc/mistral directory. • As Snapshot: Use to save modifications to an existing configuration under a new name in the ARCHIVE directory. The snapshot configuration is saved in /var/opt/CSCOvsp26/data/mgc/mistral/configname/ARCHIVE. • As New Config: Use to save a modified configuration under a new name, leaving the original intact. |
| Exit | Stop any open provisioning sessions and close the VSPT. |

View Menu

Table 2-3 describes View menu commands.

Table 2-3 View Menu Commands

| Command | Description |
|------------------|--|
| MML | Show generated MML for the current configuration |
| MGW Commands | Show generated Cisco MGX 8850 commands for the current configuration |
| Trunk Group File | Show generated trunk group file for the current configuration |
| Trunk File | Show generated trunk file for the current configuration |

Tools Menu

Table 2-4 describes Tools menu commands.

Table 2-4 Tools Menu Commands

| Command | Description |
|-----------------------|---|
| Integrity Check | Check your configuration for inconsistencies and missing information. |
| Deploy | Move the configuration to one or more target hosts and Cisco media gateways (MGWs). |
| Remote Shell | Open a Telnet or SSH session. |
| MGC Viewer | View, activate, remove, and synchronize configurations on the MGC. |
| BAMS Config | View and configure a Billing and Measurements Server (BAMS). See the Billing and Measurements Server <i>User's Guide</i> for your release of BAMS for information about BAMS configuration. |
| State Operation | View and configure the state of MGC components. |
| Screening Editor | View and configure screening number provisioning. See the <i>Cisco MGC Software Release 9 Dial Plan Guide</i> for information about using the VSPT Screening Editor. |
| Audit | Audit bearer trunk information between the Cisco MGC and the BAMS. |
| Backup and Restore | Create, modify, or delete scheduled backups or restores on the Cisco MGC Host, Catalyst 2900XL, Catalyst 5500, Catalyst 6509, SLT 2600, BAMS P3, and HSI server components. |
| Administrators | |
| Change Password | Change your password. |
| User Administration | Add, modify, or delete users. |

Help Menu

Table 2-5 describes Help menu commands.

Table 2-5 Help Menu Commands

| Command | Description |
|-----------------|--|
| VSPT User Guide | View a local version of the VSPT User Guide. |
| About VSPT | View information about the current version of VSPT, including the software release number. |

Configuration Editor Views

You create, view, and modify configurations using the VSPT Configuration Editor, which has three different views.

To select a view, click one of the radio buttons at the top of the Configuration Editor window:

- **MGC Config**—MGC Configuration view. Use to add components and provision component properties.
- **Traffic**—Traffic view. Use to create customer-specific files, including trunk groups, trunks, and routing.
- **Number Analysis**—Number Analysis view. Use to provision dial plans.

In each view, the left pane displays selectable components in an Explorer-type tree view.

The right pane displays data entry fields for the selected component.

Click a component to select it. To see all of the subcomponents for the component you select, click the icon next to the component name to expand the component list.

For instructions for using the VSPT to provision components, component properties, trunk groups, trunks, and routing, see the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*.

For instructions for using the VSPT to provision a dial plan, refer to the *Cisco Media Gateway Controller Software Release 9 Dial Plan Guide*.

Defining Users and Permissions

After you install the VSPT, you define users and their respective permissions using the following procedure:

-
- Step 1** Log in to the server as root.
 - Step 2** Start VSPT, either by first starting Cisco MGC Node Manager and then starting VSPT, or by starting it standalone.
 - Step 3** Click **Tools > User Admin**.
The User Administration screen in [Figure 2-3](#) appears.

Figure 2-3 VSPT User Administration

| Username: | Permission: |
|-----------|-------------|
| admin | admin |

Username:

Password:

Permission:

- Step 4** To add a user, do the following:
- a. Enter a user name and password.
 - b. From the Permission dropdown list, select the desired permission level, **Viewer**, **User**, or **Admin**.
 - c. Click **Add**.
 - To modify a user, select the user name, change the password or permission level, and click **Modify**.
 - To delete a user, select the user name, and click **Delete**.

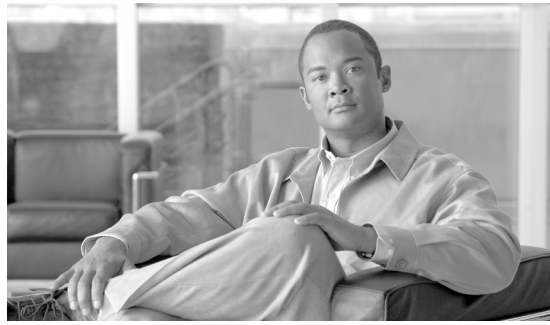
Exiting the VSPT

You can exit the VSPT by performing one of these actions:

-
- Step 1** Click **File > Exit**.
- Step 2** Click **OK** at the resulting prompt.
-

Or

-
- Step 1** Click the close box in the upper right of the VSPT window.
- Step 2** Click **OK** at the prompt.
-



CHAPTER 3

VSPT Utilities

VSPT Release 2.6(1) provides utilities to accomplish the following tasks:

- [Perform an Integrity Check, page 3-1](#)
- [View Generated Output, page 3-5](#)
- [View Generated Cisco MGW Commands, page 3-6](#)
- [Deploy a Configuration, page 3-6](#)
- [Use Telnet or ssh, page 3-11](#)
- [MGC Viewer, page 3-12](#)
- [State Operation, page 3-14](#)
- [Perform an Audit, page 3-16](#)
- [Back Up and Restore, page 3-17](#)

Perform an Integrity Check

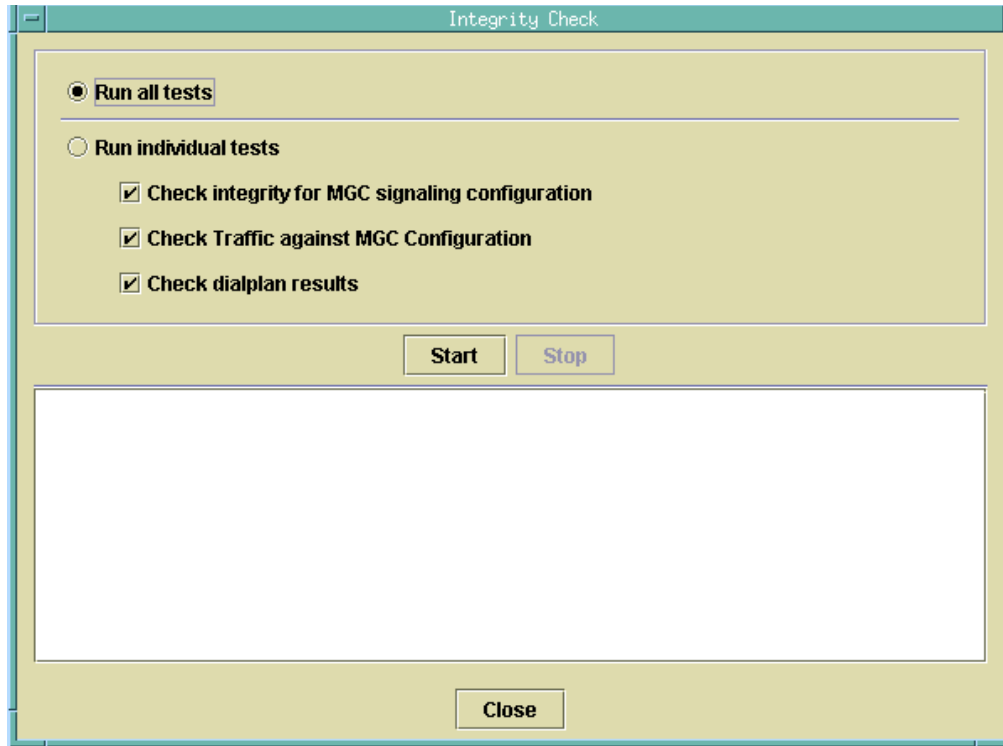
When provisioning is complete, you can perform an integrity check to prevent possible configuration errors. You can check one or all of the following:

- Integrity for the MGC signaling configuration
- Traffic against the MGC configuration
- Dial plan results

Use the following procedure to perform an integrity check of the currently open configuration:

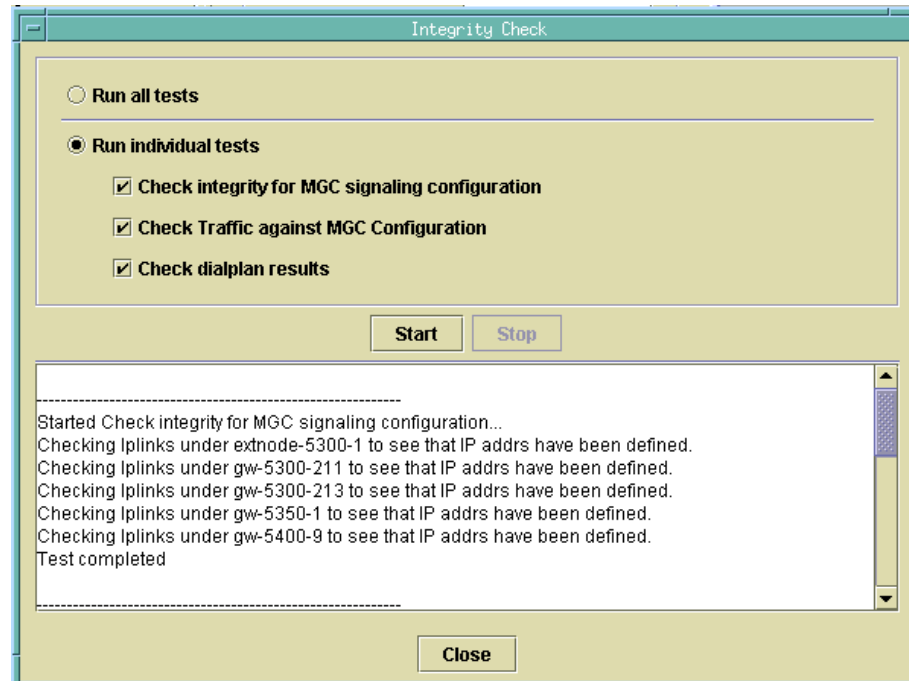
-
- Step 1** Click **Tools > Integrity Check**. The Integrity Check dialog box appears ([Figure 3-1](#)).

Figure 3-1 Integrity Check Dialog Box



- Step 2** Select the tests you want to run:
- Click **Run all tests** to run all three tests. See [Integrity Check Dialog Box Options](#) below for a description of each test.
 - To run one or more individual tests, click **Run individual tests**. All tests are checked. Uncheck the tests you do not want to run.
- Step 3** Click **Start**. VSPT runs the selected tests.
- When the tests finish, a dialog box similar to the one in [Figure 3-2](#) appears showing the results of the integrity checks.

Figure 3-2 Integrity Check Results



Integrity Check Dialog Box Options

This section describes the options in the Integrity Check dialog box.

Check Integrity for MGC Signaling Configuration

When you perform an integrity check for MGC signaling configuration, the VSPT does the following:

- Checks that the hostname is specified for MGC
- Checks that logins and passwords are specified for MGC
- Checks that MGC ipaddr's are specified
- Checks that if MGC failover is specified, the failover IP's are specified
- Checks that MGX hostname is specified
- Checks that the MGX login and password are specified
- Checks the MGX IPaddr's
- For EXTNODES where the configuration refers to an MGX, checks PeerAddr's on IPLNK to ensure that they are addresses on the specified MGX

- For IPFAS IPLNK:
 - Ensures that SigSlot/SigPort is specified
 - Checks SigSlot/SigPort on the MGX to ensure that the values are valid as specified on the MGX
 - Ensures that MGC ports and MGX ports match on the IPLNK
 - Checks that all IPLNKs under a single IPFASPATH map to the same port number

**Note**

The number of IPFAS sessions using a given port is displayed because some IPLNKs might use different port IDs.

**Note**

After Cisco MGC Release 9.3(2) and VSPT Release 2.3(2), IPFAS signaling services apply to the VISM and VXSM cards.

Check Traffic Against MGC Configuration

When you perform an integrity check of traffic against the MGC configuration, the VSPT does the following:

- When D channels are defined as FAS and NFAS PRI in the trunk group/trunk section, verifies that there are corresponding IPFASPATH signaling services with corresponding IPLNKs
- Checks if there are any defined IPFASPATH signaling services defining a D channel but no corresponding trunk group or trunk in the traffic information with a corresponding NFAS/FAS PRI
- Checks that signaling services defined for trunk groups exist in the configuration

Check Dial Plan Results

The dial plan integrity check validates that the route names used within the dial plan route results actually exist on the traffic side.

Background Information

In the dial plan, the Bdigittree maps a called digit string to select the desired result. For the Bdigittree, the digit string indicates what it should do when a call destined for the number xxx-xxxx is received. The selected value identifies what to do with the call. The result set contains results (processing actions for the call). One of the results can be a route result. Associated with the route result is the name of a route (from the traffic branch) that shows the trunk groups that exist within a route. This implies that the call should be routed onto the specified route and routed onto one of the trunk groups within the route.

View Generated Output

The VSPT automatically generates output of various types which you can view using View menu commands:

- Generated MML commands
- Generated Cisco MGW commands
- Trunk group file
- Trunk group

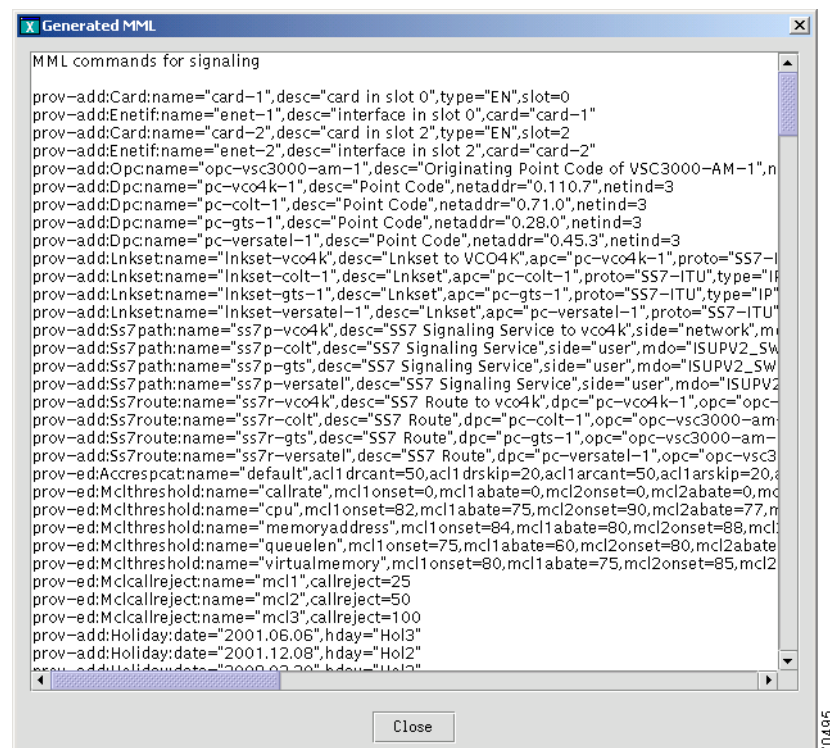
View Generated MML Commands

VSPT automatically generates MML commands to provision your Cisco MGC and saves these commands in a file to be executed when you deploy the configuration.

To view the MML commands generated from your VSPT provisioning session, click **View > MML**.

A screen displaying generated MML, similar to the one shown in [Figure 3-3](#), appears.

Figure 3-3 First Generated MML Screen



View Generated Cisco MGW Commands

To view the Cisco MGW commands generated from your provisioning session, click **View > MGW Commands** on the main VSPT menu bar. A screen with generated Cisco MGW commands, similar to that shown in [Figure 3-4](#), appears.

Figure 3-4 Example of Generated Cisco MGW Commands

```

-----[MGW CLI Commands For 10.3.4.5]-----
chidletm 20
chsyslnmd 2
y
chsysip1 10.233.20.9 0.0.0.0
chsysip2 10.233.20.73 0.0.0.0
addsonetln 9.1
chmpc 3
chndinf ## 1
chpcksrc 9 1 3 1
addmacsapprof 1 1 # 15
adddlsp 1 # # # # # # # # 0
chmgcpdname mgx8260-am-1
chmgcplocaladdr1 10.233.20.9 2427
chmgcplocaladdr2 10.233.20.73 2427
chprmgcpaddr 172.18.126.51 2427 0.0.0.0 0
chsmgcpaddr 0.0.0.0 0 0.0.0.0 0
chmgcpcore ## 1 # # 2000
addssset 1 1 1 12 3 1
addssgrp 1 1
addss1ln 1 1 1 10.233.20.9 7009 172.18.126.51 7009 1
addss1ln 1.1 1 4 # # # 1
addss1ln 2.2 1 4 # # # 1
addss1ln 3.3 1 4 # # # 1
addss1ln 4.1 16 4 # # # 1
addss1ln 5.4 1 4 # # # 1
addvport 1 1 1 1 15
addvport 1 17 1 17 15
addvport 2 32 2 0 31
addvport 3 63 2 31 31
addvport 4 1 1 1 496 512
addvport 5 94 3 30 31
adddchan 1.1 1 # 1

```

Deploy a Configuration

When you finish defining a configuration, you must deploy that configuration to the Cisco MGC. You can deploy to the Cisco MGC alone, to the Cisco MGC and one or more gateways, or to gateways only.



Note

A new configuration should not be deployed during times of peak load on the Cisco MGC.

A configuration created in VSPT can be deployed to a Cisco MGC as a new configuration or incrementally. Deploying incrementally allows you to quickly deploy modifications to an existing configuration without having to redeploy the entire configuration. VSPT also allows you to visually check the incremental commands it generates before deploying those commands to the MGC.

If the Cisco MGC has SSH enabled, you should deploy the configuration using the SSH protocol.

Deploying a New Configuration

Use the following procedure to deploy a new configuration.



Note

If you want to delete a component and plan to reuse the component name, first delete the component, deploy the session, and verify that the component name has been deleted before reusing the name.

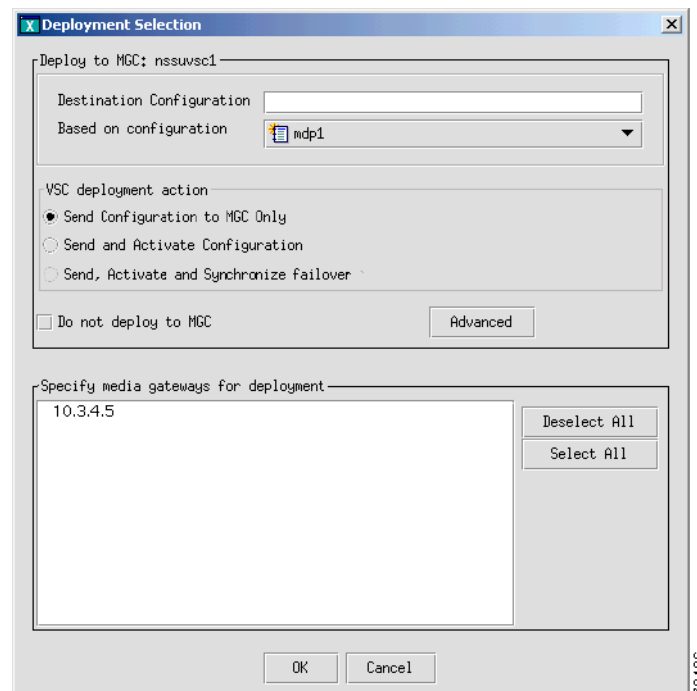
Step 1 Click **Tools > Deploy on the main VSPT menu**. The Protocol Options dialog box appears.

Step 2 Select the desired protocol:

- Choose **SSH** if SSH is enabled on the device.
- Choose **None** if SSH is not enabled on the device.

The screen shown in [Figure 3-5](#) appears.

Figure 3-5 Deploying a Configuration



Step 3 Indicate how you want to deploy the configuration:

- To deploy to the Cisco MGC only, do one of the following:
 - If you want to send the configuration to the MGC but not activate it, click the button next to **Send Configuration to MGC Only**.
 - If you want to send the configuration to the MGC and activate it, click the button next to **Send and Activate Configuration**.
 - If you have a continuous-service configuration with two Cisco MGC hosts, click the button next to **Send, Activate and Synchronize failover**. The configuration is saved on the active host and copied to the standby host. You must restart the standby server after reconfiguration to apply changes.

- To deploy to the Cisco MGC and one or more selected gateways, select one of the above three options and in Step 4 also select one or more gateways from the list in **Specify media gateways for deployment**.
- To deploy to selected gateways only (and not the Cisco MGC), check the box next to **Do not deploy to MGC** and in Step 4 select one or more gateways from the list in **Specify media gateways for deployment**.



Note If you select an option other than New, the Advanced button is enabled. For information about the options this button provides, see the [“Configuring an Incremental Deployment” section on page 3-9](#).

- Step 4** Select a configuration in the **Based on configuration** drop-down list. This list displays all existing configurations on the selected MGC and the [LAST IMPORT] and [NEW] options.
- Last Import—The VSPT compares your provisioning session to the last imported configuration and deploys only changes you have made.



Note The LAST IMPORT option allows multiple users to modify an existing configuration. However, they must each be modifying a different area of the configuration for this option to work properly.

- New—Your entire provisioning session is deployed as a new configuration.
- Existing Configurations—VSPT imports the selected configuration from the Cisco MGC, compares the differences between that configuration and your current provisioning session, and deploys changes you have made.



Note Since you are deploying a new configuration, make sure to choose the New option in the Based on configuration drop-down list.

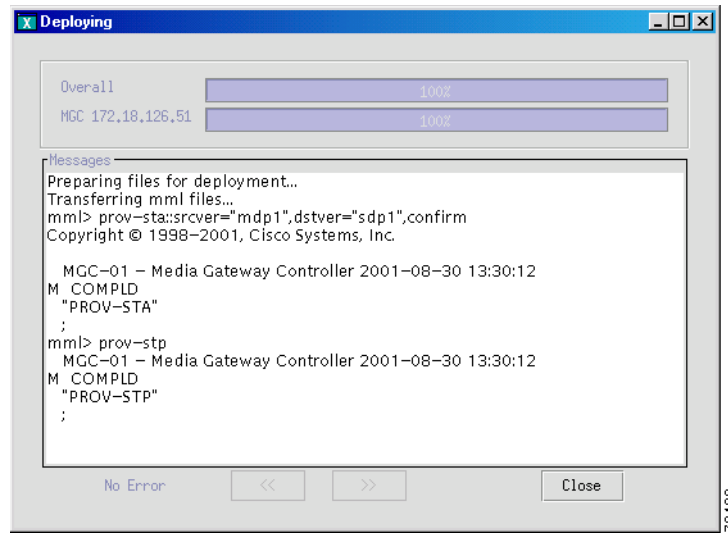
- Step 5** Select the gateways you want to deploy, if applicable.



Note To select multiple gateways, you can use standard selection methods: Shift+click to select a contiguous range, Ctrl+click to select or deselect noncontiguous gateways.

- Step 6** Click **OK**. The screen shown in [Figure 3-6](#) appears and displays the status as the current provisioning session is deployed.

Figure 3-6 Deployment Progress

**Note**

In a continuous-service configuration, the XECfgParm.dat file on each machine must be configured. If you experience problems, verify the integrity of the XECfgParm.dat files on both machines. Refer to Chapter 2, “Installing Cisco Media Gateway Controller Software,” in the *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*.

Configuring an Incremental Deployment

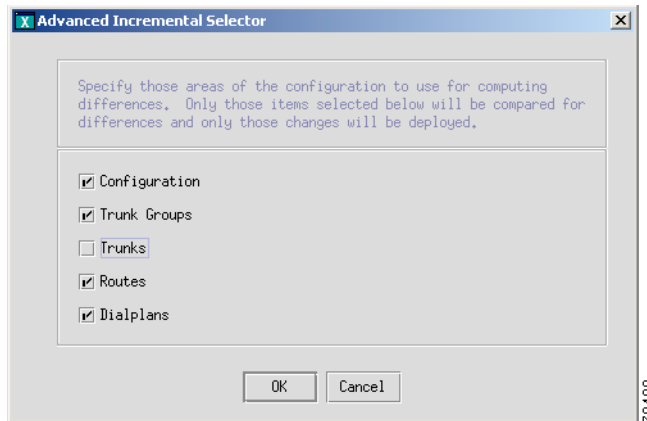
An incremental deployment allows you to modify an existing configuration and deploy only the modified areas to the Cisco MGC. Modifications can be made more quickly, and errors affecting unmodified areas are minimized. In addition, provisioning modifications made by other users in separate areas are not affected.

**Note**

The Cisco MGC does not support some incremental deployment processes. If you have a problem with an incremental deployment, examine the MML commands to ensure that you have properly configured the desired components. Modify the component presenting the problem, or cancel the deployment and redeploy the component as a new configuration.

Use the following procedure to configure an incremental deployment:

- Step 1** Follow Step 1 through Step 5 in the “Deploying a New Configuration” section on page 3-7.
- Step 2** Click **Advanced** in the window shown in Figure 3-5. The screen shown in Figure 3-7 appears.

Figure 3-7 Incremental Deployment Component Selector

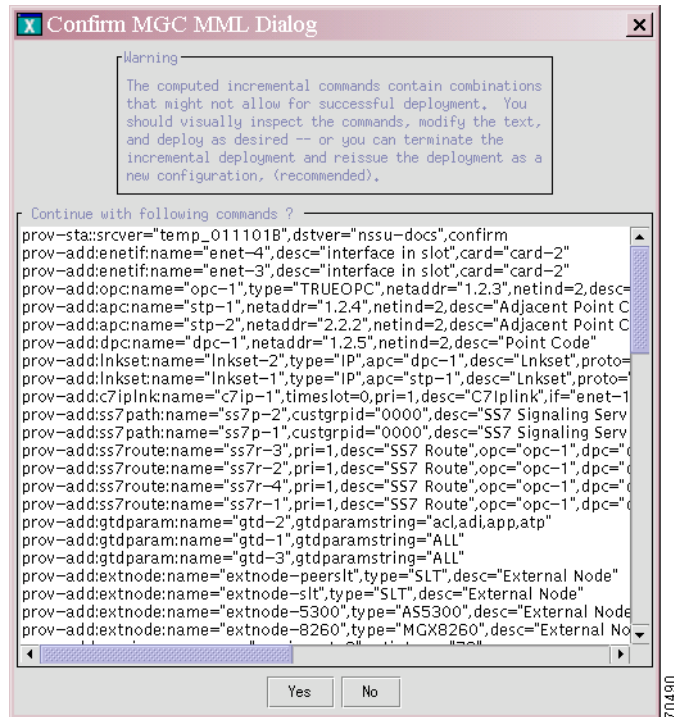
If you have only made configuration changes to one or more of the areas listed, you can direct the VSPT to compare only those areas with the current configuration, and your modifications can be deployed more quickly.



Note If you select areas in this window, be sure to include all areas that you have modified.

- Step 3** Select one or more component types to deploy, and click **OK**.
- Step 4** Go to Step 7 in the “[Deploying a New Configuration](#)” section on page 3-7, and complete the procedure described there. When you click **OK**, a screen similar to the one displayed in [Figure 3-8](#) appears.

Figure 3-8 Confirm MML Commands



- Step 5** Inspect the MML commands, modify them if desired, and click **Yes** to continue with the incremental deployment. Click **No** to reissue the deployment as a new configuration.

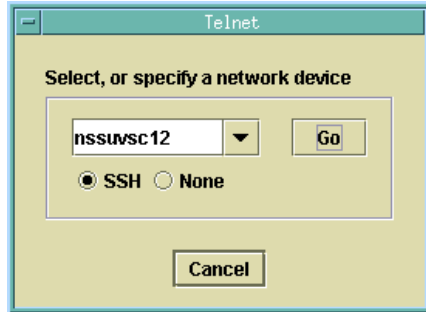
Use Telnet or ssh

VSPT provides a utility to open a Telnet session and connect directly to a device. Once you have established your Telnet connection, you can log in to the device and execute commands remotely on the device through the Telnet interface.

If you have installed SSH for VSPT and the remote device also supports SSH, you can select the ssh utility instead of Telnet.

Use the following procedure to open a Telnet or ssh session with a network device:

- Step 1** Click **Tools > Telnet**. A screen similar to that shown in [Figure 3-9](#) appears.

Figure 3-9 Select Remote Network Device

- Step 2** Select the device and connection method:
- Select a device from the dropdown list, or enter the name or IP address of a device on your network.
 - Select the connection method, either **SSH** (if the device supports it) or **None** for Telnet.
 - Click **Go**.

A Telnet or SSH window opens for you to log in to the device.

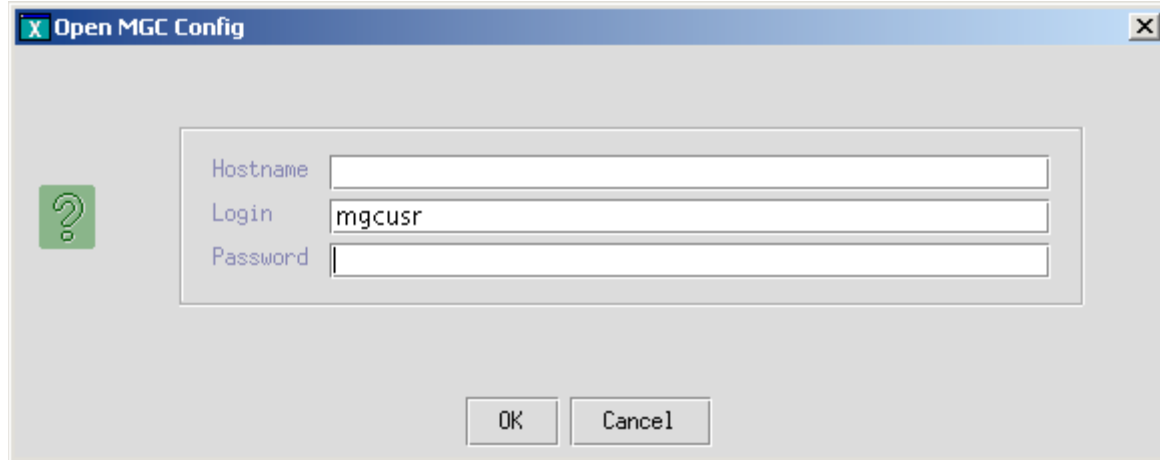
MGC Viewer

The MGC Viewer allows you to view, activate, remove, and synchronize configurations on the MGC. If you are communicating with an SSH-enabled Cisco MGC, you can use SSH instead of Telnet for the communication.

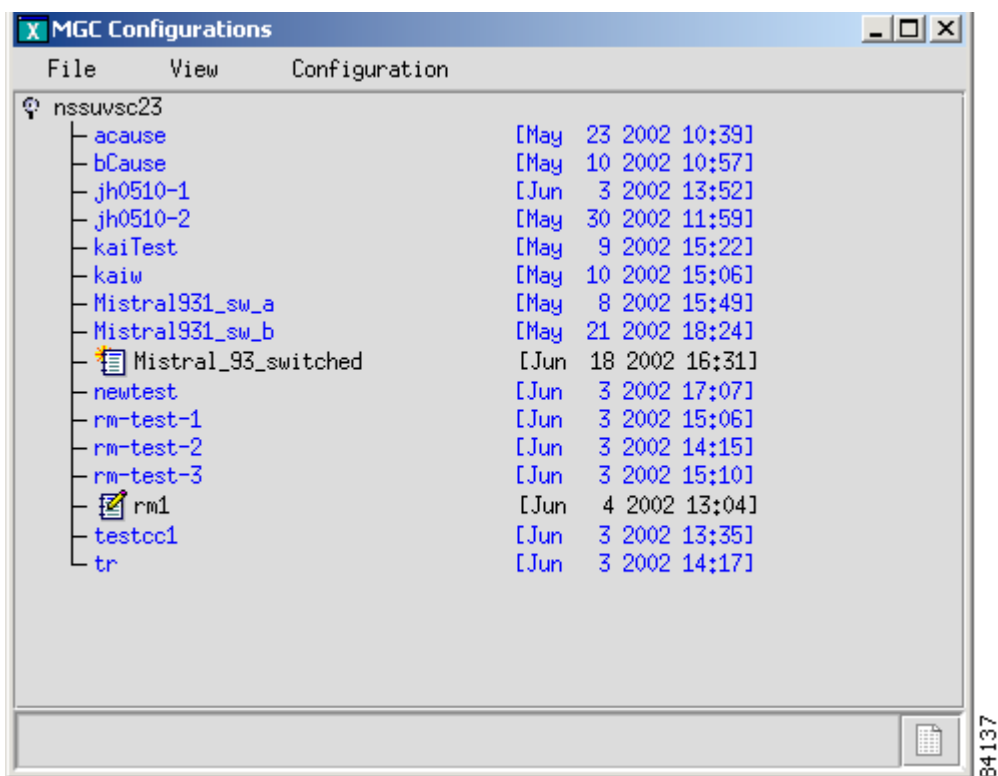
Use the following procedure to view configurations on a Cisco MGC:

- Step 1** Click **Tools > MGC viewer** on the main VSPT menu. On the MGC Configuration screen that appears, click **File > Open MGC**. The Protocol Options dialog box appears.
- Step 2** Select the desired protocol:
- Choose **SSH** if SSH is enabled on the device.
 - Choose **None** if SSH is not enabled on the device.

A screen similar to the one in [Figure 3-10](#) appears.

Figure 3-10 *elect MGCs*

- Step 3** Enter the host name of the MGC in the **Hostname** box, enter the MGC login and password, and click **OK**. A screen similar to the one in Figure 3-11 appears and lists all configurations on the specified MGC.

Figure 3-11 *MGC Configurations*

- Step 4** Click **Configuration** on the MGC Viewer menu bar, and select one of the following actions:
- Activate—Activate the configuration
 - Synchronize—Synchronize with the current configuration
 - Delete—Delete the configuration

State Operation

The State Operation utility enables you to query the active configuration on the Cisco MGC for the state of managed objects. After a query, you can modify the state of an object and apply the update to the MGC. If you are querying the state of an SSH-enabled Cisco MGC, you can use SSH instead of Telnet for the communication.

Use the following procedure to query the state of managed objects on the Cisco MGC:

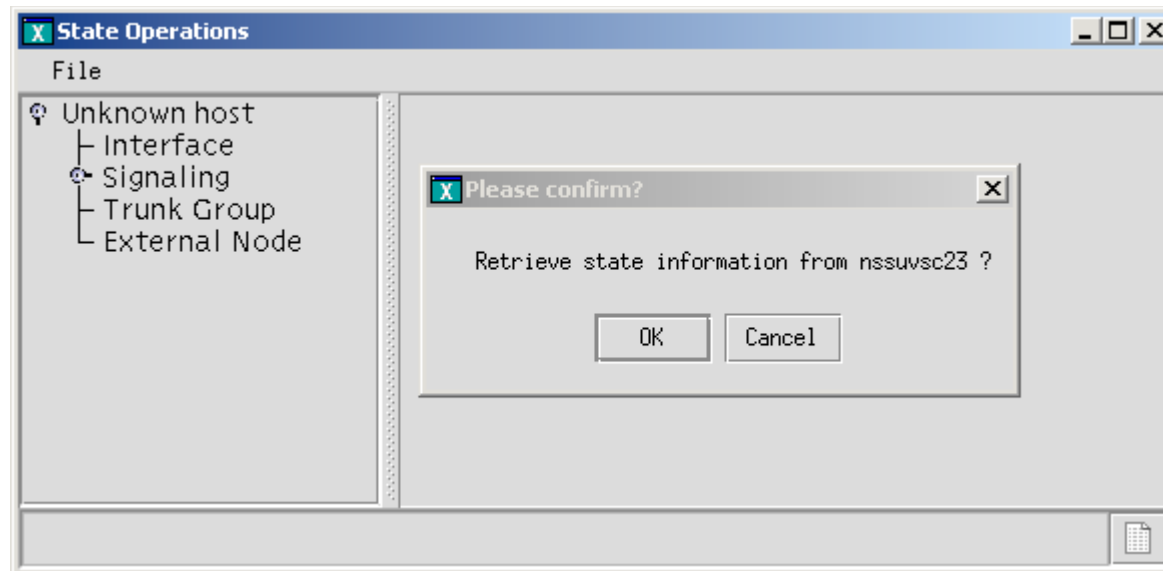
Step 1 Click **Tools > State Operation** on the main VSPT menu. The Protocol Options dialog box appears.

Step 2 Select the desired protocol:

- Choose **SSH** if SSH is enabled on the device.
- Choose **None** if SSH is not enabled on the device.

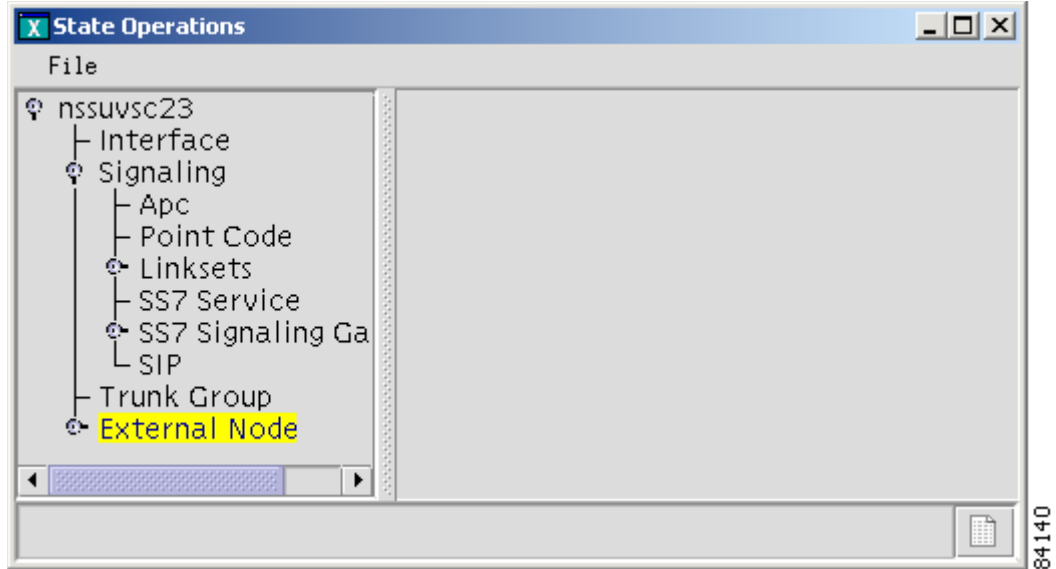
A screen similar to the one in [Figure 3-12](#) appears.

Figure 3-12 State Operation Dialog



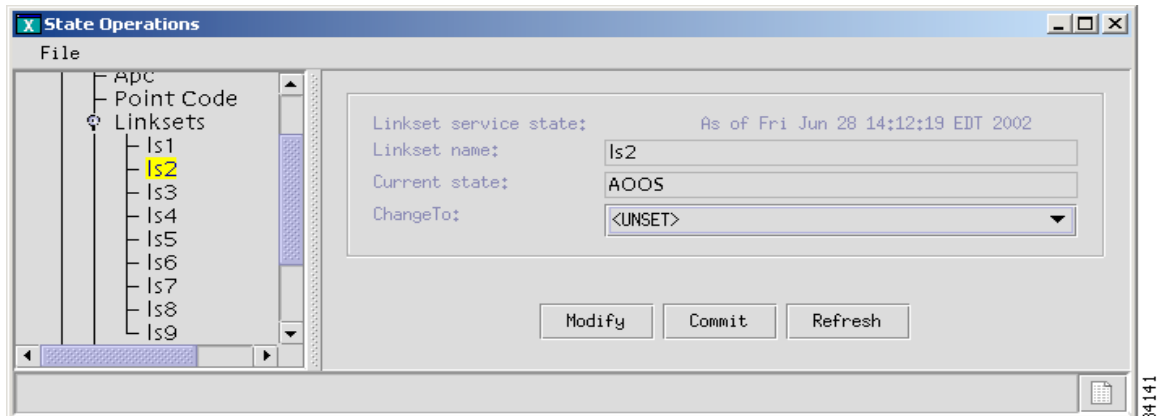
Step 3 Click OK. The VSPT queries the MGC and a screen similar to the one in [Figure 3-13](#) appears.

Figure 3-13 MGC Managed Objects



- Step 4** Expand the hierarchical tree in the left pane of the State Operations window to locate and highlight the object for which you want to know the state. In this example, we will display the state of linkset2. A window similar to the one in Figure 3-14 appears and the right pane displays information about the state of the object you selected.

Figure 3-14 State Operations



- Step 5** From this window, you can modify the state by selecting the desired state in the **ChangeTo** box. Click **Modify** to change the state in this window, and click **Commit** to change the state on the Cisco MGC. To query the object again, click **Refresh**.

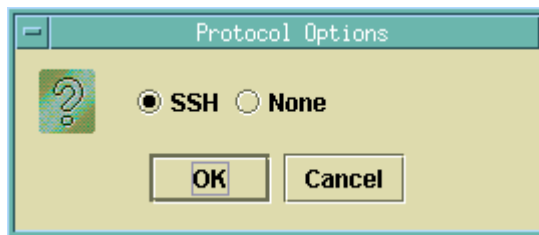
Perform an Audit

You can use an audit to ensure that both the Cisco MGC and a BAMS server supporting the Cisco MGC host have consistently configured signal paths. The audit involves examining signal path and bearer channel data on both servers, comparing the data, and reporting any differences. If you are auditing an SSH-enabled Cisco MGC, you can use SSH instead of Telnet for the communication.

Use the following procedure to perform an audit:

- Step 1** Click **Tools > Audit**. The Protocol Options dialog box appears (see [Figure 3-15](#)).

Figure 3-15 Protocol Options Dialog Box



- Step 2** Select the desired communication protocol, **SSH** (if SSH is installed on VSPT and on the devices you are auditing) or **None** (uses Telnet). Click **OK**. The Audit Dialog Box appears.
- Step 3** Enter the MGC hostname, login, and password in the top pane of the window.
- Step 4** To specify the configuration to audit, click **Select**, highlight the configuration to audit, and click **OK**.
- Step 5** Enter the BAMS hostname, login, and password in the bottom pane of the window.
- Step 6** To specify the configuration to audit, click **Select**, highlight the configuration to audit, and click **OK**.
- Step 7** Click **Audit**. A screen similar to the one displayed in [Figure 3-16](#) appears.

Figure 3-16 Audit Results

| Trunkgrp | # of Circuits | Trunkgrp | # of Circuits |
|----------|---------------|----------|---------------|
| 2182 | 120 | | |
| 4040 | 30 | | |
| 2181 | 30 | | |
| 2016 | 1710 | | |
| 4012 | 120 | | |
| 4011 | 30 | | |
| 4010 | 30 | | |
| 2012 | 120 | | |
| 2011 | 30 | | |
| 1221 | 120 | | |
| 1021 | 30 | | |
| 4032 | 1200 | | |
| 2173 | 60 | | |
| 4031 | 120 | | |
| 2172 | 30 | | |
| 4030 | 30 | | |
| 2171 | 30 | | |
| 1181 | 30 | | |
| 3012 | 210 | | |
| 1015 | 1710 | | |
| 3011 | 30 | | |
| 1012 | 60 | | |

The left pane displays the signal path and bearer channel data configured on the MGC host, and the right pane displays the same data configured on the BAMS server.

Back Up and Restore

The VSPT backup and restore tool allows you to create, modify, and delete scheduled backups and restores hourly, daily, weekly, monthly, or on demand.

You can perform backup and restore activities on any of the following devices if they have been configured for the MGC:

- MGC Host—Active configuration or entire MGC system
- Catalyst 2900XL—Running-config and image in Flash
- Catalyst 5500—For switch module and RSM, configuration and image in Flash
- Catalyst 6509—For switch module and MSFC, configuration and image in Flash
- SLT 2600—Running-config and image in Flash
- BAMS Phase 3—Active configuration
- HSI Adjunct Server—Active configuration

The backup and restore tool also provides the status of each activity and generates user-viewable status logs.

Before you begin:

- You must have selected an appropriate backup host and enabled TFTP on that machine.
- You must start VSPT from a UNIX shell with the Backup ID. The Backup ID is specified during installation. You can start VSPT in either of two ways:
 - If VSPT is launched from Cisco MGC Node Manager (Cisco MNM), you must have started the Cisco EMF client with the Backup ID. If your normal ID is different from the Backup ID, you must start a new Cisco MNM session with the Backup ID.
 - From the command line in a UNIX shell opened with the Backup ID.

About the Backup and Restore Process

The Backup process includes these main steps:

- VSPT connects to the managed component using Telnet or, if the component is SSH enabled, using a secure ssh connection. (You must have specified the component's IP address, login, and password, and you must have selected the security policy, None or SSH, in the Add... Schedule dialog box when you set up the backup.)
- The managed component makes a TFTP connection (as a client) to the TFTP server on the backup host.
- As a TFTP client, the managed component puts the configuration file onto the backup host. TFTP is used whether or not SSH is enabled. (You must have specified the backup host's IP address, Login, and Password in the Add Schedule dialog box.) TFTP must be enabled on the backup host.

The Restore process includes these main steps:

- VSPT connects to the managed component using Telnet or, if the component is SSH enabled, using a secure ssh connection.
- The managed component makes a TFTP connection (as a client) to the TFTP server on the backup host.
- As the TFTP client, the managed component gets the backup file (tar file) from the backup host and places it in a temporary location (/tmp).
- The managed component untars the tar file from the temporary location into the /opt/CiscoMGC/etc/cust_specific/ directory location.

Schedule a Backup or Restore

To schedule a backup or restore, use the following procedure:

-
- Step 1** Click **Tools > Backup and Restore** on the main VSPT menu bar. The Backup and Restore window appears listing components that can have scheduled backups.
- Step 2** Click the component for which you want to schedule a backup. In the following example, the MGC component configuration is backed up. On the right side of the window, the schedules list for that component appears.



Note If you want to perform a restore, you must have a backup file already created and available on the MGC or other managed component.

Step 3 In the Add/View Schedules pane, click **Add**. A screen similar to the one shown in [Figure 3-17](#) appears.

Figure 3-17 Add MGC Schedule



Note The fields available in the dialog box vary according to the component selected.

Step 4 In the Action field, select the action you want to perform. Choices include Backup and Restore.

Step 5 Enter information for the component you are backing up:

- Enter the IP address of the Cisco MGC.
- Enter the MGC login and password.

Step 6 In the File Name field, enter a name for the backup file.

Step 7 In the File Type drop-down list, select one of the following:

- MML Config—Backs up MML files for the active configuration on the MGC
- MGC System—Backs up MML files for the active configuration (as does MML Config), plus the Times Ten database, the XEconfigParm.dat file, and UNIX configuration files

Step 8 Enter TFTP information for the server to which you are backing up (destination for the configuration file):

- Enter the IP address of the TFTP server.
- Enter the TFTP login and password.

Step 9 Specify whether or not to use verbose log mode. Verbose mode records all commands issued by the VSPT and any system responses.

Step 10 Select whether to connect to the component you are backing up using **SSH** or Telnet (**None**).



Note The operation itself is executed with TFTP or in the case of the MGC system, FTP.

Step 11 Select the schedule type. Choices include:

- Monthly
- Daily
- Hourly
- Weekly
- Now
- Later

Step 12 Select the protocol to use for connecting to and logging in to the component you are backing up:

- Choose **SSH** to use ssh.
- Choose **None** to use Telnet.

Step 13 Select the hour and minute that the backup should begin.

Step 14 Click **OK**. The backup activity is scheduled, and the scheduled event appears in the schedule list.

After the backup has been completed, the status of the activity is immediately available. The backup file with the name you specified is available for use with VSPT.

Check Status of Backup or Restore

The VSPT generates status logs that provide information about each scheduled activity. The status log displays the following information for the activity:

- Date and time when activity began
- Success or failure
- File name on the TFTP server
- Directory of configuration files
- Image file name

If you specified verbose log mode, the status log also displays the sequence of commands issued by the VSPT and any system responses.

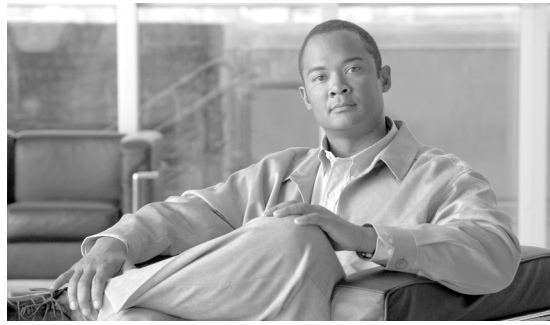
Use the following procedure to check the status of a backup or restore activity:

Step 1 In the left pane of the backup and restore tool window, click the device that has been backed up or restored. Click the **Status** tab in the right pane.

Step 2 Highlight the backup or restore for which you want information.

Step 3 Select the appropriate button for the action you want to perform. Choices are:

- Show status—Displays the log file for the activity.
 - Acknowledge—Removes the text from the Status window and deletes the log file from the server.
 - Clear—Removes the text from the Status window, but the log file remains on the server.
-



INDEX

A

- adapter
 - component [2-4](#)
- adjacent point code [2-5](#)
- APC
 - component [2-5](#)

B

- backup and restore
 - planning [1-5](#)
 - setting up [1-5](#)
- Backup host [1-6](#)
- Backup ID [1-5](#)
- basics [2-3](#)

C

- C7 IP link
 - component [2-7](#)
- committing, configuration [3-7](#)
- component
 - adapter [2-4](#)
 - APC [2-5](#)
 - C7 IP link [2-7](#)
 - external node [2-6](#)
 - ExtNode [2-6](#)
 - IP link [2-4](#)
 - linkset [2-5](#)
 - point code [2-4, 2-5](#)
 - SigMGCP [2-4](#)
 - SS7 Route [2-5](#)

SS7 SubSys [2-5](#)

SS7SubSys [2-5](#)

- configuration
 - committing [3-7](#)
 - deploying [3-7](#)
- CSCOk9000 security package [1-7](#)

D

- deploy command [2-11](#)
- deploying, configuration [3-7](#)
- descriptions [2-7](#)
- destination point code [2-5](#)

E

- enabling TFTP on Backup host [1-6](#)
- exit command [2-10](#)
- exiting the VSPT [2-13](#)
- exiting VSPT [1-9](#)
- ExtNode component [2-6](#)

F

- field definitions [2-3](#)
- field names [2-3](#)

H

- Help menu [2-9](#)

I

installing SSH on VSPT [1-7](#)
 IP link component [2-4](#)

L

linkset component [2-5](#)
 logging in to the VSPT [2-8](#)
 logging in to VSPT [1-8](#)
 login screen [1-8, 2-8](#)

M

menu
 Session [2-9](#)
 View [2-9](#)
 menus [2-9](#)

N

Number Analysis tab [2-12](#)

O

origination point code [2-4](#)

P

planning
 for backup and restore [1-5](#)
 point oode component [2-5](#)

S

secure communication [3-14](#)
 secure communications [3-16](#)
 security enhancements

 installing on VSPT [1-7](#)
 Session menu [2-9](#)
 setting up
 backup and restore [1-5](#)
 SigMGCP component [2-4](#)
 SS7 route
 component [2-5](#)
 SS7SubSys component [2-5](#)
 SSH [3-12, 3-14, 3-16](#)
 installing on VSPT [1-7](#)
 ssh or Telnet [3-11](#)
 SSH-related VSPT toggles [1-7](#)
 starting
 VSPT [1-8, 2-8](#)
 STP [2-5](#)
 STP, mated pair [2-5](#)
 sync command [2-10](#)

T

tabs
 Number Analysis [2-12](#)
 Telephony Controller [2-12](#)
 Traffic [2-12](#)
 Telephony Controller tab [2-12](#)
 Telnet or ssh [3-11](#)
 TFTP
 enabling on Backup host [1-6](#)
 tips, before provisioning [1-2](#)
 Traffic tab [2-12](#)

U

user ID for Backup [1-5](#)

V

View menu [2-9](#)

VSPT

- exiting [1-9, 2-13](#)
- logging in [1-8, 2-8](#)
- starting [1-8, 2-8](#)

VSPT Backup ID [1-5](#)

VSPT basics [2-3](#)

VSPTfield definitions [2-3](#)

VSPT overview [2-2](#)

X

X windows [1-8, 2-8](#)

