



## MNM-PT Utilities

---

MNM-PT Version 2.4(1) provides utilities to accomplish the following tasks:

- [Perform an Integrity Check, page 2-25](#)
- [View Generated Output, page 2-28](#)
- [View Generated Cisco MGW Commands, page 2-29](#)
- [Deploy a Configuration, page 2-30](#)
- [Use Telnet or ssh, page 2-35](#)
- [MGC Viewer, page 2-36](#)
- [State Operation, page 2-38](#)
- [Perform an Audit, page 2-39](#)
- [Back Up and Restore, page 2-41](#)

### Perform an Integrity Check

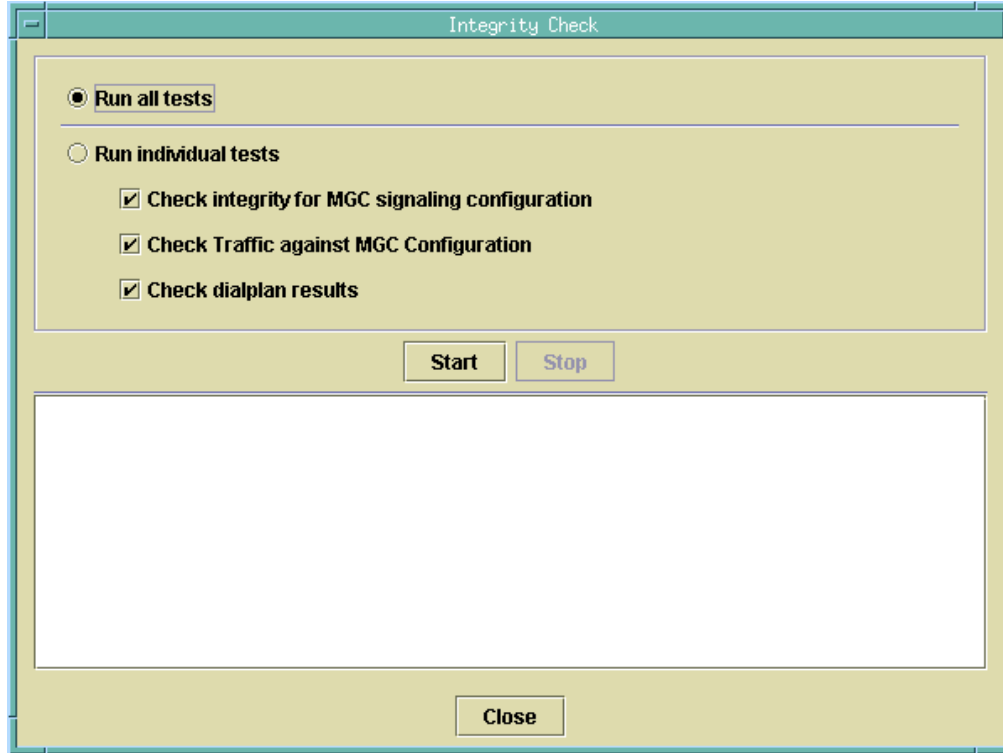
When provisioning is complete, you can perform an integrity check to prevent possible configuration errors. You can check one or all of the following:

- 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:

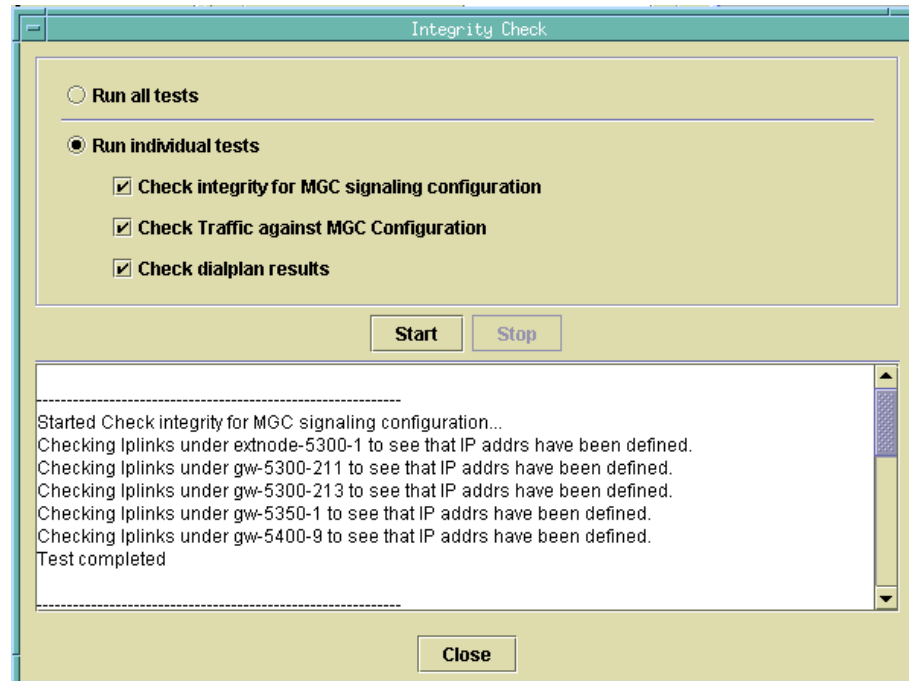
- 
- Step 1** Click **Tools > Integrity Check**. The Integrity Check dialog box appears ([Figure 2-1](#)).

Figure 2-1 Integrity Check



- 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**. MNM-PT runs the selected tests.
- When the tests finish, a screen similar to the one in [Figure 2-2](#) appears showing the results of the integrity checks.

Figure 2-2 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 MNM-PT does the following:

- Checks that the hostname is specified for MGC
- Checks that login/passwords are specified for MGC
- Checks that MGC ipaddds are specified
- Checks that if MGC failover is specified, the failover IPs are specified
- Checks that MGX hostname is specified
- Checks that MGX login/password is specified
- Checks the MGX IPaddds
- For EXTNODES where the configuration refers to an MGX, checks PeerAddds 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 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 IPLNK 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 Version 9.3(2) and MNM-PT Version 2.3(2), IPFAS signaling services apply only to the VISM card.

---

## Check Traffic Against MGC Configuration

When you perform an integrity check of traffic against the MGC configuration, the MNM-PT 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/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 MNM-PT 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

MNM-PT 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 MNM-PT provisioning session, click **View > MML**.

A screen displaying generated MML, similar to the one shown in [Figure 2-3](#), appears.

**Figure 2-3** First Generated MML Screen

The screenshot shows a window titled "Generated MML" with a scrollable text area containing the following MML commands:

```

MML commands for signaling
prov-add:Card:name="card-1",desc="card in slot 0",type="EN",slot=0
prov-add:Enetif:name="enet-1",desc="interface in slot 0",card="card-1"
prov-add:Card:name="card-2",desc="card in slot 2",type="EN",slot=2
prov-add:Enetif:name="enet-2",desc="interface in slot 2",card="card-2"
prov-add:Opcname="opc-vsc3000-am-1",desc="Originating Point Code of VSC3000-AM-1",n
prov-add:Dpcname="pc-vco4k-1",desc="Point Code",netaddr="0.110.7",netind=3
prov-add:Dpcname="pc-colt-1",desc="Point Code",netaddr="0.71.0",netind=3
prov-add:Dpcname="pc-gts-1",desc="Point Code",netaddr="0.28.0",netind=3
prov-add:Dpcname="pc-versatel-1",desc="Point Code",netaddr="0.45.3",netind=3
prov-add:Lnkset:name="lnkset-vco4k",desc="Lnkset to VCO4K",apc="pc-vco4k-1",proto="SS7-I
prov-add:Lnkset:name="lnkset-colt-1",desc="Lnkset",apc="pc-colt-1",proto="SS7-ITU",type="IP
prov-add:Lnkset:name="lnkset-gts-1",desc="Lnkset",apc="pc-gts-1",proto="SS7-ITU",type="IP
prov-add:Lnkset:name="lnkset-versatel-1",desc="Lnkset",apc="pc-versatel-1",proto="SS7-ITU
prov-add:Ss7path:name="ss7p-vco4k",desc="SS7 Signaling Service to vco4k",side="network",m
prov-add:Ss7path:name="ss7p-colt",desc="SS7 Signaling Service",side="user",mdo="ISUPV2_SW
prov-add:Ss7path:name="ss7p-gts",desc="SS7 Signaling Service",side="user",mdo="ISUPV2_SW
prov-add:Ss7path:name="ss7p-versatel",desc="SS7 Signaling Service",side="user",mdo="ISUPV2
prov-add:Ss7route:name="ss7r-vco4k",desc="SS7 Route to vco4k",dpc="pc-vco4k-1",opc="opc
prov-add:Ss7route:name="ss7r-colt",desc="SS7 Route",dpc="pc-colt-1",opc="opc-vsc3000-am
prov-add:Ss7route:name="ss7r-gts",desc="SS7 Route",dpc="pc-gts-1",opc="opc-vsc3000-am
prov-add:Ss7route:name="ss7r-versatel",desc="SS7 Route",dpc="pc-versatel-1",opc="opc-vsc3
prov-e:d:Accrespcat:name="default",acl1drcant=50,acl1drskip=20,acl1arcant=50,acl1arskip=20,
prov-e:d:Mclthreshold:name="callrate",mcl1onset=0,mcl1abate=0,mcl2onset=0,mcl2abate=0,mc
prov-e:d:Mclthreshold:name="cpu",mcl1onset=82,mcl1abate=75,mcl2onset=90,mcl2abate=77,m
prov-e:d:Mclthreshold:name="memoryaddress",mcl1onset=84,mcl1abate=80,mcl2onset=88,mcl
prov-e:d:Mclthreshold:name="queuelen",mcl1onset=75,mcl1abate=60,mcl2onset=80,mcl2abate
prov-e:d:Mclthreshold:name="virtualmemory",mcl1onset=80,mcl1abate=75,mcl2onset=85,mcl2
prov-e:d:Mclcallreject:name="mcl1",callreject=25
prov-e:d:Mclcallreject:name="mcl2",callreject=50
prov-e:d:Mclcallreject:name="mcl3",callreject=100
prov-add:Holiday:date="2001.06.06",hday="Hol3"
prov-add:Holiday:date="2001.12.08",hday="Hol2"
prov-add:Holiday:date="2000.03.20",hday="Hol3"

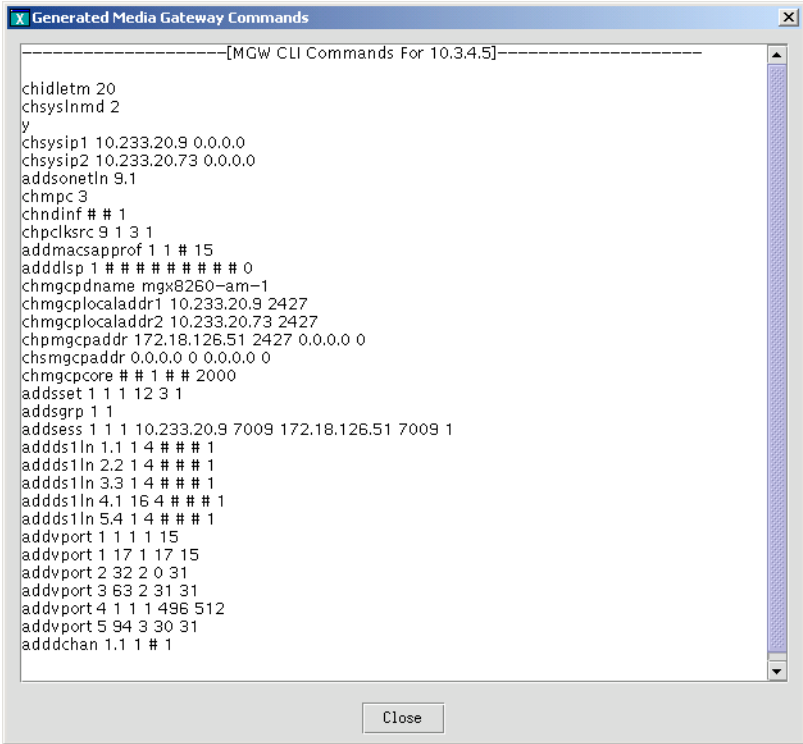
```

The window has a "Close" button at the bottom center. A vertical number "70495" is visible on the right side of the window frame.

## View Generated Cisco MGW Commands

To view the Cisco MGW commands generated from your provisioning session, click **View > MGW Commands** on the main MNM-PT menu bar. A screen with generated Cisco MGW commands, similar to that shown in [Figure 2-4](#), appears.

Figure 2-4 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
adddsp 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
addmgrp 1 1
addsess 1 1 1 10.233.20.9 7009 172.18.126.51 7009 1
addds1ln 1.1 1 4 # # # 1
addds1ln 2.2 1 4 # # # 1
addds1ln 3.3 1 4 # # # 1
addds1ln 4.1 16 4 # # # 1
addds1ln 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 MNM-PT can be deployed to a Cisco MGC as a new configuration or incrementally. Deploying incrementally allows you to more quickly deploy modifications to an existing configuration without having to redeploy the entire configuration. MNM-PT 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.

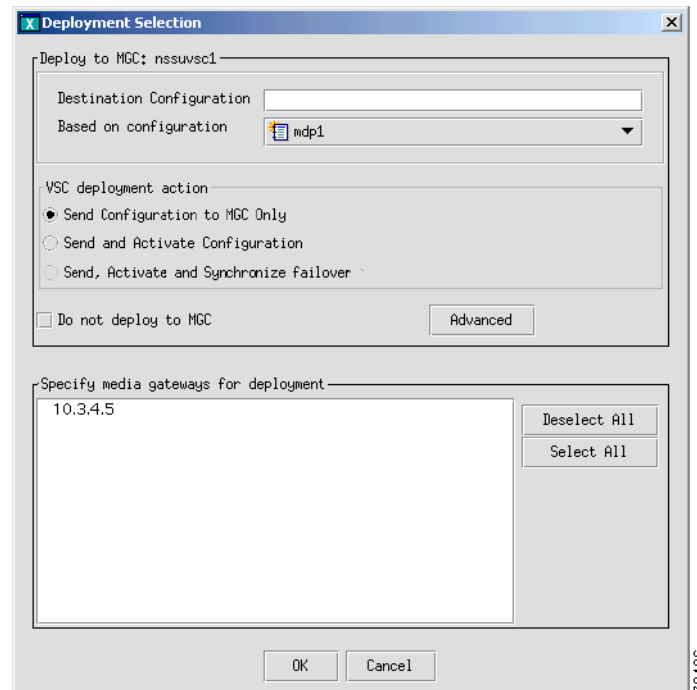
**Step 1** Click **Tools > Deploy** on the main MNM-PT menu bar ( see [Figure 1-3](#) on page 1-12). The Protocol Options dialog box appears.

**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 2-5](#) appears.

**Figure 2-5 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 2-33.

---

- 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 MNM-PT 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—MNM-PT 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.



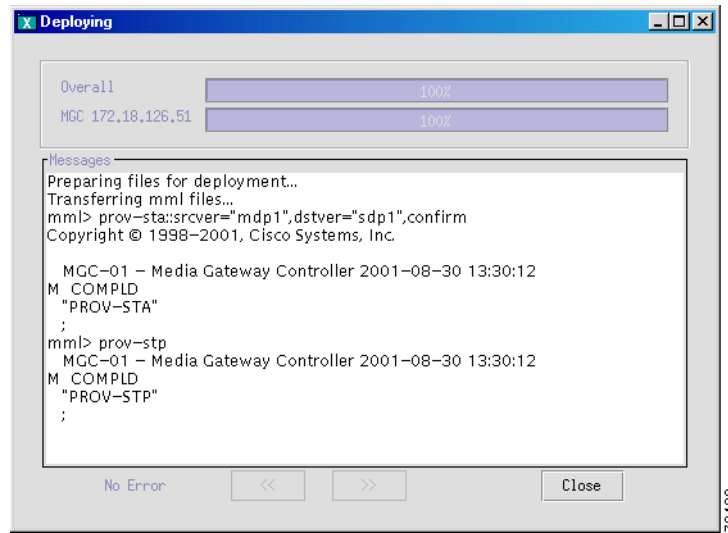
---

**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 2-6](#) appears and displays the status as the current provisioning session is deployed.

Figure 2-6 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 Version 9 Installation and Configuration Guide*.

## Configuring an Incremental Deployment

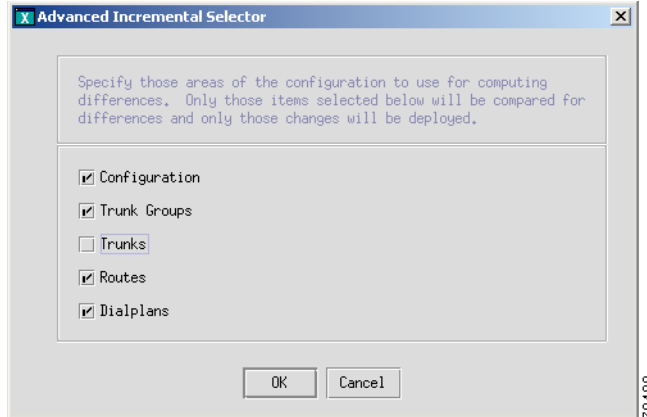
An incremental deployment allows you to modify an existing configuration and deploy only the modified areas to the Cisco MGC. Modifications can be made more quickly, and errors affecting unmodified areas are minimized. In addition, provisioning modifications made by other users in separate areas are 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 2-30.
- Step 2** Click **Advanced** in the window shown in [Figure 2-5](#). The screen shown in [Figure 2-7](#) appears.

**Figure 2-7 Incremental Deployment Component Selector**

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



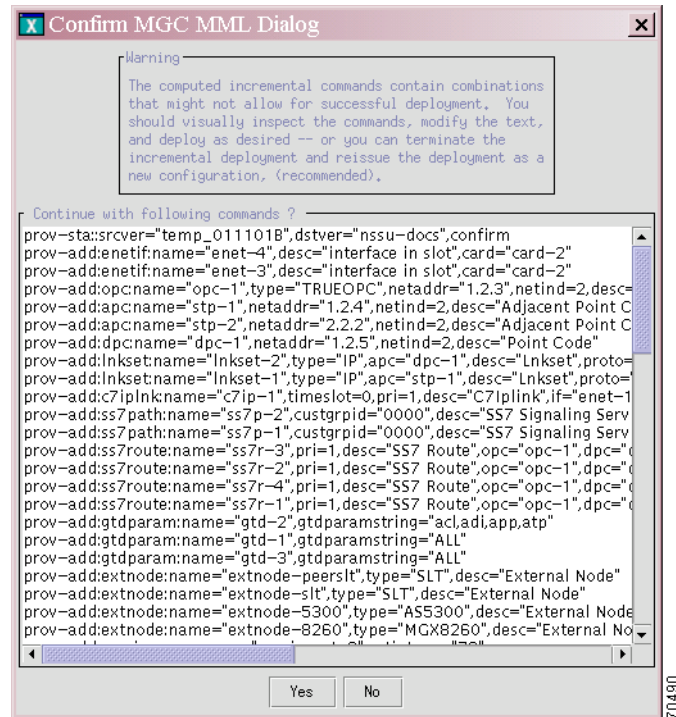

---

**Note** If you select areas in this window, make 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 2-30, and complete the procedure described there. When you click **OK**, a screen similar to the one displayed in [Figure 2-8](#) appears.

Figure 2-8 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.

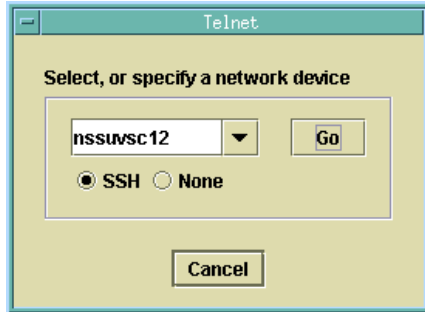
## Use Telnet or ssh

MNM-PT provides a utility to open a Telnet session directly to a device. Once you have established your Telnet connection, you then log in to the device and execute commands remotely on the device through the Telnet interface.

If you have installed SSH for MNM-PT 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 2-9](#) appears.

**Figure 2-9 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, **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.

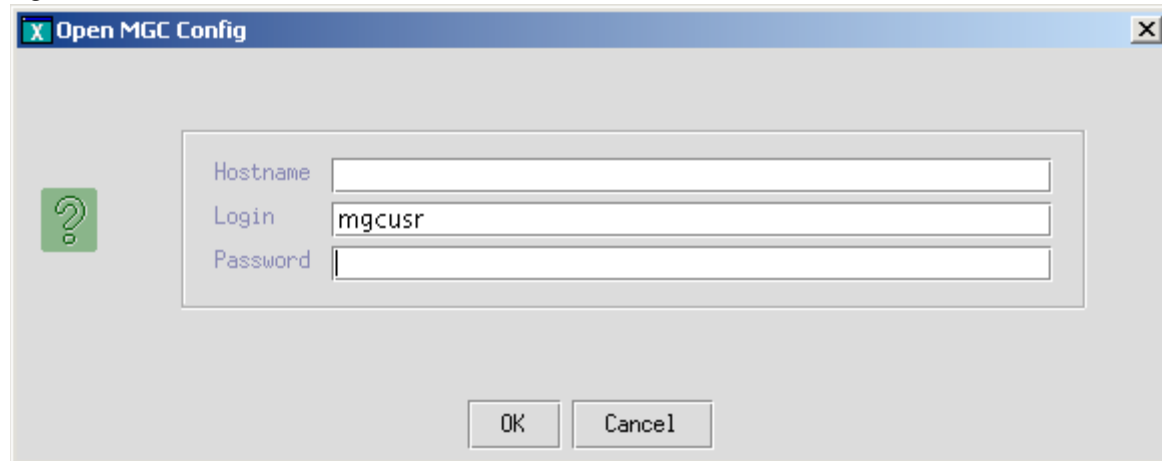
Use the following procedure to view configurations on a Cisco MGC:

---

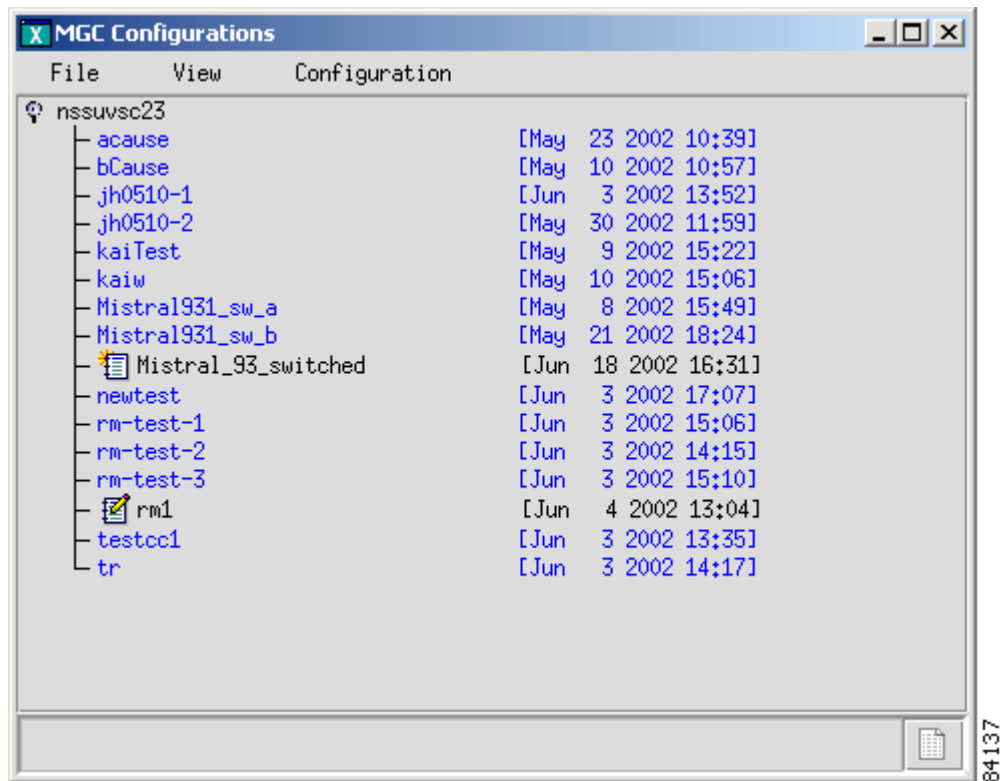
- Step 1** Click **Tools > MGC viewer** on the main MNM-PT menu. On the MGC Configuration screen that appears, click **File > Open MGC**. The Protocol Options dialog box appears.
- Step 2** Select the desired protocol:
- Choose **SSH** if SSH is enabled on the device.
  - Choose **None** if SSH is not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

A screen similar to the one in [Figure 2-10](#) appears.

Figure 2-10 Select MGC



- 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 appears and lists all configurations on the specified MGC.



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

Activate—Choose to activate the configuration.

Synchronize—Choose to synchronize with the current configuration.

Delete—Choose to delete the configuration.

# State Operation

The State Operation utility provides the ability 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:

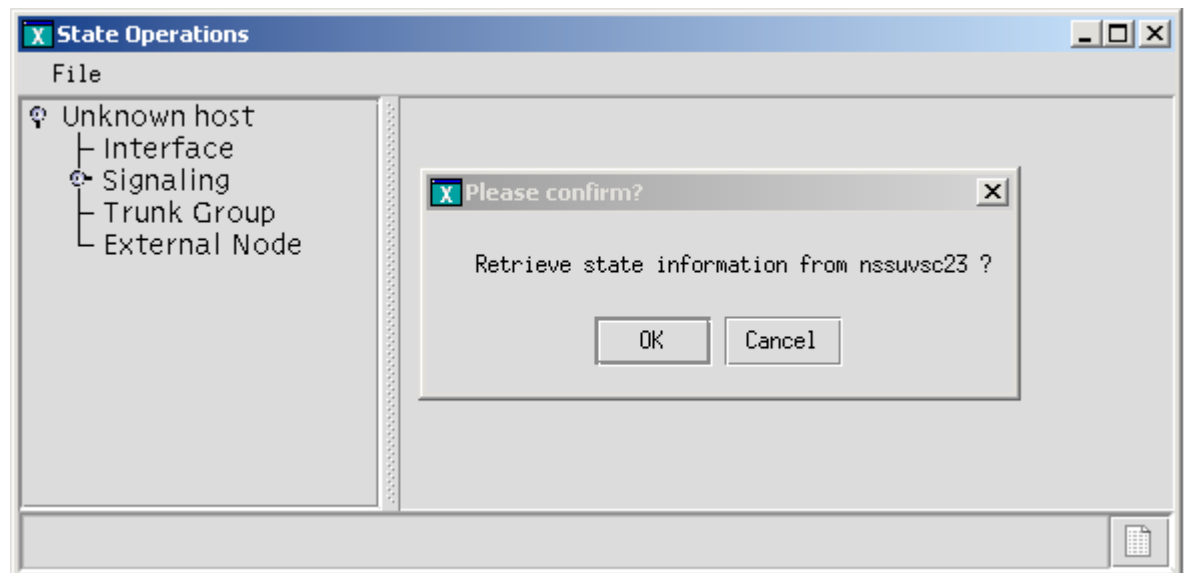
**Step 1** Click **Tools > State Operation** on the main MNM-PT menu. The Protocol Options dialog box appears.

**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.

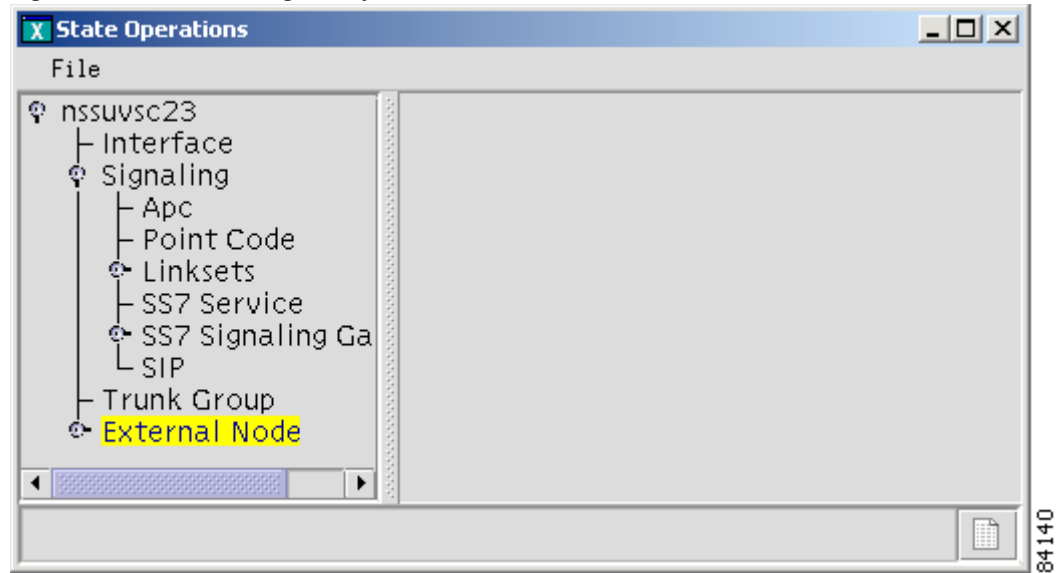
A screen similar to the one in [Figure 2-11](#) appears.

**Figure 2-11 State Operation Dialog**



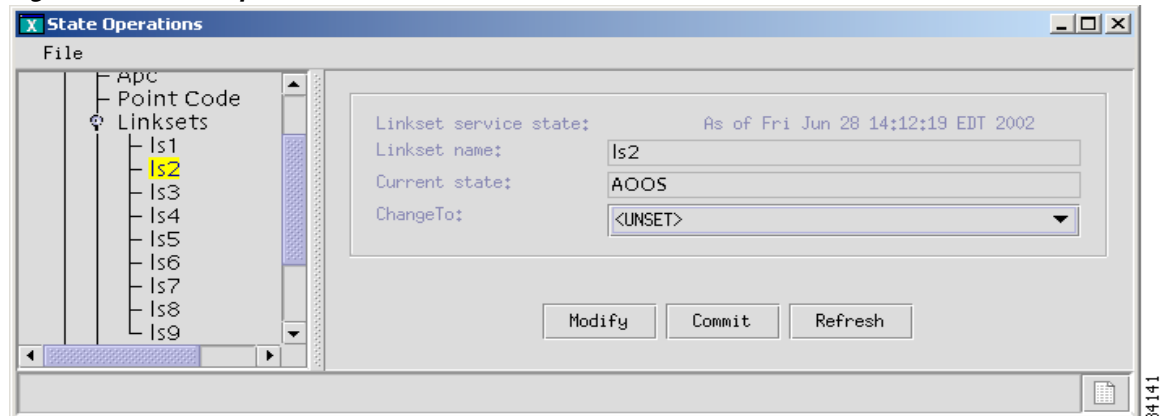
**Step 3** Click OK. The MNM-PT queries the MGC and a screen similar to the one in [Figure 2-12](#) appears.

Figure 2-12 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 will appear and the right pane will display information about the state of the object you selected.

Figure 2-13 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**.

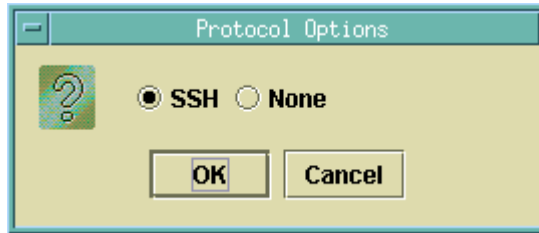
## Perform an Audit

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 examines 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 as shown in [Figure 2-14](#).

**Figure 2-14 Protocol Options Dialog Box**



- Step 2** Select the desired communication protocol, **SSH** (if SSH is installed on MNM-PT 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 2-15](#) appears.

**Figure 2-15 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 MNM-PT 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 back up and restore activities on any of the following devices if they have been configured for the MGC:

- MGC Host—Active configuration
- CAT5500—Configuration and image in Flash
- CAT2900XL—Running-config and image in Flash
- SLT2600—Running-config and image in Flash
- BAMS P3—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.

Backup and restore support using SSH for the log in to the device you are backing up. See [Backup and Restore Requirements](#) for details.

## Backup and Restore Requirements

You typically use MNM-PT Backup to back up the configuration on Server A (one of the supported components) onto a different server, Server B. The configuration can then be restored if needed back to Server A, or copied to other components of the same type (Server C, D, etc), as a way to clone a configuration.

In the Backup process, MNM-PT logs into Server A, copies the configuration, and transfers it to Server B using TFTP. Server B must have the TFTP server enabled. Refer to the *Cisco MGC Node Manager Installation Guide* at <http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/emins/index.htm> for instructions on enabling TFTP.

If you are using SSH on a managed Cisco PGW, BAMS, or HSI server, please keep the following in mind:

- The log in to Server A to get the configuration can (and should) be done securely, using SSH. You specify the Server A's IP address, Login, and Password, and you select SSH, in the Add ... Schedule dialog box when you set up the backup.
- The transfer of the configuration onto Server B is done using TFTP. You also specify Server B's IP address, Login, and Password in the Add Schedule dialog box. The TFTP transfer is nonsecure, although the password is encrypted.
- The TFTP server on Server A (and any server where SSH is installed) is turned off (along with ftp) in conjunction with the CSCOh013 package, and thus configurations cannot be backed up onto such a server. Generally you would not want to do this anyway, since it would defeat the purpose of the backup operation.
- Although MNM-PT has SSH installed, it uses the CSCOk9000 package only, and not CSCOh013. As long as MNM-PT is not on a server where CSCOh013 is installed (such as the PGW server), you can back up configurations onto the MNM-PT server.

## 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 MNM-PT 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.

- Step 3** In the Add/View Schedules pane, click **Add**. A screen similar to the one shown in [Figure 2-16](#) appears.

**Figure 2-16 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:

- MGC System—Backs up data files for the active configuration, the Times Ten database, the XEconfigParm.dat file, and UNIX configuration files.
  - MML Config—Backs up exported MML files for the active configuration on the MGC
- 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 MNM-PT and any system responses.
- Step 10** Select whether to set up the backup operation using **SSH** or Telnet (**None**).



---

**Note** The operation itself is executed with TFTP.

---

- Step 11** Select the schedule type. Choices include:
- Monthly
  - Daily
  - Hourly
  - Weekly
  - Now
  - Later
- Step 12** Select the protocol to use when 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 the MNM-PT.
- 

## Check Status of Backup or Restore

The MNM-PT 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 MNM-PT 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.
-