Cisco Voice Services Provisioning Tool User Guide, Release 2.7(3)

March 18, 2010

CONTENTS

Preface

This preface describes the objectives of this document and explains how to find additional information on related products and services. It contains the following sections:

Document Objectives

This document provides information you need to get started with the Cisco Voice Services Provisioning Tool, Release 2.7(3).

Note The Cisco Voice Services Provisioning Tool (VSPT) 2.7(3) is no longer available as a free download at Cisco.com. In order to use Cisco VSPT 2.7(3), you are required to purchase the Cisco Media Gateway Controller (MGC) Node Manager (MNM) 2.7(3) Media Kit which includes both Cisco VSPT 2.7(3) and Cisco MNM 2.7(3). All the Cisco VSPT patches and releases prior to Release 2.7(3) are available at

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

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.

Related Documentation

The documents that contain information related to the Cisco VSPT are at the following URL:

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

The documents that contain information related to the Cisco PGW 2200 Softswitch are at the following URL:

http://www.cisco.com/en/US/products/hw/vcallcon/ps2027/tsd_products_support_series_home.html

You can also find the *Cisco PGW 2200 Softswitch Documentation Map* at the following URL:

http://www.cisco.com/en/US/products/hw/vcallcon/ps2027/products_documentation_roadmaps_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Document Change History

Table 1   Change History

Subject	Document No, Change Date	Change Summary
Updated to document features new in Cisco VSPT 2.7(3) P5	OL-8907-06, July, 2009	Reorganized the chapters. Updated Table 1-4 in Chapter 1. Updated the section, "State Operation" and "Backup and Restore" in Chapter 4.
Updated to document features new in Cisco VSPT 2.7(3) P4	OL-8907-05, January, 2009	Updated Table 1-2 Field Definitions in Traffic Window (Switched-mode Cisco PGW 2200 Softswitch), added Table 1-3 Field Definitions in Traffic Window (Nailed-mode Cisco PGW 2200 Softswitch), and updated Table 1-4 Field Definitions in Number Analysis Window in Cisco VSPT Field Definitions in Chapter 1.

Table 1   Change History (continued)

Subject	Document No, Change Date	Change Summary
Updated to document features new in Cisco VSPT 2.7(3) P3	OL-8907-04, March, 2008	Updated Table 1-1 Field Definitions in MGC Config Window, and added Table 1-2 Field Definitions in Traffic Window and Table 1-3 Field Definitions in Number Analysis Window in Cisco VSPT Field Definitions in Chapter 1.
Updated to document features new in Cisco VSPT 2.7(3) P2	OL-8907-03, October, 2007	Updated Table 1-1 Field Name Definitions in Cisco VSPT Field Definitions in Chapter 1.
Updated to document features new in Cisco VSPT 2.7(3)	OL-8907-02, October, 2007	Updated to document new features in Cisco VSPT Release 2.7(3).
Updated to document features new in Cisco VSPT 2.6(1)	OL-8097-01, July 2005	Updated to document new features in Cisco VSPT Release 2.6(1).
Updated to document features new in Cisco VSPT 2.5(2)	OL-6449-01, August 2004	Updated to document to reflect name change and separation from Cisco MGC Node Manager.
Updated to document features new in MNM-PT 2.4(1)	OL-3871-01, June 2003	Updated to document features new in Cisco PGW 2200 Softswitch software Release 9.4(1) and to reflect name change and tighter integration with Cisco MGC Node Manager.
Updated to document features new in Cisco VSPT 2.3(2)	OL-3541-01, December 05, 2002	Updated to document features new in Cisco PGW 2200 Softswitch software Release 9.3(2).
Updated to document features new in Cisco VSPT 2.3(1)	OL-1910-02, July 30, 2002	Updated to document HSI adjunct, 6509 LAN Switch, and integrated SLT.
Initial release, Cisco VSPT 2.2	OL-1910-01, February 15, 2002	Initial online release

Cisco Voice Services Provisioning Tool Overview

The Cisco PGW 2200 Softswitch provides the framework for delivering voice services over packet-based data, voice, and video networks.

The Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch is at the center of the Cisco PGW 2200 Softswitch solutions.

Provisioning a Cisco PGW 2200 Softswitch is preparing it to communicate with an SS7 network, with Cisco media gateways, and with the other components of a Cisco PGW 2200 Softswitch solution. The Cisco Voice Services Provisioning Tool (Cisco VSPT) provides an easy-to-use graphical tool for provisioning the Cisco PGW 2200 Softswitches.

Individual releases of the Cisco VSPT are designed to be used with specific releases of the Cisco PGW 2200 Softswitch software. Cisco VSPT Release 2.7(3) is designed to be used with Cisco PGW 2200 Softswitch Release 9.7(3). If you are using a different release of the Cisco PGW 2200 Softswitch software, see the "Determine the Correct Provisioning Tool Release" section on page 2-1 to identify the release of Cisco VSPT that you need.

The Cisco MGC Node Manager (MNM) provides fault and performance management for the Cisco PGW 2200 Softswitch, Cisco HSI, Cisco BAMS, Cisco Catalyst switches and Cisco IP Transfer Point LinkExtender (ITP-L). Cisco VSPT Release 2.7(3) is shipped with Cisco MNM 2.7(3). The Cisco VSPT Release 2.7(3) is no longer available as a free software for downloading. Previous versions of the Cisco VSPT and all the Cisco VSPT patches are still available for free downloading from Cisco.com to customers who have a Cisco.com subscription. See the following URL

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

Cisco VSPT Release 2.7(3) supports FlexLM license control which provides license management for the Cisco VSPT. The licenses are installed after the Cisco VSPT installation. The license installation is described in Chapter 2, "Installing Cisco VSPT".

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

- Provisioning Introduction, page 1-2
- Cisco VSPT Introduction, page 1-2
- Provisioning Data in Cisco VSPT, page 1-3

Provisioning Introduction

All solutions involving the Cisco PGW 2200 Softswitch are configured through the use of one or more Cisco PGW 2200 Softswitch 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 a list of the components you want to provision, including component names, IP addresses, properties, and other parameters, and refer to the drawing and the list while configuring your network.

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

- Plan your network configuration. See the documentation for your solution for detailed network configuration information.

- Set up your system hardware, and install all required software. For more information, see Chapter 1 of the *Cisco PGW 2200 Softswitch Hardware Installation Guide - Releases 7 & 9* at

    http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/hardware/hrdwrnst.html

    , and the *Cisco Media Gateway Controller Software Installation and Configuration (Release 9.7)* at

    http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/installation/software/SW1/97.html

Cisco VSPT Introduction

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

Using the Cisco 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 Cisco VSPT generates configuration files that you need to provision the Cisco PGW 2200 Softswitch, including the following provisioning information:

- Signaling

- Trunk groups

- Trunks

- Routes

- Dial plans

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

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

- Cisco PGW 2200 Softswitch host—Active configuration or entire Cisco PGW 2200 Softswitch system

- Catalyst 2900XL—Running-config and image in Flash
- Catalyst 5500—For switch module and Route Switch Module (RSM), configuration and image in Flash
- Catalyst 6509—For switch module and Multilayer Switch Feature Card (MSFC), configuration and image in Flash
- Cisco ITP-L 2600—Running-config and image in Flash
- Cisco BAMS Phase 3—Active configuration
- Cisco HSI Adjunct Server 4.3—Active configuration

Cisco VSPT can support secure communications to SSH-enabled devices, the Cisco PGW 2200 Softswitch host, the Cisco BAMS server, or the Cisco HSI server.

The following operations can use SSH:

- Provisioning of an SSH-enabled Cisco PGW 2200 Softswitch.
- Launching of SSH rather than Telnet for communicating with SSH-enabled network devices through a CLI.
- 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. TFTP is used for MML configuration backup and restore. FTP is used for system backup and restore.

The Cisco VSPT can be deployed as an integrated component of the Cisco MNM or as a standalone application. If it is installed on the Cisco PGW 2200 Softswitch, call throughput might be diminished when the Cisco VSPT is active.

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

You can launch the Cisco VSPT from the managed object icon in the Cisco MNM Map Viewer. For information about Cisco MNM, see the *Cisco MGC Node Manager User Guide* at

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

This document is designed to help you get started using the Cisco VSPT and does not include complete provisioning instructions, which are found in Chapter 3, Provisioning with VSPT, 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/R9GUI.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 Chapter 3, Provisioning Dial Plans with VSPT, 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/DP_VSPT.html

Provisioning Data in Cisco VSPT

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

Cisco VSPT Field Descriptions

Table 1-1 lists Cisco VSPT field names that correspond to system components in the Cisco PGW 2200 Softswitch, and their descriptions. When you use Cisco VSPT to provision the Cisco PGW 2200 Softswitch, you can find useful information in this table. 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. The fields are displayed using indents to show the subordination that you can see in the MGC Config window.

Table 1-1   Field Descriptions for Entries in the MGC Config Window

Field Name	Description
MGC Host	Basic information for Cisco PGW 2200 Softswitch and Cisco BAMS, for example, hostname, IP addresses, Cisco PGW 2200 Softswitch mode, and so forth.
Point Codes	
Originating Point Code (OPC)	The address for the Cisco PGW 2200 Softswitch.
Adjacent Point Code (APC)	Address of an STP[1] that sends and receives signaling messages to and from the Cisco PGW 2200 Softswitch.
Destination Point Code (DPC)	Address of an endpoint, such as a PSTN[2] 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	Call limiting value settings.
LinkSet	Set of links from the Cisco PGW 2200 Softswitch to an endpoint, such as an adjacent STP.
SS7 Subsystem	Logical connection between a pair of mated STPs that allows the Cisco PGW 2200 Softswitch 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 that can be changed at any time and is dynamically reconfigurable.
SS7 Path (SS7 Signaling Service)	Connection between the Cisco PGW 2200 Softswitch and a specified point code.
SS7 Route	Route for each signaling path from the Cisco PGW 2200 Softswitch to the PSTN switch through the linksets you have created to the STPs.
IP Route	Static IP route.
M3UA Route	This field contains routes using M3UA for each signaling path from the Cisco PGW 2200 Softswitch to the PSTN switch through the SG node. On Release 2.7(3) Patch 3, external node type VXSM support is added.

Table 1-1   Field Descriptions for Entries in the MGC Config Window (continued)

Field Name	Description
SUA Route	This field contains routes using SUA for each signaling path from the Cisco PGW 2200 Softswitch to the PSTN switch through the SG node.
SS7 Signaling Gateway	
SS7 SG Nodes	SS7 signaling gateway nodes.
SS7 SG Pairs	SS7 signaling gateway pair.
SS7 SG Subsystem	SS7 signaling gateway subsystem.
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	
DNS	DNS server-related information, including IP address, cache size, and other parameters.
SIP Links	IP Links for the SIP signaling service.
SIP Port	Added in Release 2.7(3) Patch 3. This field contains SIP ports on an existing siplnk.
Auto Congestion Ctrl	
Response Category	Auto Congestion Control response categories that can be associated with a trunk group or a signaling path.
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 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 defines the tariff rates (table index key for tariff.dat) and their durations.
Tariff	Tariff table contains 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 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 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 stores the tariff information retrieved from tariff table. It is also used to generate AOC charge information for the subscribing user.
GTD Parameters	GTD (generic transparency descriptor) transports ISUP messages and parameters, using a generic format, between the ingress and egress Cisco PGW 2200 Softswitch Signaling Controllers.
TOS	Type of service.

Table 1-1   *Field Descriptions for Entries in the MGC Config Window (continued)*

Field Name	Description
External [3]Nodes	
Association	An SCTP association represents the connection between the Cisco PGW 2200 Softswitch and a Cisco access server.
Association for H.248	Added in Release 2.7(3) Patch 2. An SCTP[4] link for H.248 signaling service.
BRI	A QSIG/Q.931 over BRI backhaul signaling service
C7 IP Link	Links to the SS7 network (for example, an SSP[5] or STP) from the Cisco PGW 2200 Softswitch through a Cisco ITP-L.
CTI	CTI signal path.
DPNSS	DPNSS[6] signaling path is backhauled over IP to/from a Network Access Server (destination).
EISUP	EISUP signaling service or signaling path. The signaling path to an externally located Cisco PGW 2200 Softswitch (destination).
H.248 Signaling Service	Added in Release 2.7(3) Patch 2. Another signaling service (in addition to MGCP) between the Cisco PGW 2200 Softswitch and the VXSM media gateways.
IPFAS	An IPFAS signaling service.
IP Link for H.248	Added in Release 2.7(3) Patch 2. A UDP[7] link for H.248 signaling service.
IP Link for MGCP	Links for the MGCP signaling services.
ITP	Internet Protocol Transfer Point (ITP) is a signaling gateway to the SS7 network.
LI	Lawful Intercept (LI) mediation device signal path.
MGCP[8] Signaling Service	Signaling service between the Cisco PGW 2200 Softswitch and a media gateway.
NASPath	Network access server (NAS) signaling path. The Q.931 protocol path between the Cisco PGW 2200 Softswitch and the media gateway.
Rapath	RADIUS[9] accounting server signal path.
Raserver	RADIUS accounting server.
Sessionset	A pair of backhaul IP links used on the Cisco PGW 2200 Softswitch to communicate with external nodes that support IPFAS or BSMV0.
SGP	Signaling gateway process.
CTI Manager	CTI manager details, including IP addresses, ports and other parameters.
AXL Server	AXL server details, including IP addresses, ports and other parameters.

1. STP = signal transfer point.
2. PSTN = public switched telephone network.
3. External nodes = Any object in the network that is connected to the 12. For example, media gateways (Cisco MGWs) and associated Broadband Service Cards (BSCs).
4. SCTP = Stream Control Transmission Protocol.
5. SSP = service switching point.
6. DPNSS = Digital Private Network Signaling System.

7. UDP = User Datagram Protocol.

8. MGCP = Media Gateway Control Protocol.

9. RADIUS = Remote Authentication Dial-in User Service.

Table 1-2 describes the major fields displayed in the Traffic window when the Cisco PGW 2200 Softswitch is in switched mode. Table 1-3 describes the major fields displayed in the Traffic window for nailed-mode Cisco PGW 2200 Softswitches.

Table 1-2   Field Descriptions for Entries in the Traffic Window (Switched-mode Cisco PGW 2200 Softswitch)

Field Name	Description
Profiles	A trunk group profile allows you to define a collection of trunk group properties and associate trunk groups with those properties.
Trunk Groups	A trunk group is a collection of DS0 circuits arranged so that dialing a single trunk number provides access to the entire trunk group.
Trunks	A trunk is an individual circuit (DS0) on a T1/E1.
Ipinmapping	Added in Release 2.7(3) Patch 3. This is an IP IN Trunk mapping which maps an inbound SIP or H.323 call to a trunk group.
CodecString	A series of codec choices separated by semicolons
BearerCap	Bearer capability is a string of Transmission Medium Requirement (TMR) values less than or equal to 96 characters (0 through 9 and "only") that are separated by semicolons.Users can define a required bearer capability (ies) and include the definitions. The Cisco PGW 2200 Softswitch can preferentially route calls with a specific bearer capability.
ATMProfiles	ATM profiles are used on the Cisco PGW 2200 Softswitch to change the network Service Level Agreement.
Routing	
Routes	A route is a collection of trunk groups associated with the same set of dialed digits. The route is a communication path identified for a particular destination.
Route Lists	A route list is a collection of names of routes/trunk groups that go to the same endpoint.
Descriptions	Conditional route description is used in the time-of-day routing, which provides the capability for the user to select a route list or an entry point into the percentage based routing based on the time of day, and day of week.Users can add time conditional routing descriptions to connect the entries of the conditional route description to route list names or percentage based routing names.
Conditional Routing	Conditional routing allows the Cisco PGW 2200 Softswitch to use different conditional route descriptions for weekdays and holidays. Users apply the descriptions to distribute the traffic load on Monday through Sunday and other specified holidays.
Percentage Routing	The percentage routing permits the user to distribute the traffic load across route lists based on assigned percentage values.

Table 1-3   *Field Descriptions for Entries in the Traffic Window (Nailed-mode Cisco PGW 2200 Softswitch)*

Field Name	Description
Trunks	A trunk is an individual circuit (DS0) on a T1/E1.

Table 1-4 describes the major fields displayed in the Number Analysis window.

Table 1-4   *Field Descriptions for Entries in the Number Analysis Window*

Field Name	Description
Dial Plans	
Customer Group ID	A unique four-character alphanumeric identifier for the dial plan.
Results	
Digmodstring	The digit modification string is used to modify numbers in either the A-number (calling party number) or the B-number (called party number).
BC	When you change the BC information elements (IEs) in the outgoing Initial Address Message (IAM), an ISUP call from the PSTN can be translated to a fax call in the Global System for Mobile Communications (GSM) network based on the dialed called party number. You need to create the BC table and add a BCMOD result in order to change the BC IEs in the outgoing IAM.
HLC	When you change the High Layer Compatibility IE in the outgoing IAM, the Cisco PGW 2200 Softswitch translates an ISUP call from the PSTN to a data call in the GSM network. You need to create the HLC table and add the HLCMOD result in order to change the HLC IEs in the outgoing IAM.
Customervpnid	The customer VPN ID overwrites the configured VPN ID in the incoming trunk groups or sigPaths.
Resultset	The result of analysis might require that an action be taken. A result set defines that action or a set of actions.
DefResultset	Defines a default result set to be used when a digit string is not configured in the B digit tree.
Screening	Call screening is a type of analysis done on the digit string to determine if the call is to be accepted or rejected.
Service	The service names in the Service table are defined by the users to indicate services for screening that are available to the users. You must define a service before you add a B-number-triggered call screening.
Triggers	
Achgorigin	The Cisco PGW 2200 Softswitch returns a result with CHARGEORIGIN result type during the A-number analysis if the Advice of Charge (AOC) feature is enabled on the ingress trunk group or sigpath. You need to add A-number charge origin data before you add a result with CHARGEORIGIN result type.
Adigtree	The Adigtree table is the analysis table for calling numbers (A-numbers). You add data to it by defining an entry for each digit in the digit string.

Table 1-4   *Field Descriptions for Entries in the Number Analysis Window (continued)*

Field Name	Description
A-Num Dp Selection	A-number dial plan selection. The dial plan selection table provides the functionality to select a new dial plan based on the customer group ID and the full A-number.
Bdigtree	The Bdigtree table is the analysis table for called numbers. You add data to it by defining an entry for each digit in the digit string.
Cause	The Cause table lists the cause codes generated when a call is either rejected or cleared by the system. The cause for release can be either a result type (from either B-number analysis or cause analysis) or a failure (generated during call processing).
Cliprefix	Advanced screening on the Cisco PGW 2200 Softswitch requires the provisioning of the calling line identification prefix table. The CLI prefix parameter allows you to associate a CLI prefix with a specific customer group. If an incoming call matches the CLI prefix parameter, you can apply certain dial plan functions to it.
CliIpAddr	The advanced screening and modification on CLI IP address parameter allows you to associate an IP address with a CLI set name. If the source IP address of the incoming call message matches the provisioned IP address, the Cisco PGW 2200 Softswitch selects the CLI set. If that incoming call matches a CLI prefix defined in that cliset, the Cisco PGW 2200 Softswitch selects the customer group ID of that CLI prefix entry to continue the number analysis.
CPC	Pre-analysis is the first phase in the Cisco PGW 2200 Softswitch number analysis. CPC analysis is the first stage of the pre-analysis. Users configure a CPC table so that it links CPC values received from the incoming call setup message to a result.
DP Selection	The dial plan selection functionality enables the Cisco PGW 2200 Softswitch to go from one dial plan to another one under specific conditions. You need to add dial plan selection data before you use this function.
H323iddivfrom	The h323iddivfrom parameter allows you to associate an H.323 ID with a specific customer group. If an incoming call matches the H.323 ID parameter, you can apply certain dial plan functions to it.
Location	The Location table is used to identify an associated result set. This table is accessed from the cause table through the location index. The location index is used to refer to a block of 16 entries in the location table. The location value is used as an offset into the location block. An action can be associated with a specific location value by associating a result set with the value in the location block.
Anoa	The NOA table is used to define actions to be taken, based on the incoming A-number NOA.
Bnoa	The NOA table is used to define actions to be taken, based on the incoming B-number NOA.
Anpi	The A-number NPI table is used to identify an associated result set. This table is accessed from the A-number NOA table through the NPI block.

Table 1-4   Field Descriptions for Entries in the Number Analysis Window (continued)

Field Name	Description
Bnpi	The B-number NPI table is used to identify an associated result set. This table is accessed from the B-number NOA table through the NPI block.
RTE Holiday	The holiday table allows you to select specific days of the year to be routed differently from the actual day of the week that a holiday occurs on.
TMR	The TMR analysis is the second stage in Pre-analysis that enables analyzing the TMR value in the IAM or Setup message. For example, this would allow the Cisco PGW 2200 Softswitch to set different media gateway bearer capabilities within the network.
TNS	The TNS analysis is the fourth stage in Pre-analysis that enables analyzing the transit network selection parameter information (or the Carrier Selection parameter information) as received in the incoming message.
Global Items	
Announcement	The ToneAndAnnouncement database table contains all the announcement details. An announcement ID identifies the announcement.
Porttbl (Moved to Tools> Advanced Number Editor in Release 2.7(3))	The ported number table determines if the B-number has been ported to another network. If the presented B-number is found in this table, the call is rerouted to the recipient network.
Script	To support the MGCP scripting feature on the Cisco PGW 2200 Softswitch, you need to provision a script table.
FullNumberTrans	The full number translation table is used for the result type NUM_TRANS. The NUM_TRANS result type is returned from A-number (the calling number) or B-number analysis (the called number), indicating that one or more numbers encountered require full replacement. The full number translation table contains all the replacement information.
Crptmesg	Added in Release 2.7(3) Patch 5. Call reporting messages are customized data that can be included in a call detail record through the provisioning of the CALL_REPORT result type.
Termtbl (Moved to Tools> Advanced Number Editor in Release 2.7(3))	The number termination table contains B-numbers. If the presented B-number is found in this list, the call is routed to the RouteID associated with the corresponding digit string.
Testline	The test line table is used to specify the delay, loop requirement, duration, and other parameters for test calls.

Cisco VSPT Data Entry Requirements

When you are entering data into the Cisco 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 PGW 2200 Softswitch to a switch through a linkset, you could say, "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 Cisco 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*.

C H A P T E R 2

Installing Cisco VSPT

Revised: March 18, 2010, OL-8907-06

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

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

Individual releases of Cisco VSPT are designed to be used with specific releases of the Cisco PGW 2200 Softswitch software. See the "Determine the Correct Provisioning Tool Release" section on page 2-1 to identify the release of the Cisco VSPT that you need.

This chapter provides directions for installing the Cisco VSPT. It contains the following sections:

- Installing Cisco VSPT Release 2.7(3), page 2-2
- Installing an Earlier Version of Cisco VSPT, page 2-9
- Upgrading Cisco VSPT, page 2-9
- Uninstalling Cisco VSPT, page 2-10

Determine the Correct Provisioning Tool Release

You must install the provisioning tool release that is compatible with your Cisco PGW 2200 Softswitch and Cisco BAMS software. Select the correct provisioning tool version by referring to Table 2-1. The following versions are included on the Cisco MGC Node Manager CD. Check the applicable release notes for possible later patches.

Table 2-1   Cisco VSPT and Cisco MGC Software Version Compatibility

Cisco VSPT Release	Cisco PGW 2200 Softswitch Software Release	Cisco BAMS Software Release
Cisco VSPT 2.7(3)	Cisco PGW 2200 Softswitch Release 9.7(3)	Cisco BAMS Phase 3 (3.20 and 3.30)

Table 2-1   Cisco VSPT and Cisco MGC Software Version Compatibility (continued)

Cisco VSPT Release	Cisco PGW 2200 Softswitch Software Release	Cisco BAMS Software Release
Cisco VSPT 2.6(1)	Cisco PGW 2200 Softswitch Release 9.6(1)	Cisco BAMS Phase 3 (3.13)
Cisco VSPT 2.5(2)	Cisco PGW 2200 Softswitch Release 9.5(1)	Cisco BAMS Phase 3 (3.13)

Installing Cisco VSPT Release 2.7(3)

The Cisco VSPT Release 2.7(3) can be installed on the Solaris 8 and Solaris 10 (Opteron and Sparc) platform.

Before installing Cisco VSPT Release 2.7(3), verify the following:

- You want to provision the Cisco PGW 2200 Softswitch running Cisco PGW 2200 Softswitch software Release 9.7(3). If you are provisioning an earlier version, see the "Determine the Correct Provisioning Tool Release" section on page 2-1.

- 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 selected an installation configuration, one of the options described in the "Determine the Correct Provisioning Tool Release" section on page 2-1.

- You have decided if you are installing SSH for secure communications with SSH-enabled components.

Note A Cisco VSPT installation must be carried out from the Cisco 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 Descriptions of the properties and values contained in Cisco VSPT are included in Appendix A of the Cisco *Media Gateway Controller Software Release 9 Provisioning Guide* and Table 2-2 of this document. Review this information before you begin provisioning, and keep it available for reference during provisioning.

To install Cisco VSPT Release 2.7(3), follow this procedure:

Step 1 Verify that the requirements listed in the "Determine the Correct Provisioning Tool Release" section on page 2-1 have been met.

Step 2 Open an X 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: sentenv DISPLAY <hostname>:<display name>
- In sh or ksh: DISPLAY=<hostname>:<display name> ; export $DISPLAY

✎

Note   The default value for the display number is 0. Replace the value <hostname> with the hostname of your machine.

Step 5 Insert the Cisco VSPT 2.7(3) CD in the CD-ROM drive.

Step 6 Change the directory using the following command.

    # **cd /cdrom/cdrom0/dart**

Step 7 Enter the following command to run the installation script:

    # **./setup**

The Cisco VSPT InstallShield Wizard opens, displaying the Welcome window.

Step 8 Click **Next**.

The License Agreement window displays.

Step 9 Accept the license agreement and click **Next**.

The Destination Folder window displays, indicating the default destination directory.

Step 10 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 11 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 2-5 for more information. This is applicable only if you are conducting backup operations. All other features of Cisco VSPT function without the entering of a backup user ID.

The Ready to Install window displays.

Step 12 Click **Install Now**.

Cisco VSPT 2.7(3) installation takes place and the Installation Summary window displays upon completion.

Step 13 Click **Exit**.

The Cisco VSPT InstallShield Wizard closes.

Step 14 If you are using the Cisco VSPT Backup and Restore feature, enable TFTP and FTP on the backup server. See the "Planning and Setting Up for Backup and Restore" section on page 2-4.

Step 15 If you are installing SSH for Cisco VSPT, see the "Enabling SSH on Cisco VSPT" section on page 2-6.

Step 16   Install FlexLM license control. (See the "Installing and Updating FlexLM License Control" section on page 2-7.)

Step 17   Go on to the "Starting Cisco VSPT" section on page 2-9.

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

Table 2-2   Provisioning Tool Installation Files and Directories

File or Directory	Description
/opt/CSCOvsp27	
vspt	Provisioning tool application script
/classes	Class and property files
/config	Configuration related to license
/docs	—
/expect	A tool used for automating interactive applications such as telnet, ftp, passwd, fsck, rlogin, tip, and so on
/flexlm	FlexLM software
/help	Online help files
/images	Images or logos used in Cisco VSPT
/jre/	Java Runtime Environment
/netscape	Netscape web browser files
/uninstall	Uninstall script directory
/utils	Utilities for Cisco VSPT
/version	Provisioning Tool version
/var/opt/CSCOvsp27 (home directory)	
/data	Configuration files
/logs	Log files
/etc	XML files

Note   The files and directories listed in Table 2-2 are for the most recent version of Cisco VSPT. Your directory structure may be different if you are using an older version. You can verify that all these files and directories are installed to make sure the installation is successful.

Planning and Setting Up for Backup and Restore

You typically use Cisco VSPT Backup to back up the configuration on a supported component, such as a Cisco PGW 2200 Softswitch, 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 Softswitch host, Cisco VSPT logs in to the Cisco PGW 2200 Softswitch host, copies the configuration, and the Cisco PGW 2200 Softswitch transfers it to the backup host using Trivial File Transfer Protocol (TFTP). The backup host must have TFTP and FTP enabled.

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

- Specify a Backup User ID During Installation, page 2-5
- Select a Backup Host, page 2-5
- Enable TFTP on the Backup Host, page 2-6

Specify a Backup User ID During Installation

During Cisco VSPT installation, you are prompted for a backup ID. The backup ID is the UNIX ID of a user account authorized to use Cisco 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, Cisco VSPT must be started from a UNIX shell with the backup ID, in either of two ways:

- If Cisco 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 Cisco VSPT with a Different Backup ID

If you reinstall Cisco 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 the directory using the following command:

```
# cd /var/opt/CSCOvsp27/logs/
```

Step 3   Delete these two files, now.log and testValidTFTP, using the following command:

```
# rm now.log
# rm 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 Softswitch host
- A separate machine used for backups

✎

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

Enable TFTP on the Backup Host

Cisco VSPT uses TFTP as the transfer utility to transfer configuration files from the Cisco PGW 2200 Softswitch (or Cisco 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 Cisco 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
```

Enabling SSH on Cisco VSPT

SSH on Cisco VSPT is available on Cisco PGW 2200 Softswitch Release 9.7(3) on a Solaris 10 platform. Use the following command to check if you have the SSH on Cisco VSPT installed:

```
# pkginfo | grep ssh
```

```
system      SUNWsshcu                        SSH Common, (Usr)
system      SUNWsshdr                        SSH Server, (Root)
system      SUNWsshdu                        SSH Server, (Usr)
system      SUNWsshr                         SSH Client and utilities, (Root)
system      SUNWsshu                         SSH Client and utilities, (Usr)
```

> ✍
>
> **Note**   If you cannot see the above output, please use the Solaris CD to install the SSH.

If you want to enable root access to the Cisco VSPT via SSH, follow these steps:

Step 1   Edit the /etc/ssh/sshd_config file and change the value of the PermitRootLogin parameter from no to yes.

Step 2   Save your changes to this file.

Step 3   Identify the process ID of the sshd process by entering the following command:

```
ps -ef | grep ssh
```

Step 4   Restart the sshd process and activate your changes by entering the following command:

```
kill -1 process_id
```

The process_id is the ssh process ID number identified in the previous step.

Installing and Updating FlexLM License Control

Installing FlexLM License Control

Cisco VSPT 2.7(3) supports the FlexLM license control. After the Cisco VSPT is installed, you must install licenses before starting the Cisco VSPT.

Obtaining FlexLM License File

There are two ways to obtain the FlexLM license file for Cisco VSPT 2.7(3).

If the Cisco VSPT is installed alone or with the Cisco PGW 2200 Softswitch, you get the license file after the purchase of the Cisco MGC Node Manager with Cisco VSPT included.

Follow the steps below to obtain a license key file.

Step 1   Go to Cisco Product License Registration site at

https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet

Step 2   Fill in the Product Authorization Key (PAK). The PAK is provided on the Cisco EMF product CD sleeve.

Step 3   Click **Submit**.

Step 4   Verify that the product information shown on the screen is correct, and then click **Continue**.

Step 5   Select the version of the Cisco VSPT product you are licensing in the Version number field.

Step 6   Enter the hostname of the server where the Cisco VSPT product is installed. You can obtain the server's hostname by entering the hostname command at the server's command line prompt.

✎

Note The server hostname must not include a period (.).

Step 7 Enter the host ID of the server where the Cisco VSPT product is installed. (The host ID is a hexadecimal string that identifies the system; it is not the IP address.) You can obtain the server's host ID by entering the **hostid** command at the server's command line prompt.

Step 8 Read the End-User License Agreement and select **I Accept**. You must accept to get a license.

Step 9 Verify the registrant information shown on the screen.

Step 10 Click **Continue**.

Step 11 Verify the summarized information and click **Submit**.
The license request is submitted. The Cisco VSPT license key file is returned to you as an e-mail attachment.

If the Cisco VSPT is installed with CMNM, the license file for Cisco VSPT is the same as the license file for Cisco EMF license. You can find the related information in the section, "Obtain a Cisco EMF License", in the *Cisco Media Gateway Controller Node Manager Installation Guide, 2.7(3)* at

http://www.cisco.com/en/US/docs/net_mgmt/mnm/2.7.3/install/guide/MNM_install_273.html

Installing FlexLM License File

Perform the following command to install the license file:

```
# cp license.lic /opt/CSCOvsp27/config/licenses/
```

Updating FlexLM License Control

You need to update the license file when the old license file expires.

Because Cisco VSPT can be installed alone or installed with the CMNM or the Cisco PGW 2200 Softswitch, steps for updating FlexLM license control vary depending on different Cisco VSPT installation.

If the Cisco VSPT is installed alone or with Cisco PGW 2200 Softswitch, follow the steps below to update licenses:

Step 1 Stop the licenses server:

```
# /opt/CSCOvsp27/flexlm/avlm stop
```

A list of running license managers is displayed if you have several running servers.

Step 2 Enter the number of the ATL license manager if you have several running servers.

Step 3 Get updated license file:

```
# cp license.lic /opt/CSCOvsp27/config/licenses/
```

If the Cisco VSPT is installed with CMNM, follow the steps below to update licenses:

Step 1 Stop the licenses server:

```
# /opt/CSCOvsp27/flexlm/avlm stop
```

A list of running license managers is displayed if you have several running servers.

Step 2   Enter the number of the ATL license manager if you have several running servers.

Step 3   Get updated license file:

```
# cp license.lic /opt/CSCOvsp27/config/licenses/
# cp license.lic /opt/cemf/config/licenses/
```

Step 4   Restart the CEMF.

```
# /opt/cemf/bin/cemf stop
# /opt/cemf/bin/cemf start
```

Starting Cisco VSPT

See the "Starting Cisco VSPT" section on page 2-9.

Exiting Cisco VSPT

See the "Exiting Cisco VSPT" section on page 2-9.

Installing an Earlier Version of Cisco VSPT

Follow the procedure described in "Installing Cisco VSPT Release 2.7(3)" section on page 2-2 by selecting the version you want to install. You must install the base version before installing a patch.

Upgrading Cisco VSPT

To upgrade Cisco VSPT, you install the new version as described in the "Installing Cisco VSPT Release 2.7(3)" section on page 2-2. Depending on the version you are upgrading from, you may need to take some steps beforehand:

- Because two versions of Cisco VSPT (such as Cisco VSPT 2.6(1) and 2.7(3)) 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 Cisco VSPT" section on page 2-10. (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 to the new version. Of course, the configuration will not include components new in the 9.7(3) release.

Uninstalling Cisco VSPT

Uninstalling an Earlier Version of Cisco VSPT

The uninstallation process removes the /var/opt/<CSCOvsp2x> directory (where *2x* is the Cisco VSPT release, such as 27 for Release 2.7(3)) 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.

If you upgrade to Cisco VSPT Release 2.7(3) and no longer need an earlier version, follow these procedures to uninstall the earlier version.

Step 1   Enter the following commands:

```
# su - root
# cd /
# /opt/CSCOvsp2x/uninstall/uninstall
```

Step 2   Proceed with the new Cisco VSPT software installation (see the "Installing Cisco VSPT Release 2.7(3)" section on page 2-2).

Note   If your next installation specifies a different backup ID, you must manually delete two files, now.log and testValidTFTP. See the "If You Reinstall Cisco VSPT with a Different Backup ID" section on page 2-5.

Uninstalling Cisco VSPT Release 2.7(3)

Perform the following steps to uninstall Cisco VSPT Release 2.7(3):

Step 1   Log in as root.

Step 2   Go to the root directory:

```
# cd /
```

Step 3   Uninstall Cisco VSPT Release 2.7(3) using the following command:

```
# /opt/CSCOvsp27/uninstall/uninstall
```

Step 4   (Optional) If Cisco VSPT is installed with Cisco MNM, restart CEMF

```
# /opt/cemf/bin/cemf stop
# /opt/cemf/bin/cemf start
```

Getting Started with Cisco VSPT

Revised: March 18, 2010, OL-8907-06

This chapter provides directions for starting and using the Cisco VSPT. It contains the following sections:

Starting Cisco VSPT

To start the Cisco VSPT, use this procedure.

Note   If you encounter any font problems in Cisco VSPT, start the VNC server using
-fb /user/openwin/lib/X11/fonts/misc/ as the command arguments.

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

- Start Cisco VSPT standalone.

    - Log in to the Cisco VSPT server or access it from a machine with X window capability.

    - In a terminal window, change to the default directory:

        ```
        >cd /opt/CSCOvsp27
        ```

Note   Navigate to the appropriate directory if you installed the Cisco VSPT in a different location.

    - Enter the following command to start the Cisco VSPT:

        ```
        >./vspt
        ```

- Start Cisco VSPT from Cisco Media Gateway Controller Node Manager (CMNM).

    - Before starting Cisco MNM, log in as root.

- Right-click the Cisco PGW 2200 Softswitch host object in the Map Viewer and choose **Tools > Voice Service Provisioning Tool (VSPT)**.

> ✎
> **Note** If you start the Cisco VSPT from Cisco MNM, the correct Cisco VSPT version is automatically launched to match the selected Cisco PGW 2200 Softswitch. You must have that version of Cisco VSPT installed before you launch it on the Cisco PGW 2200 Softswitch host object from Cisco MNM.

The login screen shown in Figure 3-1 appears.

Figure 3-1   Login Screen
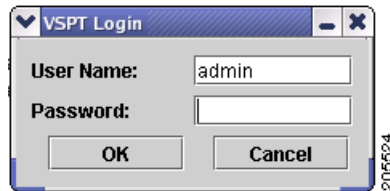
Step 2   Enter your user name and password and click **OK**.

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

> ✎
> **Note** Cisco VSPT checks the license and provides the expiry date for that license after you provide the login information.

The Welcome screen is displayed briefly during the login process, and the Main VSPT window appears (see Figure 3-2).

Figure 3-2   **Main Cisco VSPT Window**
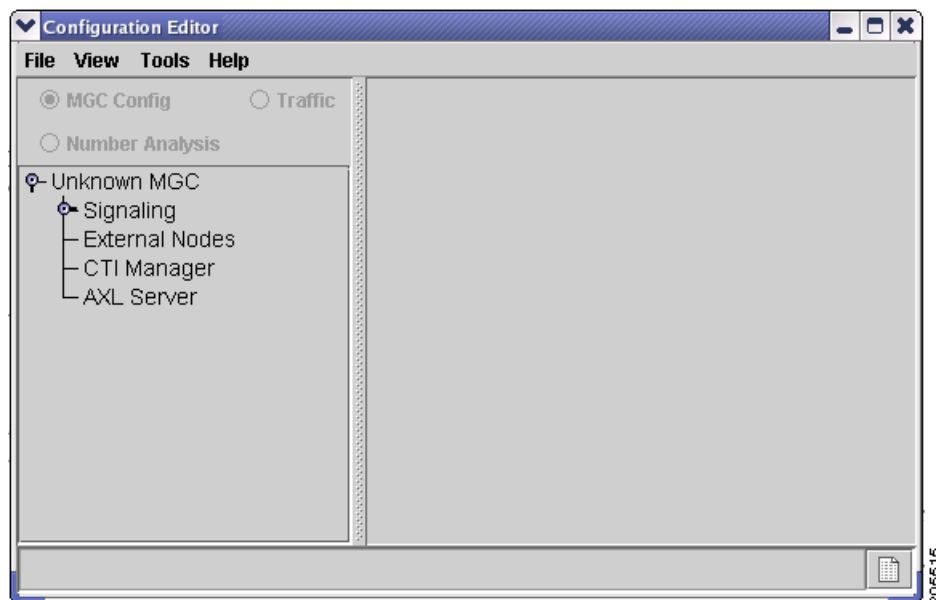
Using Cisco VSPT

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

Menus

The Cisco VSPT menu bar contains these menus:

- File
- View
- Tools
- Help

These menus are described in the following sections.

File Menu

Table 3-1 describes File menu options.

Table 3-1   *File Menu Options*

Menu Option	Description
New	Begin a new configuration session.
Open	Open an existing configuration.

Table 3-1   File Menu Options (continued)

Menu Option	Description
Import	Import an existing configuration from a Cisco PGW 2200 Softswitch, or import trunk group, trunk, routing, or dial plan files into the Cisco VSPT.
Export	Export configuration files from the Cisco VSPT to a specified directory.
Save	Save the current configuration using one of the following options: • **As Working**—Use to save a new configuration, either a configuration imported from the Cisco PGW 2200 Softswitch or a configuration created in Cisco VSPT. Use also to save modifications to an existing configuration, overwriting the last version. The configuration is saved in the /var/opt/CSCOvsp27/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/CSCOvsp27/data/mgc/mistral/*configname*/ARCHIVE. • **As New Config**—Use to save a modified configuration under a new name, leaving the original unchanged.
Exit	Stop any open provisioning sessions and close the Cisco VSPT.

View Menu

Table 3-2 describes View menu options.

Table 3-2   View Menu Options

Menu Option	Description
MML	Show generated MML 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 3-3 describes Tools menu options.

Table 3-3   Tools Menu Options

Menu Option	Description
Integrity Check	Check your configuration for inconsistencies and missing information.
Deploy	Move the configuration to one or more target hosts.
Remote Shell	Open a Telnet or SSH session.
MGC Viewer	View, activate, remove, and synchronize configurations on the Cisco PGW 2200 Softswitch.
BAMS Config	View and configure a Cisco Billing and Measurements Server (BAMS). See the *Cisco Billing and Measurements Server User's Guide* for your release of Cisco BAMS for information about its configuration.

Table 3-3   Tools Menu Options (continued)

Menu Option	Description
State Operation	View and configure the state of Cisco PGW 2200 Softswitch components.
Advanced Number Editor	View and configure screening numbers, ported number table, and the number termination table. See the *Cisco MGC Software Release 9 Dial Plan Guide* for information about using the Cisco VSPT Advanced Number Editor.
Audit	Audit bearer trunk information that moves between the Cisco PGW 2200 Softswitch and the Cisco BAMS.
Backup and Restore	Create, modify, or delete scheduled backups or restores on the Cisco PGW 2200 Softswitch Host, Catalyst 2900XL, Catalyst 5500, Catalyst 6509, Cisco ITP-L 2600, Cisco BAMS P3, and Cisco HSI server components.
Administrators	
Change Password	Change your own password.
User Admin	Add, modify, or delete users.

Help Menu

Table 3-4 describes Help menu options.

Table 3-4   Help Menu Commands

Menu Option	Description
VSPT User Guide	View a local version of the *Cisco VSPT User Guide*.
About VSPT	View information about the current version of Cisco VSPT, including the software release number.

Configuration Editor Views

You create, view, and modify configurations using the Cisco 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—Cisco PGW 2200 Softswitch 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 on using the Cisco VSPT to provision components, component properties, trunk groups, trunks, and routing, see the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide*.

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

Defining Users and Permissions

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

Step 1   Log in to the server as root.

Step 2   Start Cisco VSPT, either by first starting Cisco MGC Node Manager and then starting Cisco VSPT, or by starting the Cisco VSPT standalone.

Step 3   Click **Tools > User Admin**.

The User Administration screen in Figure 3-3 appears.

Figure 3-3   Cisco VSPT User Administration
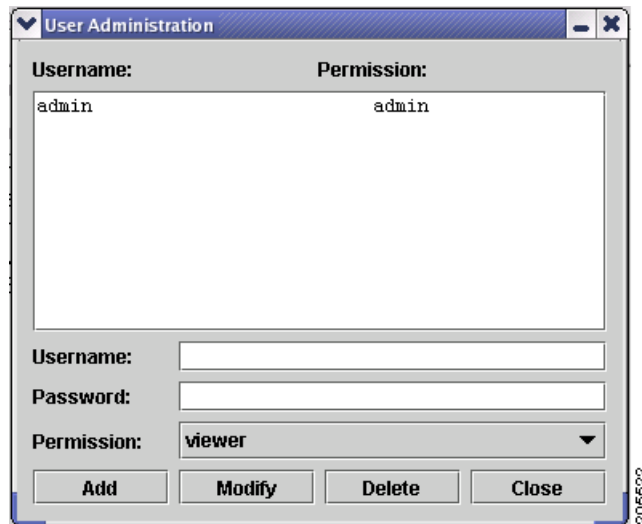
Step 4   To add a user, do the following:

a.   Enter a user name and password.

b.   From the Permission dropdown list, select the desired permission level, **Admin**, **User**, or **Viewer**.

Note   **Admin**—Can create, modify, and delete users. This type of user has full read and write access to all of the configurations on the Cisco BAMS and the Cisco PGW 2200 Softswitch.
User—Cannot create, modify, or delete users. This type of user has full read and write access to all of the configurations on the Cisco BAMS and the Cisco PGW 2200 Softswitch.
Viewer—Cannot create, modify, or delete users. This type of user has the read-only access to the Cisco PGW 2200 Softswitch configurations saved on the Cisco VSPT but has no access to the Cisco BAMS configurations saved on the Cisco VSPT. A viewer cannot access the configurations on the remote Cisco BAMS or the Cisco PGW 2200 Softswitch.

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 Cisco VSPT

You can exit the Cisco VSPT by choosing **File > Exit** or by clicking the X button in the upper right of the main window.

Cisco VSPT Utilities

Revised: March 18, 2010, OL-8907-06

Cisco VSPT Release 2.7(3) provides the following utilities:

View Generated Output

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

- Generated MML commands
- Trunk group file
- Trunk file

View Generated MML Commands

Cisco VSPT automatically generates MML commands to provision your Cisco PGW 2200 Softswitch and saves these commands in a file to be executed when you deploy the configuration.

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

A screen displaying generated MML commands, similar to the one shown in Figure 4-1, appears.

Figure 4-1 *Generated MML Window*
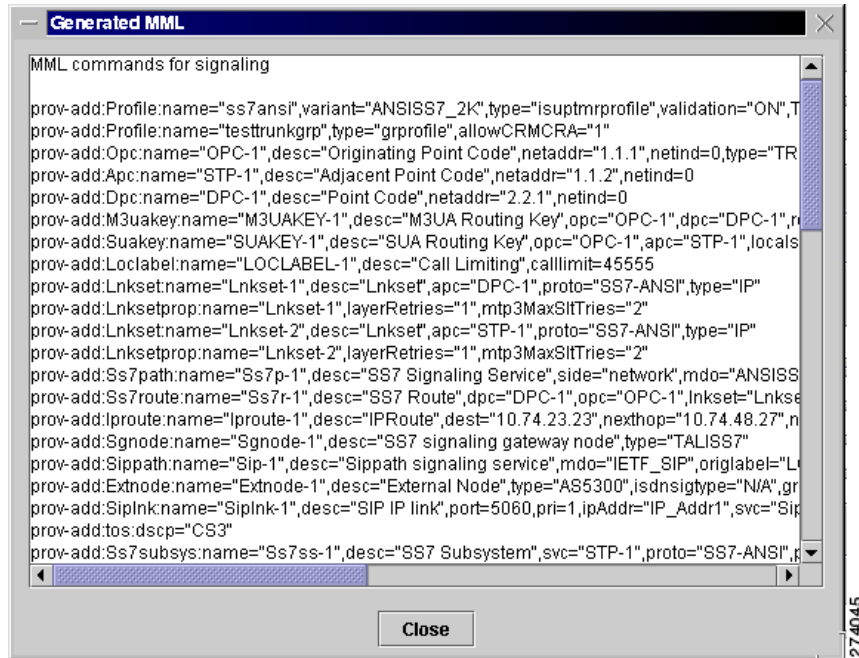
View Generated Trunk Group File

To view the trunk group file generated from your Cisco VSPT provisioning session, click **View > Trunk Group File**.

A screen displaying the generated trunk group file, similar to the one shown in Figure 4-2, appears.

Figure 4-2 *Generated Trunk Group File Window*
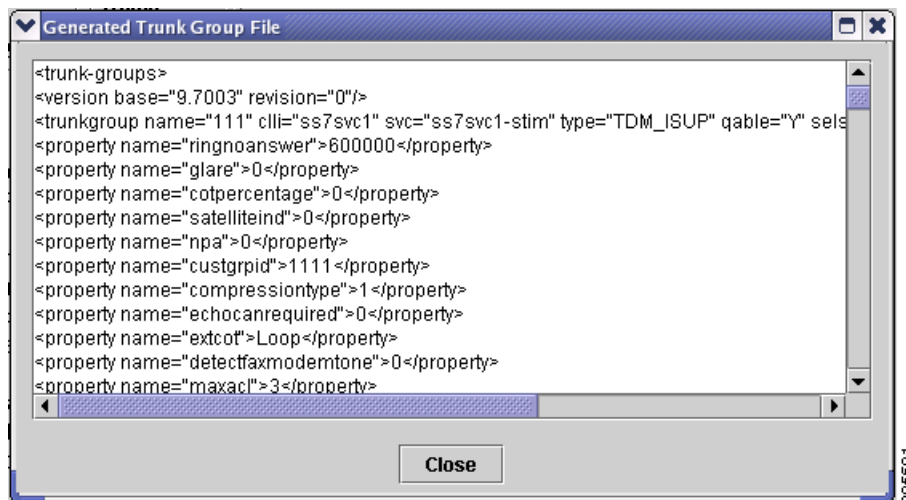
View Generated Trunk File

To view the trunk file generated from your Cisco VSPT provisioning session, click **View > Trunk File**.
A screen displaying the generated trunk file, similar to the one shown in Figure 4-3, appears.

Figure 4-3   *Generated Trunk File Window*
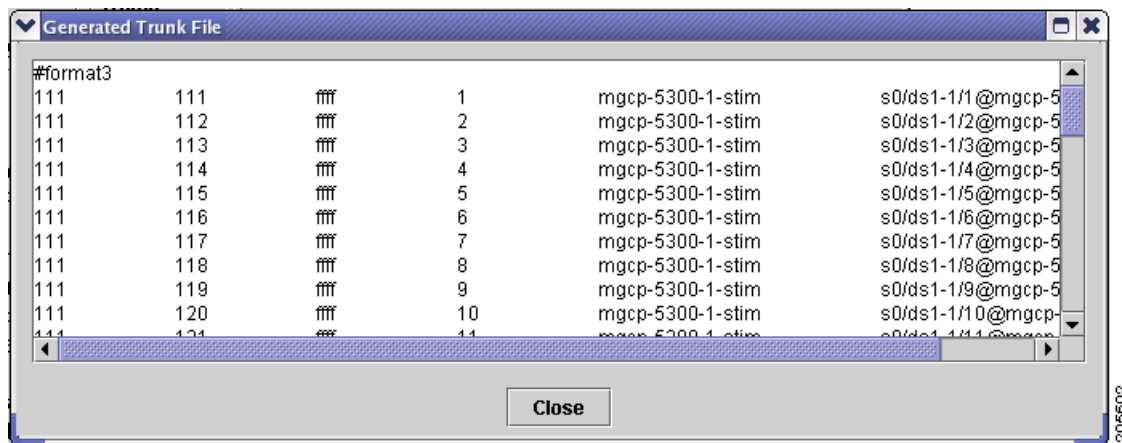
Perform an Integrity Check

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 Cisco PGW 2200 Softswitch signaling configuration
- Traffic against the Cisco PGW 2200 Softswitch 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 4-4).

Figure 4-4   *Integrity Check Dialog Box*
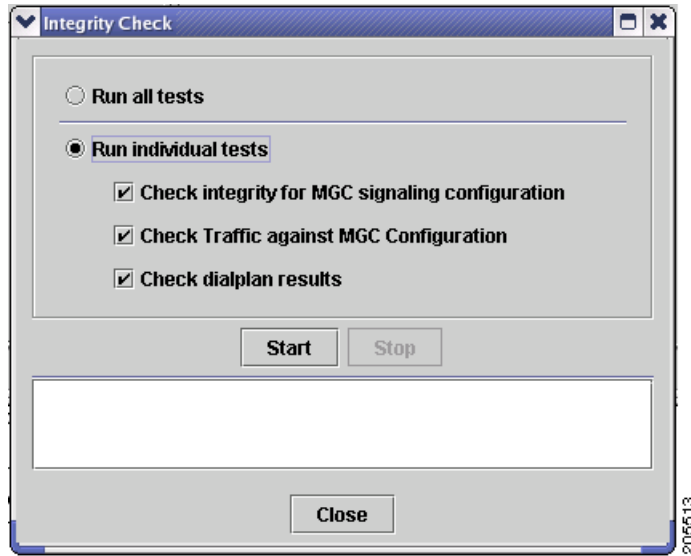
Step 2   Select the tests you want to run:

- Click **Run all tests** to run all three tests. See "Integrity Check Dialog Box Options" section on page 4-5 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**. Cisco VSPT runs the selected tests.

When the tests finish, a screen similar to the one in Figure 4-5 appears showing the results of the integrity checks.

Figure 4-5   Integrity Check Results
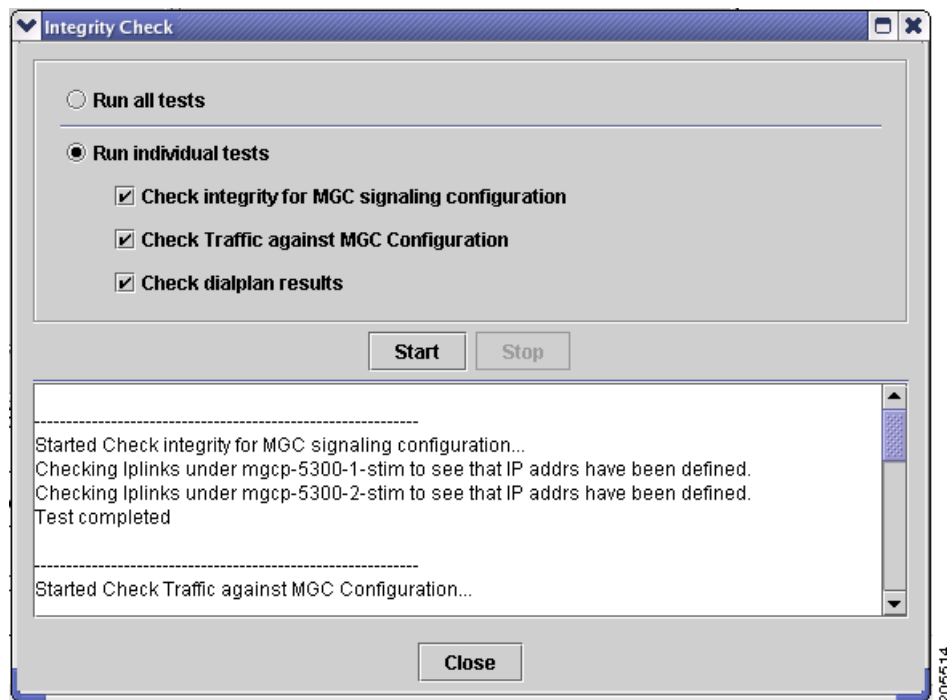
Integrity Check Dialog Box Options

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

Check Integrity for Cisco PGW 2200 Softswitch Signaling Configuration

When you perform an integrity check for Cisco PGW 2200 Softswitch signaling configuration, the Cisco VSPT does the following:

- Checks that the hostname is specified for Cisco PGW 2200 Softswitch.
- Checks that logins and passwords are specified for Cisco PGW 2200 Softswitch.
- Checks that Cisco PGW 2200 Softswitch ipaddrs are specified.
- Checks that if Cisco PGW 2200 Softswitch failover is specified, the failover IPs are specified.
- 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 Cisco PGW 2200 Softswitch ports and MGX ports match on the IPLNK.
  - Checks that all IPLNKs under a single IPFASPATH map to the same port number.
- Checks that point codes are correctly provisioned and only one true opc is defined.
- Checks that if there are Lawful Intercept Mediation Device (LIMD) sigpaths, one iplink is defined at least.

- Checks that a trunk group profile contains some property provisioning.
- Checks that signaling path for an external node is correctly provisioned. (External node types are MGX8260, VISM, VXSM (VXSM was added in Release 2.7(3) Patch 2).)
- Checks that if the property IPInScreening of one SIP signaling service is set to 2, a default trunk group of SIP_IN trunk type using that SIP signaling service is provisioned (Added in Release 2.7(3) Patch 3).

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

Check Traffic Against Cisco PGW 2200 Softswitch Configuration

When you perform an integrity check of traffic against the Cisco PGW 2200 Softswitch configuration, the Cisco VSPT does the following:

- Check if there are corresponding IPFASPATH signaling services with corresponding IPLNKs when D channels are defined as FAS and NFAS PRI in the trunk group/trunk section.
- 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.
- Checks CIC conflicts for trunk groups sharing the same SS7 or IP signaling service. (One CIC is used only in one trunk among the trunk groups sharing the same SS7 or IP signaling service.)

Check Dial Plan Results

When you perform an integrity check for the dial plan, the Cisco PGW 2200 Softswitch does the following:

- Checks that the route names in the route results actually exist on the traffic side
- Checks that the resultset is not empty
- Checks that the resultset contains an existing conditional route, codecString, and CPCMOD
- Checks that the IN_TRIGGER result contains a valid STP/SCP index which is defined in MGC Config window > SS7 Subsystem

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.

Deploy a Configuration

When you finish defining a configuration, you must deploy that configuration to the Cisco PGW 2200 Softswitch.

Note   A new configuration should not be deployed during times of peak load on the
Cisco PGW 2200 Softswitch.

A configuration created in Cisco VSPT can be deployed to a Cisco PGW 2200 Softswitch as a new
configuration or incrementally. Deploying incrementally allows you to quickly apply modifications to
an existing configuration without having to redeploy the entire configuration. Cisco VSPT also allows
you to visually check the incremental commands it generates before deploying those commands to the
Cisco PGW 2200 Softswitch.

If the Cisco PGW 2200 Softswitch 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 Cisco 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 4-6 appears.

Figure 4-6   Deploying a Configuration
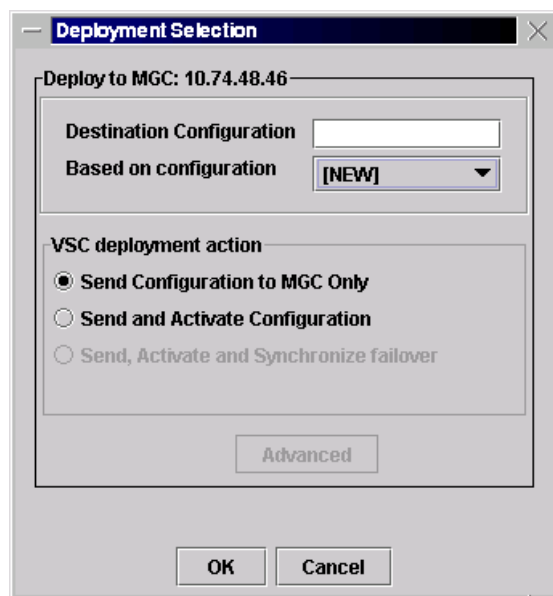
Step 3   Indicate how you want to deploy the configuration:

- To deploy the configuration to the Cisco PGW 2200 Softswitch only, do one of the following:

  - If you want to send the configuration to the Cisco PGW 2200 Softswitch but not activate it, click the button next to **Send Configuration to MGC Only**.

  - If you want to send the configuration to the Cisco PGW 2200 Softswitch and activate it, click the button next to **Send and Activate Configuration**.

  - If you have a continuous-service configuration with two Cisco PGW 2200 Softswitch 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.

✎ **Note**   If you select an option other than NEW, the Advanced button is enabled. For information about the options this button provides, see the .

Step 4   Choose a configuration in the Based on configuration drop-down list.

This list displays all existing configurations on the selected Cisco PGW 2200 Softswitch and the [LAST IMPORT] and [NEW] options. You can choose one of the following options from the drop-down list:

- LAST IMPORT—The Cisco 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—Cisco VSPT imports the selected configuration from the Cisco PGW 2200 Softswitch, 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   Click **OK**. The screen shown in Figure 4-7 appears and displays the status as the current provisioning session is deployed.

Figure 4-7   Deployment Progress
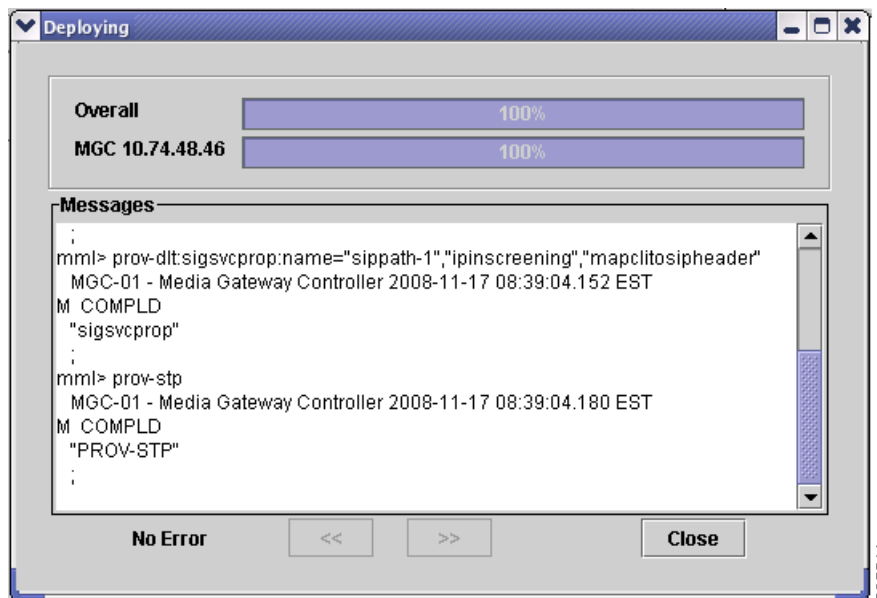
> **Note**   In a continuous-service configuration, the XECfgParm.dat file on each machine must be configured. If you experience problems, verify the integrity of the XECfgParm.dat files on both machines. See Chapter 3 in the *Cisco Media Gateway Controller Software Release 9.7 Installation and Configuration Guide*.

Configuring an Incremental Deployment

An incremental deployment allows you to modify an existing configuration and deploy only the modified areas to the Cisco PGW 2200 Softswitch. 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 PGW 2200 Softswitch 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 4 in the "Deploying a New Configuration" section on page 4-7.

Step 2   Click **Advanced** in the window shown in Figure 4-6. The screen shown in Figure 4-8 appears.

Figure 4-8   Incremental Deployment Component Selector
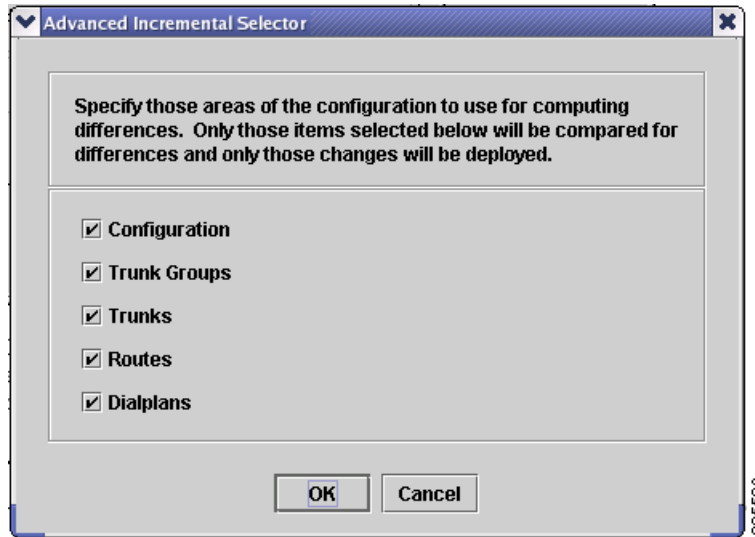
If you have only made configuration changes to one or more of the areas listed, you can direct the Cisco VSPT to compare only those areas with the current configuration, and your modifications can be deployed more quickly.

✎
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 5 in the "Deploying a New Configuration" section on page 4-7, and complete the procedure described there. When you click **OK**, a screen similar to the one displayed in Figure 4-9 appears.

Figure 4-9   Confirm MML Commands
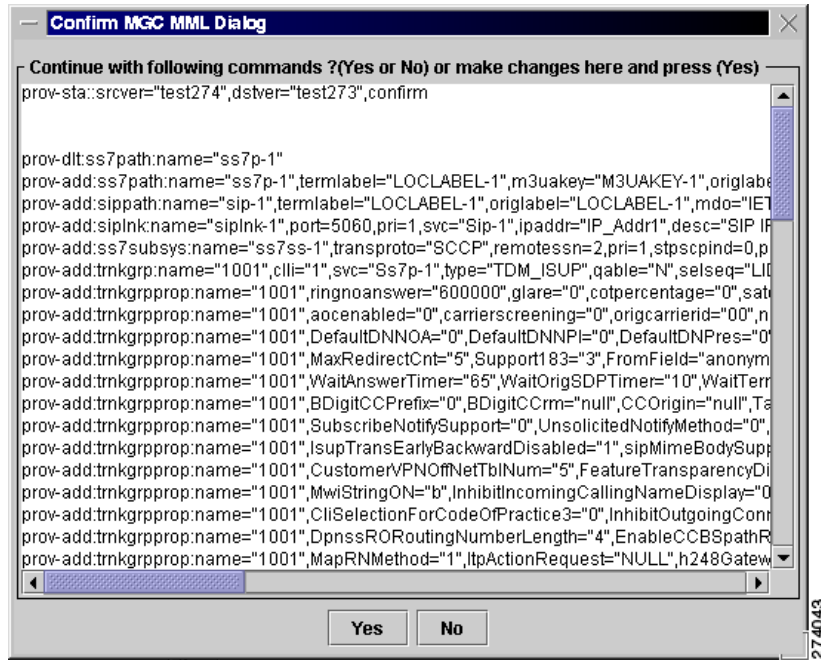
Step 5   Inspect the MML commands, modify them if desired, and click **Yes** to continue with the incremental deployment. Click **No** to reissue the deployment as a new configuration.

Remote Shell

Cisco 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 Cisco 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 > Remote Shell**. A screen similar to that shown in Figure 4-10 appears.

Figure 4-10   *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 Cisco PGW 2200 Softswitch. If you are communicating with an SSH-enabled Cisco PGW 2200 Softswitch, you can use SSH instead of Telnet for the communication.

Use the following procedure to view configurations on a Cisco PGW 2200 Softswitch:

Step 1   Click **Tools > MGC viewer** on the main Cisco 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 4-11 appears.

*Figure 4-11   Select Cisco PGW 2200 Softswitches*

Step 3   Enter the host name of the Cisco PGW 2200 Softswitch in the **Hostname** box, enter the Cisco PGW 2200 Softswitch login and password, and click **OK**. A screen similar to the one in Figure 4-12 appears and lists all configurations on the specified Cisco PGW 2200 Softswitch.

Figure 4-12   MGC Configurations
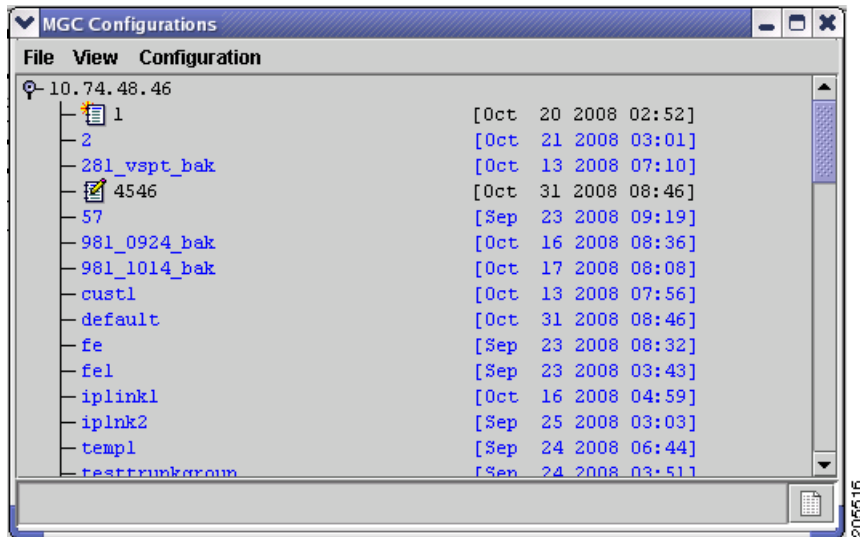
Step 4   Click **Configuration** on the MGC Viewer menu bar, and select one of the following actions:

- Activate—Activate the configuration.

- Synchronize—Synchronize with the current configuration.

- Delete—Delete the configuration.

Cisco BAMS Configuration

The Cisco BAMS Configuration utility enables you to create, copy, modify, and deploy a configuration for the Cisco BAMS server. You can use Cisco VSPT to provision general Cisco BAMS system items, including general information, zones, trunk group information, measurements, system, and other items.

You can find provisioning procedures in the section, "Starting a Cisco BAMS Provisioning Session," and the section "Cisco BAMS Server Configuration" in Chapter 3 of 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/R9GUI.html

Before you use Cisco PGW 2200 Softswitch to provision a Cisco BAMS, you need to provision the Cisco BAMS and the Cisco PGW 2200 Softswitch for using the Cisco BAMS.

- Provision the Cisco PGW 2200 Softswitch for using BAMS—See the section "Configuring the Cisco MGC for Using BAMS," and the section "Enabling SFTP on Cisco BAMS and the Cisco PGW 2200" in Chapter 2 at

    http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/bams/3.30/guide/330ch2.html

- Provision the Cisco BAMS—See the section "Configuring BAMS" in Chapter 2 at the preceding link and the section "Updating the Poll Table" in Chapter 5 at

    http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/bams/3.30/guide/330ch5.html

Note   To set up an active Cisco PGW 2200 Softswitch paired with a standby one for a Cisco BAMS, you need to provision both active and standby Cisco PGW 2200 Softswitches.

State Operation

The State Operation utility enables you to query the active configuration on the Cisco PGW 2200 Softswitch for the state of managed objects. After a query, you can modify the state of an object and apply the update to the Cisco PGW 2200 Softswitch. If you are querying the state of an SSH-enabled Cisco PGW 2200 Softswitch, you can use SSH instead of Telnet for the communication.

Use the following procedure to query the state of managed objects on the Cisco PGW 2200 Softswitch:

Step 1   Click **Tools > State Operation** on the main Cisco 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 4-13 appears.

Figure 4-13   State Operation Dialog
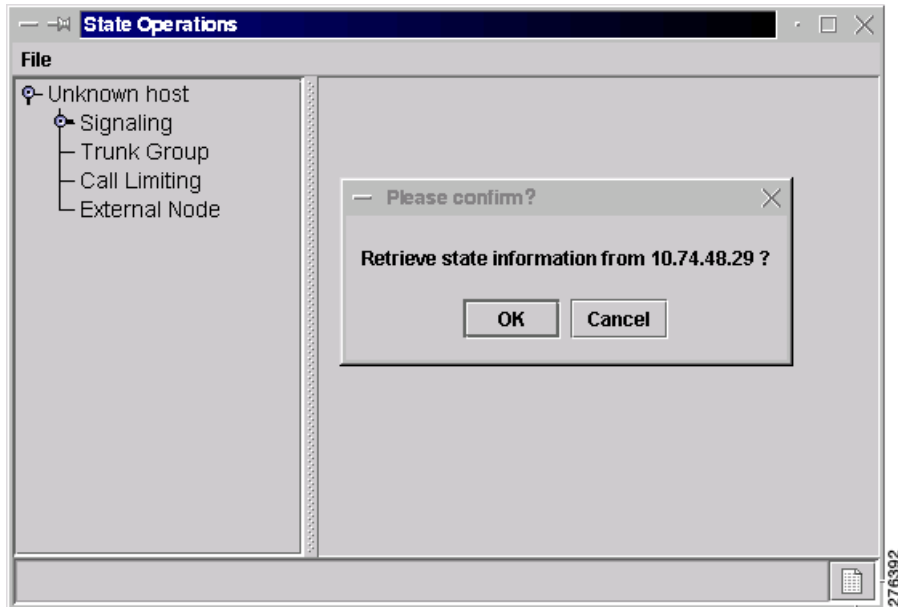
Step 3   Click OK.

The Cisco VSPT queries the Cisco PGW 2200 Softswitch.

Step 4   Expand the hierarchical tree in the left pane of the State Operations window to locate and highlight the object. See Figure 4-14

Figure 4-14   State Operations
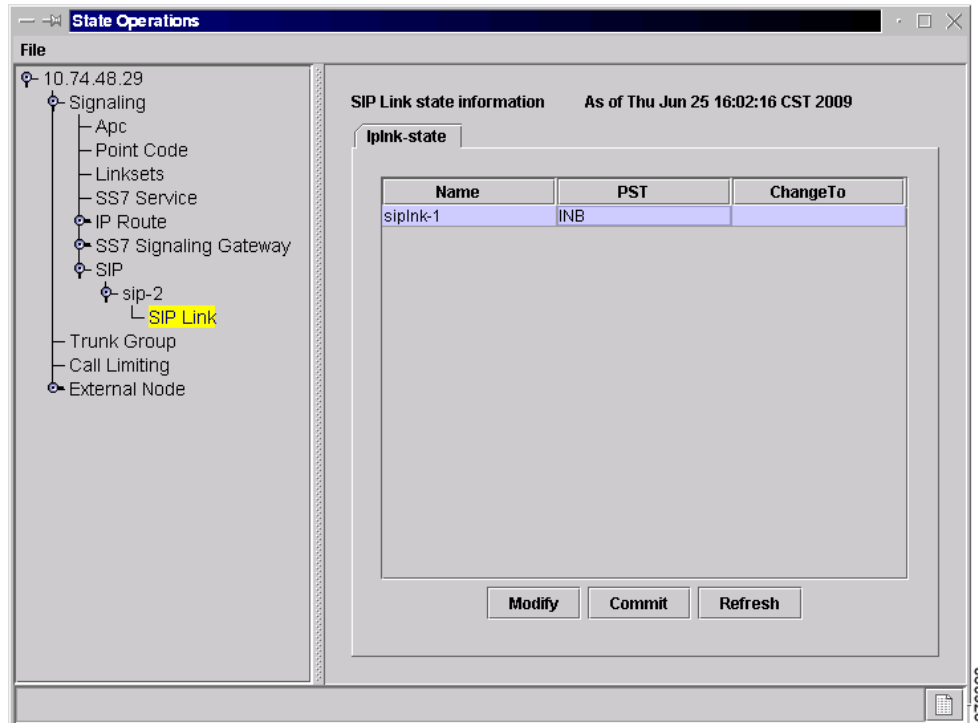
Step 5   Click **Modify** at the bottom of the right pane. A screen wimilar to the one in Figure 4-15 displays.

Figure 4-15   Modify State
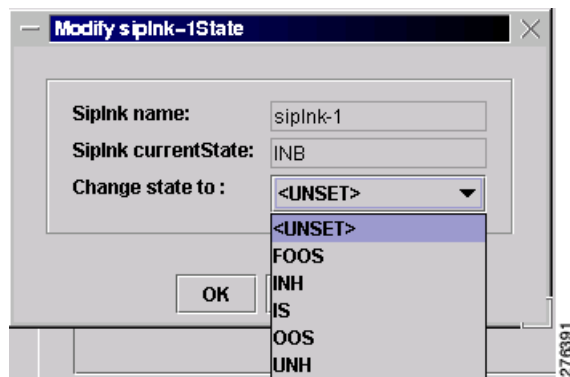
Step 6   From this window, you can modify the state by choosing the desired state in the Change state to drop-down list. Click OK to save the change. You are back to the window in Figure 4-14.

Step 7   Click **Modify** to change the state in this window, and click **Commit** to change the state on the Cisco PGW 2200 Softswitch. To query the object again, click **Refresh**.

Advanced Number Editor

You can use the advanced number editor to edit the call screening list, the ported number table, and the number termination table:

- A-number Whitelist
- A-number Blacklist
- B-number Whitelist
- B-number Blacklist
- Ported Number Table
- Number Termination Table

Click **Tools > Advanced Number Editor** and you see a window similar to the one in Figure 4-16. For details on the advanced number editor, see Chapter 3 of the *Cisco PGW 2200 Softswitch Release 9 Dial Plan Guide*.

Figure 4-16   Advanced Number Editor Window
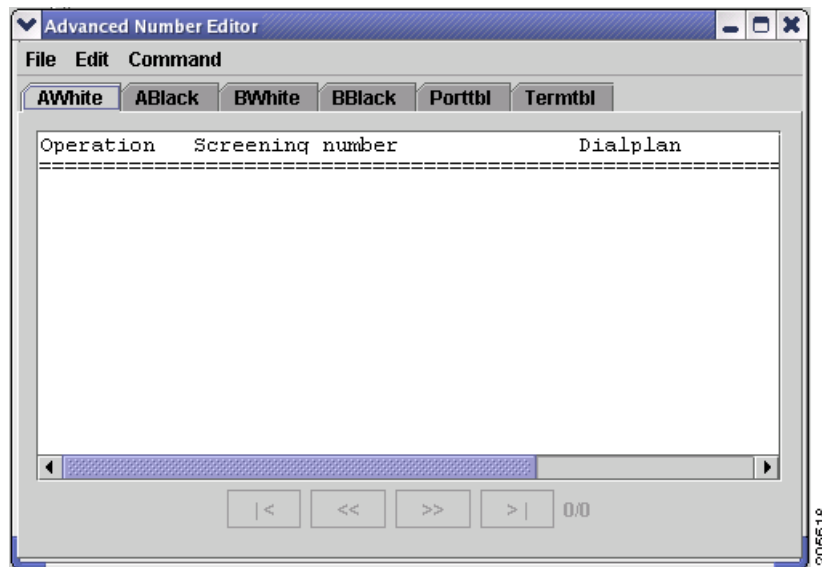
Perform an Audit

You can use an audit to ensure that both the Cisco PGW 2200 Softswitch and a Cisco BAMS server supporting the Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch, 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 4-17).

Figure 4-17   Audit

Step 2   Enter the Cisco PGW 2200 Softswitch hostname, login, and password in the top pane of the window.

Step 3   To specify the configuration to audit, click **Select**, highlight the configuration to audit, and click **OK**.

Step 4   Enter the Cisco BAMS hostname, login, and password in the bottom pane of the window.

Step 5   To specify the configuration to audit, click **Select**, highlight the configuration to audit, and click **OK**.

Step 6   Click **Audit**. A screen similar to the one displayed in Figure 4-18 appears.

Figure 4-18   Audit Results

The left pane displays the signal path and bearer channel data configured on the
Cisco PGW 2200 Softswitch host, and the right pane displays the same data configured on the
Cisco BAMS server.

Back Up and Restore

The Cisco 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 do a backup or restore on any of the following devices if they have been configured for the
Cisco PGW 2200 Softswitch:

- Cisco PGW 2200 Softswitch Host—Active configuration or entire Cisco PGW 2200 Softswitch
  system

- Cisco Catalyst 2900XL—Running-config and image in Flash

- Cisco Catalyst 5500—For switch module and RSM, configuration and image in Flash

- Cisco Catalyst 6509—For switch module and MSFC, configuration and image in Flash

- Cisco ITP-L (SLT) 2600—Running-config and image in Flash

- Cisco BAMS Phase 3—Active configuration

- Cisco 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.
- Make sure there is enough space on the backup host for the backup files.
- You must start Cisco VSPT from a UNIX shell with the backup ID. The backup ID is specified during installation. You can start Cisco VSPT in either of two ways:
  - If Cisco 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.
- Make sure the timeout value is adequate for the backup process to be finished. To adjust the timeout values, modify the following two parameters in the configuration file: /opt/CSCOvsp28/classes/com/cisco/transpath/dart/editor/configEditor.properties.
  - Modify the value of parameter DefaultTimeOut to adjust the timeout value for shell command. The default value is three minutes.
  - Modify the value of parameter Backup.timeout to adjust the timeout value for system backup and FTP session. The default value is 30 minutes.

If you receive an error message, "Time out interact..."during the backup process, you can modify the value of Backup.timeout to a larger number to solve the problem.

Note The system backup could take long time and the backup files could be very large. It is strongly recommended that you perform the system backup at non-busy time.

Backup and Restore Process

The backup process includes three main steps:

- Cisco 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. To select the policy, choose 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.
- The configuration file of the managed component is transferred to 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 four main steps:

- Cisco 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 Cisco VSPT menu bar.

The Backup and Restore window appears, listing components that can have scheduled backups.

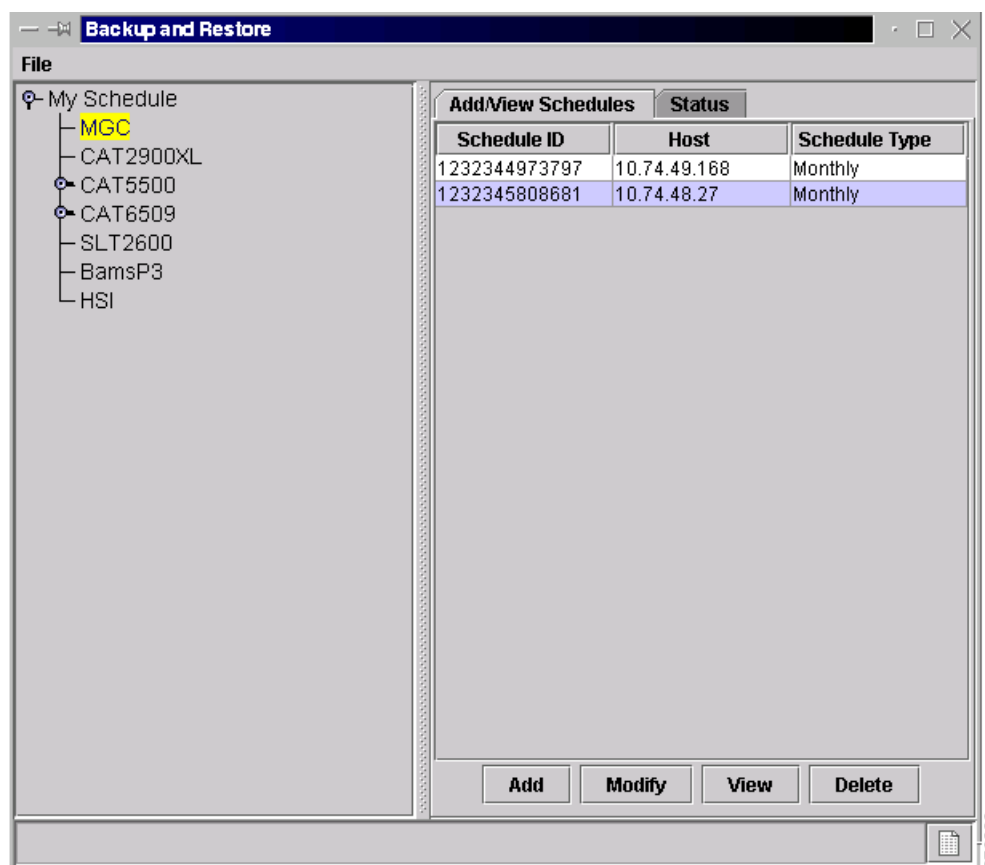**Step 2**   Click the component for which you want to schedule a backup.

In the following example, the Cisco PGW 2200 Softswitch component configuration is backed up. On the right side of the window, the schedules for that component appear.

✎
Note   If you want to perform a restore, you must have a backup file already created and available on the Cisco PGW 2200 Softswitch or on another managed component.

Step 3   In the Add/View Schedules pane, click **Add**.

Figure 4-19   Add/View Schedules

A screen similar to the one shown in Figure 4-20 appears.

Figure 4-20   Add MGC Schedule

✎

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

Step 4   From the Action drop-down list, choose the action you want to perform.

Choices are Backup and Restore.

If you choose Restore, a screen similar to the one shown in Figure 4-21 appears.

Figure 4-21   Restore

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

   • Enter the IP address of the Cisco PGW 2200 Softswitch.

   • Enter the Cisco PGW 2200 Softswitch login and password.

   > **Note**   If you want to perform a restore for the Cisco PGW 2200 Softswitch system, you must enter the
   > Cisco PGW 2200 Softswitch root password as well.

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

Step 7   From the File Type drop-down list, choose one of the following:

   • MML Config—Backs up MML files for the active configuration on the Cisco PGW 2200 Softswitch

   • 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 Cisco VSPT and any system responses.

Step 10 Choose 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 Cisco PGW 2200 Softswitch system, FTP.

Step 11 Choose the schedule type. Choices include

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

Step 12 Choose 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 Choose 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, you can view the status of the activity, and acknowledge or clear the status log file from the Status tab. The backup file with the name you specified is available for use with Cisco VSPT.

Check Status of Backup or Restore

The Cisco 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 Cisco 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.