

Managing Network Elements

Overview of Network Elements

In the GUI application developed by Cisco, network elements and the domains to which they belong are managed through the **Element Manager** window. To open this window, start the GUI application and click on the **Element Manager** button on the Main Window (or **Element Manager** on the **Tools** menu). The window displays all of the elements, domains, and subdomains to which you have access (as determined by the permissions group to which you belong). There are two kinds of elements:

- network elements
- composite elements: consist of module elements

From this window, you can create, modify, or delete domains and network elements; check the status of elements; upload configurations from the devices to your database; download configurations from your database to devices; and initiate checks on configurations (check the validity of connections, for example).

You can also import network elements into domains from a text file, using a command line script.

Composite Elements

Cisco IP Manager manages elements, domains, and composite elements. A composite element is a physical entity in the management network that contains interconnected network elements, and it has a unique name, just as does any element.

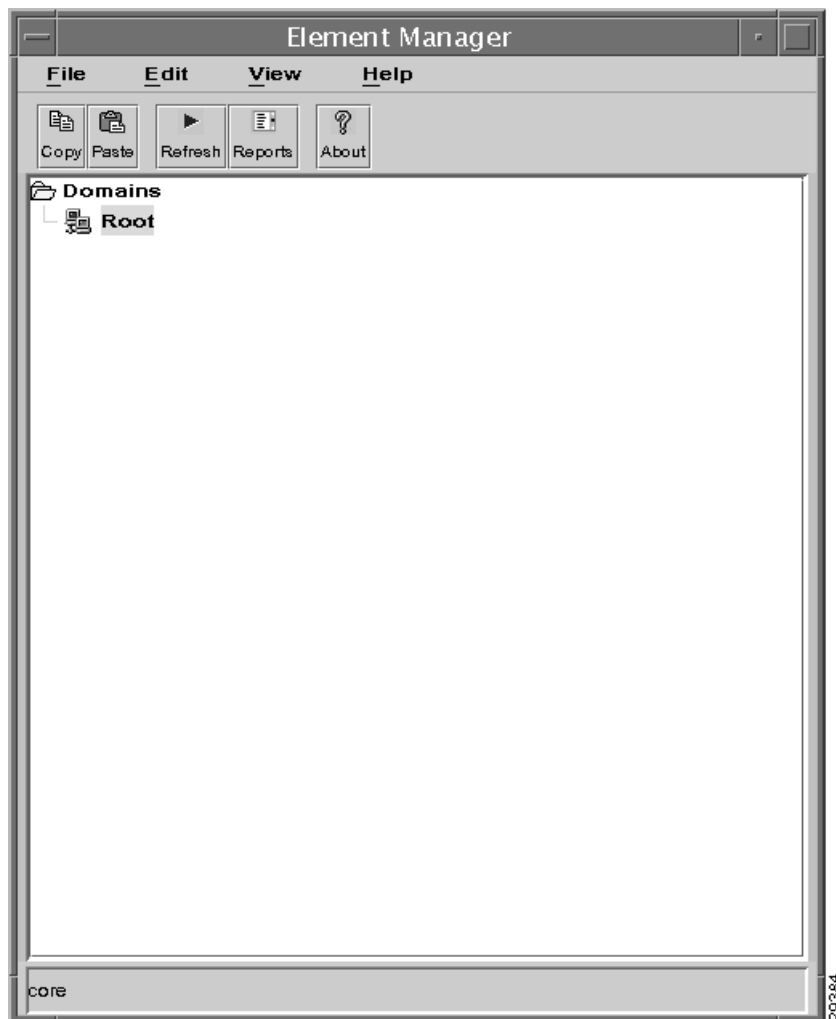
Note The SNMP connection type is not supported for composite elements.

Element Manager Window

The **Element Manager** window displays devices and domains in an expandable tree structure. The `root` entry under the heading **Domains** is reserved for system use. Only the system administrator (login `admin`) can add to the root level; all that user can add at the root level are subdomains. Elements and composite elements can be added only to subdomains beneath the root level.

The top level in the data tree is the highest-level domain that you have permission to view. When you log in and look at the **Element Manager** or **Template Manager** window, you see only as much of the data tree as the system administrator gave you permissions for. See Chapter 7, “System Administration and Log Management,” for more information about permission groups.

Figure 5-1 Element Manager window



The **Element Manager** window contains four menus and five buttons.

The **Element Manager** window contains the following menus:

File Menu

The **File** menu contains the following commands:

- **Close**—closes the **Element Manager** window.
- **Exit**—closes all Cisco IP Manager windows and exits the GUI application.

Edit Menu

The **Edit** menu contains the following commands:

- **Copy**—copies any selected (highlighted) domains and elements to the clipboard. You can then paste them into a template data object in the **Config Builder**, or paste copied elements into a different domain in the **Element Manager**. (For more information about the **Config Builder**, see Chapter 6, “Managing Templates.” For information about how to select multiple items, see “Procedural Conventions” on page ix.)
- **Paste**—pastes copied domains into a template data object in the **Config Builder** or copied elements into a different domain in the **Element Manager**. (For more information about the **Config Builder**, see Chapter 6, “Managing Templates.”)

View Menu

The **View** menu contains the following commands:

- **Refresh All**—causes the data in the tree structure displayed in the **Element Manager** window to be updated.
- **Refresh Selection**—cause the selected node in the data tree to be updated immediately (useful to overcome delays in showing changes you have made, particularly in a distributed environment).

Help menu

The **Help** menu contains the following command:

- **About**—displays the **About IP Manager** dialog.

Creating Domains

Every domain you create is a child of some other domain. To be able to create a domain, you must belong to a permissions group that has been granted *create* permission in the parent domain.

To create a new domain, right-click on the parent domain and choose the **New** option from the floating menu that opens, then choose the **SubDomain** command from the submenu. Enter a domain name in the dialog that opens and click the **OK** button (or click the **Cancel** button to close the dialog without adding a new subdomain).

Name Restrictions

Any name that is stored in the database (domain, element, template, template data, user, or permission group) can consist of any combination of alphanumeric characters (letters can be either upper or lower case) plus the underscore character, hyphen, and period. Names cannot contain leading, trailing, or embedded spaces.

Domain Properties

When you click **New** and then **SubDomain** on the floating options menu for a selected domain, and enter a new domain name, the **Domain Properties** dialog opens.

Figure 5-2 Domain Properties dialog

Domain Properties: cipm-lab

Domain

Domain Name: cipm-lab

NEM Server

Name: super60-1.cisco.... Status: In Use

Telnet Gateway SNMP Gateway

NEM Backup Server

Name: <None> Status: Not U...

Telnet Gateway SNMP Gateway

Apply OK Cancel

The **Domain Name** field displays the name you gave the domain in the previous dialog. This is a read-only field. Once a domain has been created, you cannot change its name, except by deleting the domain from the **Element Manager** window and creating a new one.

The tab also contains fields for primary and secondary NEMServers. The **NEM Server** and **NEM Backup Server** group **Name** fields are both drop-down lists containing the names of all NEM Servers currently registered with the Orbix Naming Service (launched as NS when the Cisco IP Manager servers were started). For information about NEM Servers, see the section “NEMServer” in Appendix A, “Advanced Usage.”

Select a server from the **NEM Server Name** list (set to <None> when the properties window opens for the first time) and choose **In Use** from its **Status** list.

If you have multiple NEMServers running and you want to select a backup that is automatically put into service if the primary server becomes unavailable, select a second server from the **NEM Backup Server Name** list. Choose **In Use** from its **Status** list.

Click the **Apply** button at the bottom of the window. The status fields are adjusted to reflect the actual status of the two servers. If both are up and available, the primary server’s status remains set to **In Use** and the backup server’s status is changed to **Standby**. If one of the servers is not up at the time, its status is changed to **Down** and the other server becomes the **In Use** server.

Once you have set the status and clicked the **Apply** button, you cannot manually change the status of a server. The only way to force a change in status is to shut one of the servers down and restart it.

Whenever a server that has been designated either the primary or backup NEMServer goes down, its status is changed to **Down**. When the server becomes available again and there is another NEMServer in use, the status of the newly available server is set to **Standby**.

For example, assume you have designated the server `hostOne` to be your primary NEMServer and the server `hostTwo` to be the backup. If `hostOne` goes down, `hostTwo` automatically becomes the primary server (even though it continues to be shown in the **NEM Backup Server** field in the properties window). The server `hostTwo` remains the primary NEMServer until it is brought down.

This change in status is not known to the GUI application until you close and reopen the **Domain Properties** window.

Note Upon reception of a CORBA Communication exception due to timeout, the Cisco IP Manager GUI initiates the NEM switchover by making the API call

`NetworkAdministration.getDomainAttributes()` to ADM. Since the GUI timeout is long, this can take over 24 minutes. ADM makes the switchover and sends out a domain modification event. The GUI can then make subsequent calls to `NetworkAdministration.getDomainAttributes()`. Every call to `NetworkAdministration.getDomainAttributes()` with a down NEMServer can take up to a minute. Removing the down NEM from the domain property will clear up this delay.

Configuring the Gateway

After selecting a server from the **NEM Server Name** drop-down list, select either **Telnet Gateway** or **SNMP Gateway** to configure the appropriate gateway. Similarly, later selecting a server from the **NEM Backup Server Name** drop-down list, again select either **Telnet Gateway** or **SNMP Gateway** to configure the appropriate gateway.

Note Telnet Gateway and SNMP Gateway properties can be set only by the user `admin` and apply to all domains associated with the selected NEMServer. A NEMServer and its associated TGServer and SGServer can have only one set of Telnet/SNMP properties, regardless of which **Domain Properties** dialog is open when the changes are made.

Configure Telnet Gateway

Figure 5-3 Telnet Gateway Properties dialog

Telnet Gateway Properties: super60-1.cisco.com

Properties

Server Name: super60-1.cisco.com

TFTP

Server: 172.29.102.164 Path:

Communication Attributes

Operation Timeout: 60 Prompt Timeout: 3

Socket Base Port: 9000

Customized Element Login Prompt

User Prompt 1: Username: Password 1: Password:

User Prompt 2: Username: Password 2: Password:

Apply OK Cancel

The page shows the server's name, the TFTP server name and path (relative to `/tftpboot`—if `/tftpboot` is designated as your TFTP subdirectory, this field is empty), communication attributes, and customized element login prompts.

The **Server Name** field is for information only. You cannot change this value.

Values for the **Operation Timeout**, **Prompt Timeout**, and **Socket Base Port** fields were set by server flags when the TGServer was launched. You can change these values.

The defaults for these are:

- **Operation Timeout:** 1200
- **Prompt Timeout:** 10
- **Socket Base Port:** 9000

Values for the **User Prompt 1**, **Password 1**, **User Prompt 2**, and **Password 2** fields were set by the TGServer, with the default values of `Username:` and `Password:`. You can change these values also.

You can set the TFTP server name and path (relative to `/tftpboot`—if `/tftpboot` is designated as your TFTP subdirectory, leave this field empty) here.

For information on how to change any of these values at launch time, see the section “Changing Environment Variables and Server Launch Flags” in Chapter 3, “Installation and Configuration.”

Configure SNMP Gateway

Note The SNMP connection type is not supported for composite elements.

Figure 5-4 SNMP Gateway Properties dialog

The image shows a window titled "SNMP Gateway Properties: super60-1.cisco.com". Inside, there's a "Properties" tab. The "Server Name" field contains "super60-1.cisco.com". Below it is a "TFTP" section with "Server" set to "172.29.102.164" and an empty "Path" field. The "Communication Attributes" section has "Operation Timeout" set to "20". The "SNMP Attributes" section contains two columns of fields: "SNMP Version" (1), "Retries" (2), "Read Community" (public), "SNMP Timeout" (5), "Trap Port" (162), and "Write Community" (private). At the bottom are "Apply", "OK", and "Cancel" buttons.

The page shows the server's name, the TFTP server name and path (relative to `/tftpboot`—if `/tftpboot` is designated as your TFTP subdirectory, this field is empty), operation timeout value, and several SNMP attributes.

The **Server Name** field is for information only. You cannot change this value.

Values for the **Operation Timeout** and SNMP attributes fields were set by the SGServer properties file (`install_dir/sgs/bin/sgs.properties`) when the SGServers were launched. You can change these values.

For information on how to change any of these values at launch time, see the section “Changing Environment Variables and Server Launch Flags” in Chapter 3, “Installation and Configuration.”

Saving Properties

When you have selected the desired servers and configured their associated gateways, click the **Apply** button to apply the properties to the domain and leave the **Domain Properties** window open, or click the **OK** button to apply the properties and close the window.

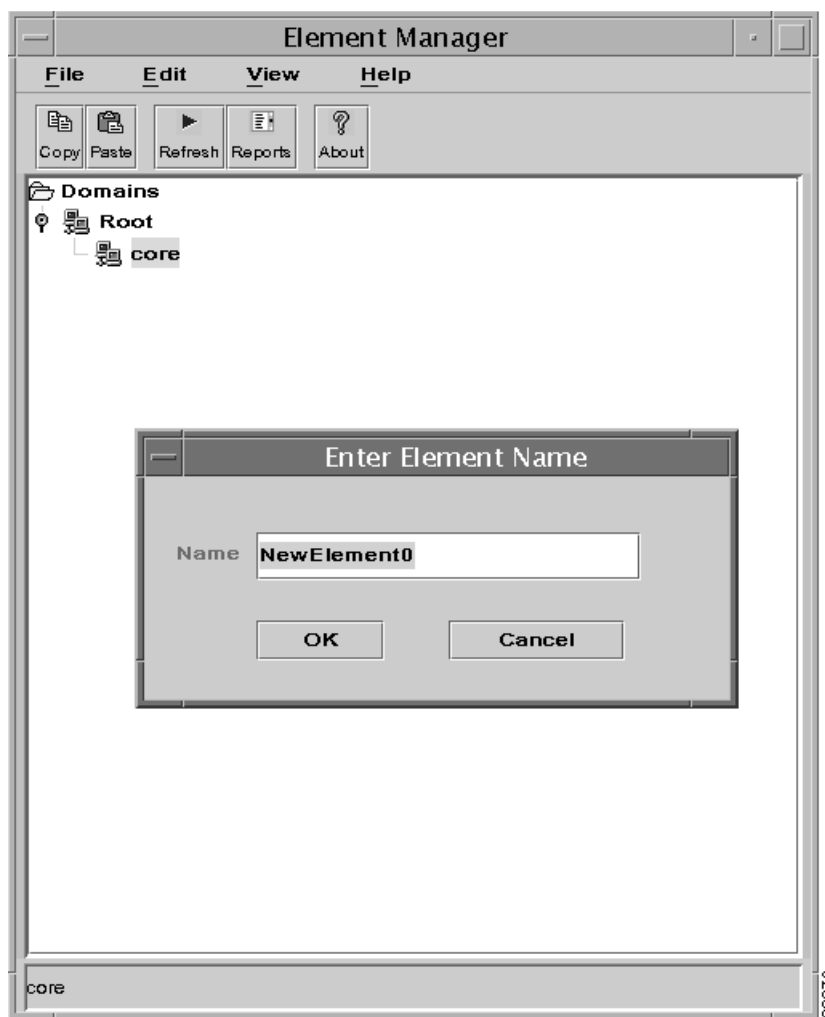
Creating Elements

To create a network element, you must belong to a permissions group that has been assigned *create* permissions for elements for the domain, on the **Domain Permissions** tab in the **Permission Manager** window. You can create a network element or a composite element.

Creating a Network Element

Right-click the mouse on a domain name in the data tree and select the **New** command, then select the **Element** command on the submenu that opens. Enter a name in the dialog that opens and click the **OK** button (or click the **Cancel** button to close the dialog without creating an element). When the **Enter Element Name** dialog appears, the name `NewElement0` appears and is highlighted. You can replace this name just by starting to type a new name.

Figure 5-5 Enter Element Name dialog



See the section “Name Restrictions” elsewhere in this chapter for limitations on characters in names.

The device is added to the data tree displayed in the **Element Manager** window. If it does not appear, you may have to choose the **Refresh** command on the **View** menu.

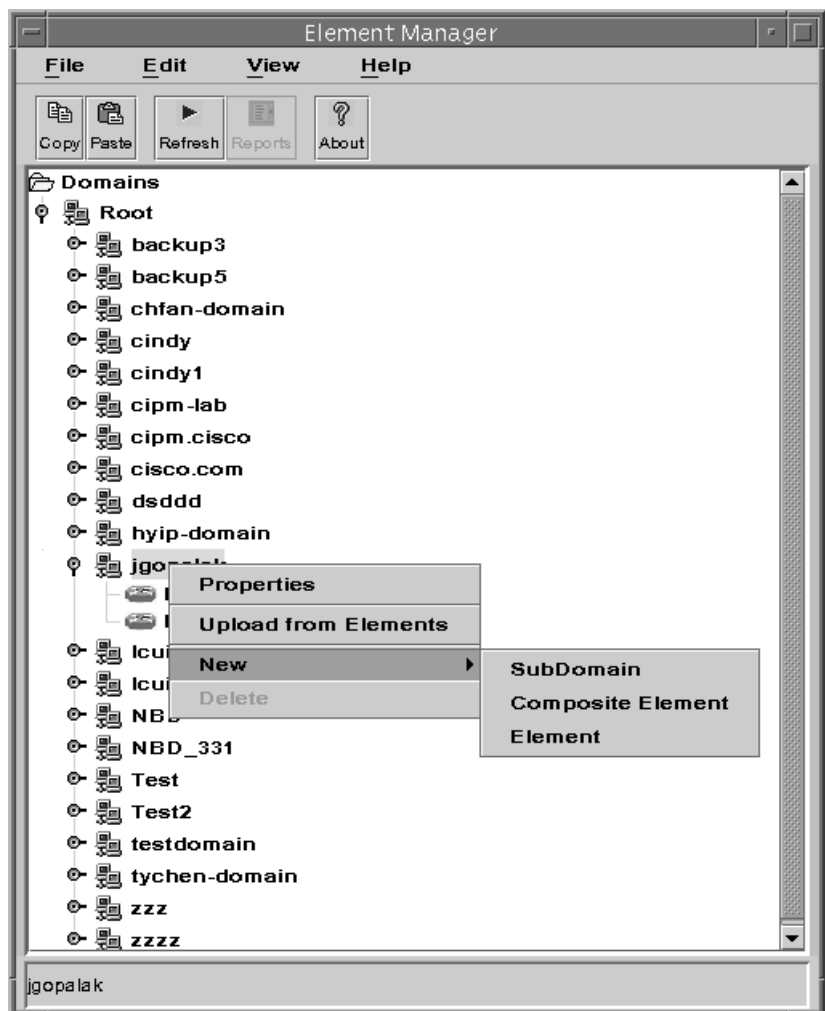
Note Failure to update the data tree could also indicate a problem with the Event Server. If this server is no longer running, you should restart all servers.

If the **Element Manager** window fails to display previously created elements in the data tree, right-click on the domain, click on the **Properties** command in the floating menu that opens, and click the **Apply** or **OK** button in the **Domain Properties** window. (If the NEMServer status has changed to **Down** and then back to **In Use**, the GUI application code can sometimes fall out of synchronization with the actual state of the server as shown in the **Domain Properties** window. The GUI can take over 24 minutes to time out before initiating the NEM switchover.)

Creating a Composite Element

Right-click the mouse on a domain name in the data tree and select the **New** command, then select the **Composite Element** command on the submenu that opens.

Figure 5-6 Element Manager: New Composite Element



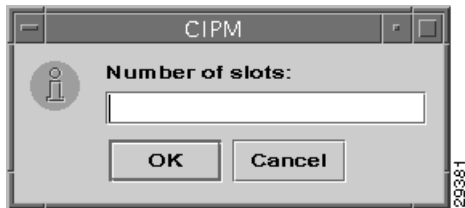
Enter a name in the dialog that opens and click the **OK** button (or click the **Cancel** button to close the dialog without creating an element). When the **Enter Element Name** dialog appears, the name `NewElement0` appears and is highlighted. You can replace this name just by starting to type a new name.

Figure 5-7 Element Manager: Enter Composite Name dialog



When you click the **OK** button, a dialog appears requesting the number of slots. Enter the number of slots associated with the composite element, up to a maximum of 100.

Figure 5-8 Element Manager: Number of slots dialog



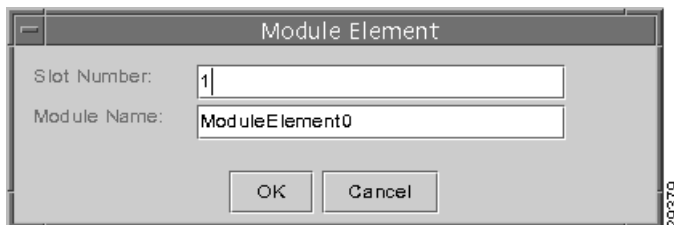
This creates a new composite element. You can then create module elements beneath this composite element, in the same manner as described under “Creating a Network Element.”

The number of module elements that you can create under a composite element is limited by the number of slots you specify when creating a composite element.

Creating a Module Element

You create a module element beneath a module element. Do this by right-clicking on a composite element, and choosing the New Element dialog. Specify the slot number, and the new module element name, and the Element Manager creates a new module element.

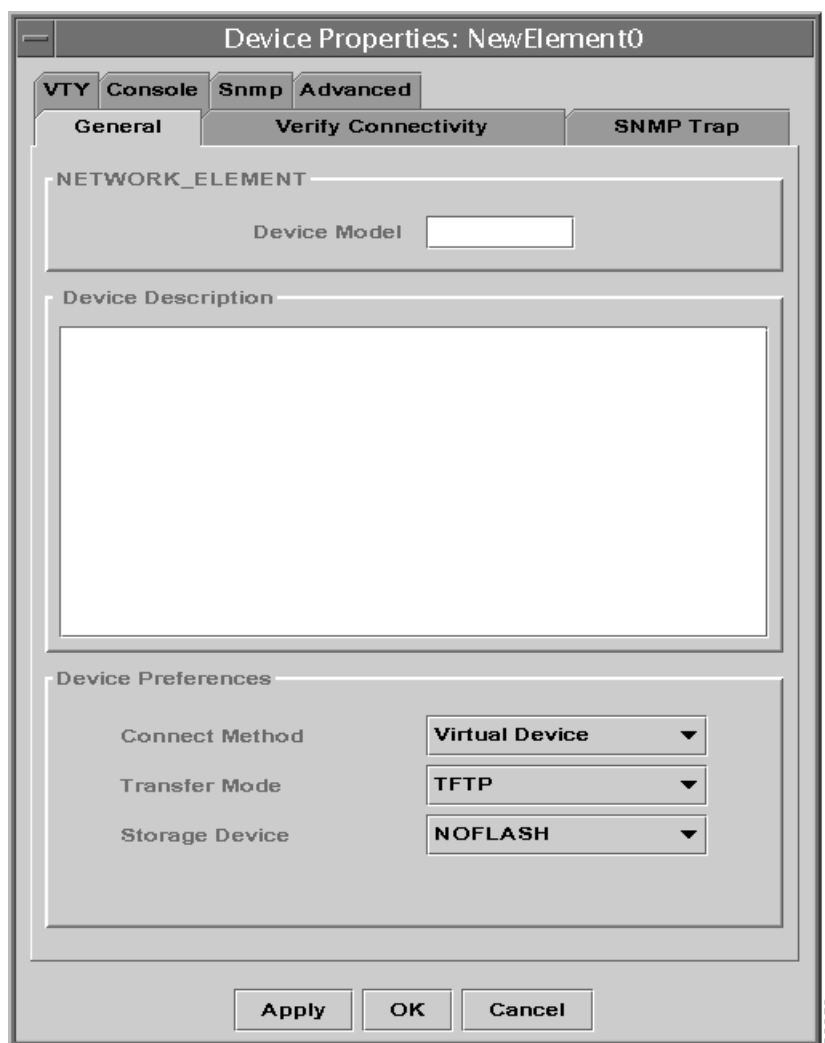
Figure 5-9 Element Manager: Module Element dialog



Element Properties

To specify or edit the properties of a network element, right-click on the newly added device in the data tree and select the **Properties** command from the floating menu that opens. The **Device Properties** dialog is displayed, with the **General** tab selected.

Figure 5-10 Device Properties dialog



This dialog tells the Cisco IP Manager software what property values—IP addresses, user names, passwords, and port numbers (depending on what is selected in the **Connect Method** list)—should be used when communicating with the selected device.

The **Device Properties** dialog has seven tabs. You can supply values on any or all of the tabs, depending on which are applicable. When you have filled in values on all the tabs, click the **Apply** button to apply the properties to the device and leave the **Device Properties** window open, or click the **OK** button to apply the properties and close the window. You do not need to click the **Apply** button before switching to another tab; clicking **Apply** at any time applies the values you have filled in on all the tabs. Or, click the **Cancel** button to close the window without saving the changes you have made anywhere in the dialog.

You enter information into the appropriate tab for the connect type. You can accept the defaults on some of the tabs, but some fields must be filled in. These are validated when that connect method is selected. For example, if you select SNMP as the connect method for a device, and have not entered a value in the **Device IP Address** field, Cisco IP Manager issues an error. The dialog offers multiple tabs to fill out because elements can support multiple connect methods.

General Tab

The **General** tab has three sections; two are for informational purposes only.

In the **NETWORK_ELEMENT** section, the **Device Model** field holds a value you enter for the name of the device. This field is functions as a reminder or comment, and is not validated. You can enter up to 16 characters in this field.

Similarly, the **Device Description** field is for informational purposes only. You can enter up to 30 characters in this field.

The remaining fields, in the **Device Preferences** section have effect.

Connect Method

Select one of the following choices from the **Connect Method** drop-down list:

- **Virtual Device**—device is not a real device; exists only in memory (and the database), for testing. You can perform any operation on a virtual device; you can provision it using templates; you can create a configuration and download the configuration to the device. When you test a virtual device (including using the **Show** and **Remote Ping** pages in the **Element Status** window), the test always succeeds. The only property you can set for a virtual device that has an effect is a text string designating the model of the device on the General tab, and this is for informational purposes only. **Virtual Device** is the default **Connect Method**.
- **VTY**—device is a real device; the Cisco IP Manager software communicates with this device through a VTY (virtual terminal) port.
- **Console**—device is a real device; the Cisco IP Manager software communicates with this device's console port through the communications server.
- **SNMP**—device is a real device; the Cisco IP Manager software communicates with this device's SNMP agent.

Elements beneath a composite element in the tree have an additional connect method available:

- **Via_Composite**—device is a real device; the Cisco IP Manager software communicates with this device by way of the parent.

Transfer Mode

- **TFTP**— specifies TFTP server communications. To use this mode, you must have specified the TFTP server IP address on the **Telnet Gateway Properties** tab of the **Domain Properties** dialog. For more information, see “Configure Telnet Gateway.”
- **TELNET**—specifies to use the Telnet server communications, that is, use of the Telnet Gateway (TGServer), which you set up in the **Domain Properties** dialog

Currently Cisco IP Manager supports only TFTP for SNMP devices. TFTP is used only for configuration upload and download operations; all other communications between the Cisco IP Manager and a router are Telnet or SNMP.

Storage Device

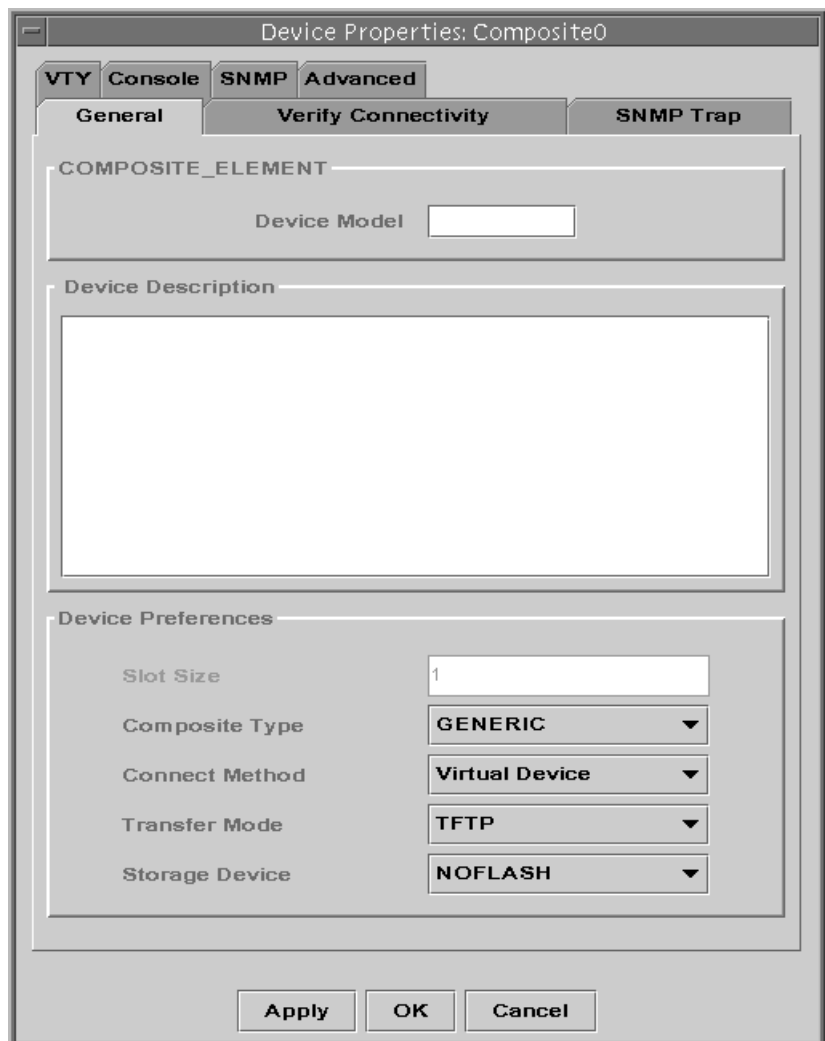
Select one of the following choices from the **Storage Device** drop-down list:

- NOFLASH
- FLASH
- SLOT0
- SLOT1
- NVRAM
- BOOTFLASH
- SLAVESLOT0
- SLAVESLOT1

These devices are described in the element documentation.

If the selected device is a composite element, the appearance of the **General** tab is slightly different:

Figure 5-11 Composite Device Properties dialog



There are two extra fields:

Slot Size

This displays the number of slots you specified as described under “Creating a Composite Element.”

Composite Type

Select one of the following choices from the **Composite Type** drop-down list:

- **GENERIC**—While supported, this type is treated only as a rack card and power supply.
- **BPX**—Not currently supported.
- **MGX**—For example, an 8850.

If the selected device is a module element, the appearance of the **General** tab is again slightly different:

Figure 5-12 **Module Element Device Properties dialog**

Slot Size

This is the slot number being displayed.

Connect Method

Same as described for “General Tab.”

Transfer Mode

Same as described for “General Tab.”

Storage Device

Same as described for “General Tab.”

VTY Tab

The **Using Telnet-VTY to Access Device** control group contains a single field:

- **Device IP Address**—can be in IP address format or as host name (DNS server host must be able to resolve host names)

The **Timeouts/Retries** control group contains two fields.

- **Prompt Timeout**—How long the software waits till it gets a prompt.
- **Operation Timeout**—How long the software waits for a device to complete an operation.

Both of these fields initially contain the value `<default>`. To see what the default values are, click on **Configure TG** in the **Domain Properties** dialog to see the **TGS Server Properties** dialog (as described under “Configure Telnet Gateway”). You can change these values here. If your entry is outside the permitted values, Cisco IP Manager issues an error message when you click **Apply**.

The **Login Security** control group specifies the level of authentication you wish.

Note For composite elements, both the parent and any child elements must specify the same type of authentication mode. Also for composite elements, when the authentication mode is **CIPM Auth**, both the parent element’s authentication password and the child element’s enable password must be configured the same as the current user profile’s router password.

Select one of the following choices from the **Authentication** drop-down list:

- **Element Auth**—uses the values you fill in in the four fields described after **CIPM then Element Auth**.
- **CIPM Auth**—uses the values entered in the **Router User Name** and **Router Password** fields on the currently logged-in user’s **Profile** tab in the User Manager. If the **Router User Name** and **Router User Password** are not set in the User Manager’s **Profile** tab, then the Cisco IP Manager login user name and password will be used to log in to the router. The **Router Enable Name** and **Router Enable Password** should be configured the same as the **Router User Name** and **Router Password**. For more information about setting these values in the User Manager, refer to “Profile” in Chapter 7, “System Administration and Log Management.”
- **CIPM then Element Auth**—first uses **CIPM Auth** for authentication; if that fails, it then uses the values you fill in in the four fields below.

If you choose either **Element Auth** or **CIPM then Element Auth**, then the following fields appear for you to fill in:

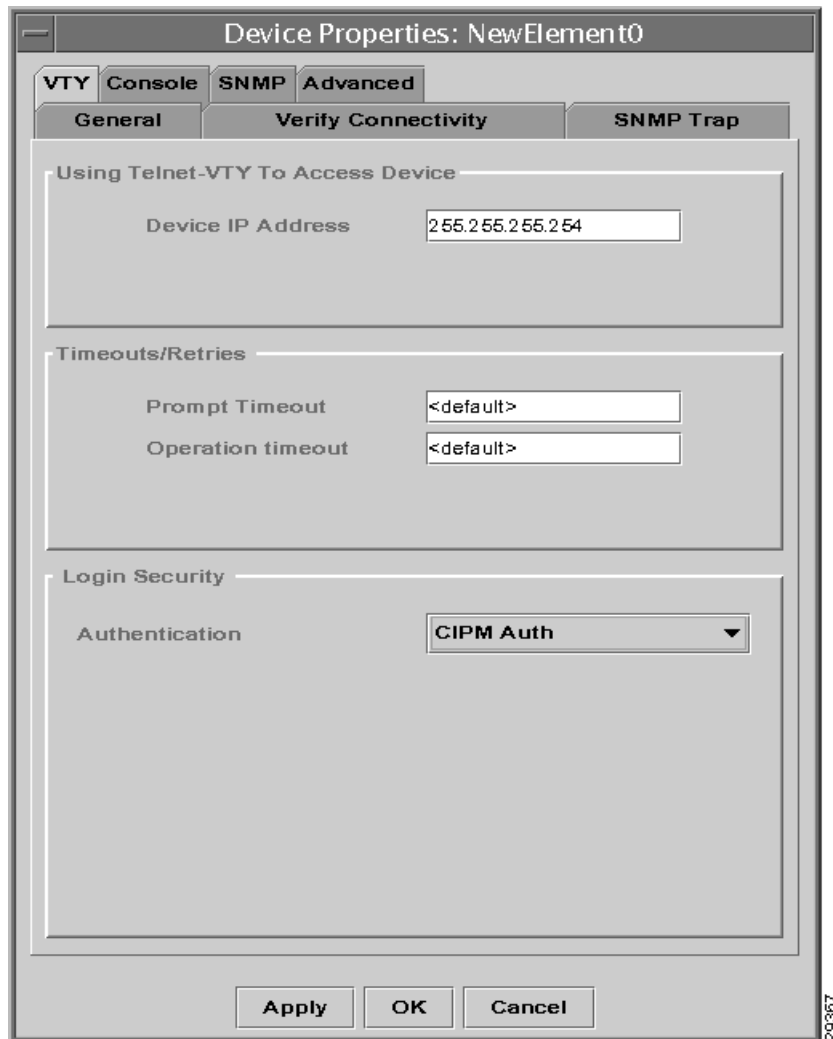
- **User Name**—user name specified in the device's configuration
- **User Password**—user password specified in the device's configuration
- **Enable Username**—user name for entering privileged mode, specified in the device's configuration
- **Enable Password**—password for entering privileged mode, specified in the device's configuration

Figure 5-13 shows the appearance of the dialog with **Element Auth** selected; Figure 5-14 shows the appearance of the dialog with **CIPM Auth** selected.

Figure 5-13 Device Properties Dialog, VTY Tab, Element Authentication

The screenshot shows the 'Device Properties: NewElement0' dialog box with the 'VTY' tab selected. The 'General' sub-tab is active, showing configuration for 'Using Telnet-VTY To Access Device'. The 'Device IP Address' is set to '255.255.255.254'. Under 'Timeouts/Retries', both 'Prompt Timeout' and 'Operation timeout' are set to '<default>'. The 'Login Security' section shows 'Authentication' set to 'Element Auth'. Below this, the 'User Name' is 'quidnunc', 'User Password' is masked with '*****', 'Enable Username' is 'qanat', and 'Enable Password' is masked with '*****'. At the bottom are 'Apply', 'OK', and 'Cancel' buttons. A vertical text '29368' is visible on the right side of the dialog.

Figure 5-14 Device Properties Dialog, VTY Tab, CIPM Authentication



The image shows a screenshot of the 'Device Properties: NewElement0' dialog box. The 'VTY' tab is selected, and the 'General' sub-tab is active. The 'Using Telnet-VTY To Access Device' section contains a 'Device IP Address' field with the value '255.255.255.254'. The 'Timeouts/Retries' section has 'Prompt Timeout' and 'Operation timeout' fields, both set to '<default>'. The 'Login Security' section has an 'Authentication' dropdown menu set to 'CIPM Auth'. At the bottom are 'Apply', 'OK', and 'Cancel' buttons. A vertical text '29367' is visible on the right side of the dialog box.

Device Properties: NewElement0

VTY Console SNMP Advanced

General Verify Connectivity SNMP Trap

Using Telnet-VTY To Access Device

Device IP Address 255.255.255.254

Timeouts/Retries

Prompt Timeout <default>

Operation timeout <default>

Login Security

Authentication CIPM Auth

Apply OK Cancel

29367

Console Tab

Figure 5-15 Device Properties Dialog—Console Tab

Device Properties: Composite0/ModuleElement0

VTY Console SNMP Advanced

General Verify Connectivity SNMP Trap

Using Communications Server

Server IP Address

Server User Name

Server User Password

Port Number

Port Password

Timeout

Prompt Timeout

Operation timeout

Login Security

Console User Name

Console Password

Enable User Name

Enable Password

Apply OK Cancel

The **Console** tab displays the following control groups and fields:

The **Using Communications Server** control group contains the following fields:

- **Server IP Address**—IP address of the device you are using as a communications (or terminal) server. (The Cisco IP Manager software does not support a direct workstation-to-device console connection). Address can be in IP address format or host name if the DNS is set up on the server host.
- **Server User Name**—login user name for the communications server (if one is required).
- **Server User Password**—password for the communications server (if required).
- **Port Number**—communications server port to which the device is connected.
- **Port Password**—password to access the port, if required (password is configured on the commserver lines).

The **Timeout** control group contains the following fields:

- **Prompt Timeout**—How long the software waits till it gets a prompt.
- **Operation Timeout**—How long the software waits for a device to complete an operation.

Both of these fields initially contain the value <default>. To see what the default values are, click on **Telnet Gateway** in the **Domain Properties** dialog to see the **TGS Server Properties** dialog (as described under “Configure Telnet Gateway”). You can change these values here. If your entry exceeds the permitted values, Cisco IP Manager issues an error message when you click Apply. If your entry is outside the permitted range, Cisco IP Manager issues an error message.

The **Login Security** control group contains the following fields:

- **Console Username**—user name specified in the device’s configuration.
- **Console Password**—password specified in the device’s configuration for communicating through the console port (configured on the router’s console line).
- **Enable Username**—user name specified in the device’s configuration for entering privileged mode.
- **Enable Password**—password specified in the device’s configuration for entering privileged mode.

SNMP Tab

Except for **Device IP Address**, the **SNMP** tab uses default values for its fields.

Figure 5-16 Device Properties Dialog—SNMP Tab

Device Properties: NewElement0

VTY Console **SNMP** Advanced

General Verify Connectivity **SNMP Trap**

Using SNMP-VTY To Access Device

Device IP Address 255.255.255.254

Timeouts/Retries

Retries <default>

SNMP Timeout <default>

Operation Timeout <default>

Security

Read Community String <default>

Write Community String <default>

Apply OK Cancel

The **SNMP** tab has three sections.

The **Using SNMP-VTY to Access Device** control group contains a single field:

- **Device IP Address**—can be in IP address format or as host name (NEMServer host must be able to resolve host names)

The **Timeouts/Retries** control group contains three fields.

- **Retries**—How many times the SNMP request is retried; must be in the range 0-50
- **SNMP Timeout**—How long the server waits till initiating a retry; must be in the range 2-600
- **Operation Timeout**—How long the server waits for the entire operation (including all retries); must be in the range 50-1200

The **Security** control group contains two fields.

- **Read Community String**—A string (analogous to a password) passed between the server and the device for an SNMP read operation.

- **Write Community String**—A string (analogous to a password) passed between the server and the device for an SNMP write operation.

All of these fields initially contain the value `<default>`. To see what the default values are, click on **SNMP Gateway** in the **Domain Properties** dialog to see the **SGS Server Properties** dialog (as described under “Configure SNMP Gateway”). You can change these values here. If a numeric entry exceeds the permitted values, Cisco IP Manager issues an error message when you click **Apply**. If your entry is less than the permitted values, Cisco IP Manager substitutes the minimum permitted value.

SNMP Trap Tab

The **SNMP Trap** tab has three sections. Figure 5-17 shows the tab after one address has been moved from the **Enter Trap Source IP Address** field to the **Trap Source IP Addresses List**.

Figure 5-17 Device Properties Dialog—SNMP Trap Tab

Device Properties: NewElement0

VTU Console **SNMP** Advanced

General Verify Connectivity **SNMP Trap**

SNMP Trap

☐ Trap Notification ☐ Trap Forwarder

Trap Community String

Trap Source Interface

Trap Source Ip Addresses List

255.255.255.253

Enter Trap Source IP Address

Add Remove

Apply OK Cancel

29365

The **SNMP Trap** control group contains two buttons and two fields.

- **Trap Notification**—Click this button to specify trap notification on the current element. This button remains checked only if the communication succeeds when you click **OK** or **Apply**.
- **Trap Forwarder**—Click this button to specify trap notification on the current element. When enabled, this specifies to the NEMServer not to configure the router to forward traps to the SGServer Gateway, but to use instead another (third-party) forwarder (for example, HP OpenView). Specify trap forwarding if the router is configured to perform this operation, so that the router doesn't send traps to two places. This button remains checked only if the communication succeeds when you click **OK** or **Apply**.
- **Trap Community String**—A string (analogous to a password) passed between the device and the server for an SNMP trap operation. This can be anything you specify, such as `public`.
- **Trap Source Interface**—The IP address of the agent sending the trap datagram. This is as defined in the configuration file of the router, and can be viewed in the running config. An example is `loopback0`.

The **Trap Source IP Addresses List** control group contains two fields and two buttons. To add addresses to the **Trap Source IP Addresses List**, enter them in the **Enter Trap Source IP Address** field, and then click the **Add** button. To remove addresses from the **Trap Source IP Addresses List**, highlight them and then click the **Remove** button.

Advanced Tab

The **Advanced** tab provides information only. Check boxes indicate whether the following properties are set:

- **Lock**—The NEM Server makes the device unavailable for writer access.
- **Commission**—The NEM Server makes the device available for operations by any user. If the box is not checked, operations are not available to any user

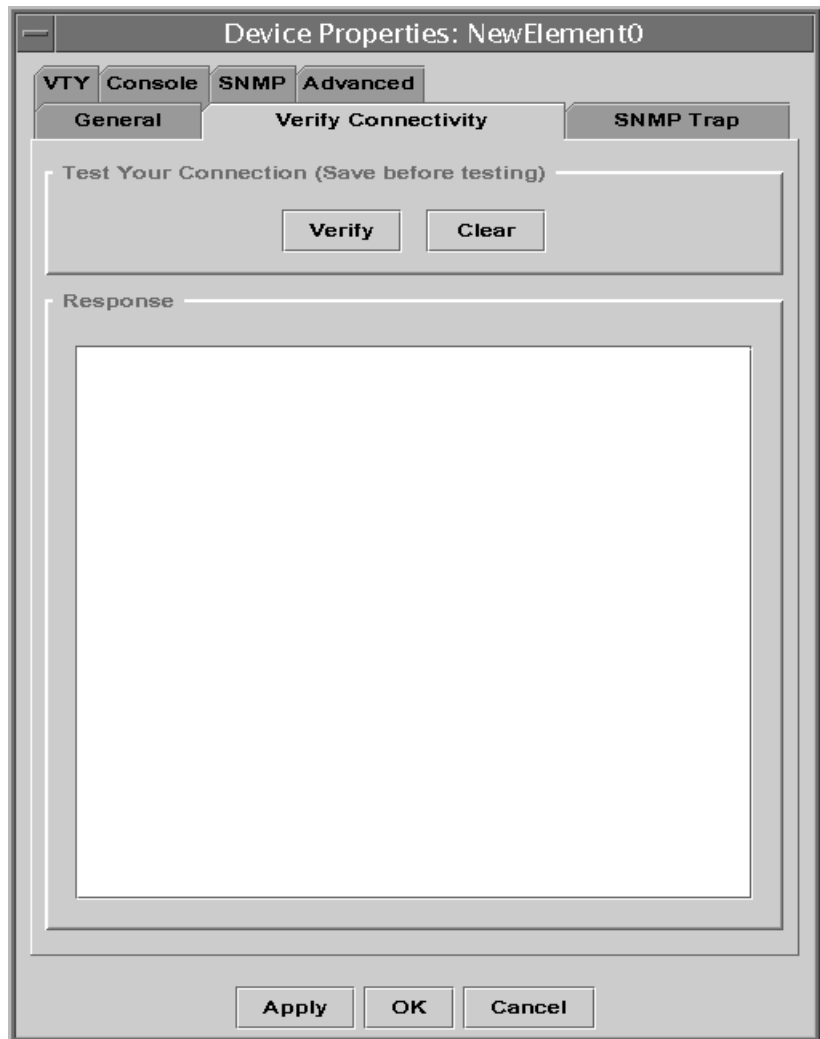
In addition, if the element is locked, the tab shows what user locked it.

To actually make these changes, you right-click on the element (in the **Element Manager** window) and specify **Lock State** or **Commission State**.

Verify Connectivity Tab

Once you have set the properties and saved them (by choosing the **Apply** button at the bottom of the window), select the **Verify Connectivity** tab of the **Device Properties** window to test the properties. This also verifies the TFTP server communications, if you are using it.

Figure 5-18 Device Properties Dialog—Verify Connectivity Tab



Click the **Verify** button to initiate a connection with the device.

The results are displayed in the **Response** window. Use the **Clear** button to clear text from this window.

If the connection cannot be established (incorrect console password or IP address, for example), you receive a general error message.

If the connection can be established but there is an error in the device properties, you receive a more specific error message.

Applying Properties

When you have set the properties, click the **Apply** button to save the data to the database but keep the **Device Properties** dialog open. Click the **OK** button to save the data to the database and close the window. Or, click the **Cancel** button to close the window without saving the changes you have made in the dialog.

Note Apart from checking field size for **Device Model** and **Device Description**, when you click the **Apply** or **OK** button, the GUI does not validate any of the fields you have modified (or left blank).

Importing Elements by Script

You can use the command-line utility **importElement** to add new elements that are defined in a text file. This script is located in the `utility/import` subdirectory of your Cisco IP Manager installation. The script reads a text file that you specify to import elements to a domain. The **importElement** script uses the following syntax:

```
importElement username password filename
```

All parameters are required

Identify elements by entering the device's properties into the text file in the following order:

- element name (required)
- domain name (required)
- element model
- connect method (required; can be **VTY**, **Console**, or **Virtual Device**—*not* case sensitive)
- element's IP address or DNS name (required if connect method is **VTY**)
- element's login user name
- element's user password
- element's enable password
- communications server's IP address or DNS name (required if connect method is **console**)
- communication server's login user name
- communication server's user password
- port number
- port password
- console password
- filename of element's configuration (identifies a file to be imported as the element's working config; can include path)

If a required property is omitted, the element is skipped.

Use commas to separate variables, and new-line characters to separate elements. You can leave fields empty, but there must be a comma for each. Empty lines and lines beginning with the # character are ignored.

The following text file would add a virtual device called `element_1`, another device called `element_2`, which lists **VTY** as the connect method, and a device called `element_3`, which lists **console** as the connect method, to the domain `myDomain`:

```
element_1,myDomain,,Virtual Device,,,,,,,,,
element_2,myDomain,,VTY, 1.2.3.4, cisco, sesame,,,,,,,,,element_2.cfg
element_3,myDomain,,Console,,,,,1.2.3.4,comm_srvr_user_id,
comm_srvr_password,1,port_password,consol_password,/tmp/element_3.cfg
```

The **importElement** utility takes a Cisco IP Manager user name, password, and the name of the import file as arguments. If the user's login name is `ipmgr_user`, the password `ipmgr_password`, and the elements are listed in a text file called `elements` that is in the same directory as the **importElement** utility, then launch the script by entering the following on the command line:

```
./importElement ipmgr_user ipmgr_password elements
```

The domain `myDomain` must already exist in the Cisco IP Manager database, and the person launching the script (the user identified by `ipmgr_user`) must be a valid Cisco IP Manager user with permission to create elements in the domain `myDomain`.

If you are importing a large number of devices with this script, you should close all instances of the GUI application. As each device is added, the Cisco IP Manager servers attempt to update any GUI application that is open. This can consume significant resources and, if the number of devices is very large, the GUI could experience a significant event interruption.

Working Config

To view the device's working config, right-click on the device name and select the **Working Config** command from the menu that appears. For a description of a working config, see the section "Working Config versus Running Config" in Chapter 4, "Running the GUI."

The **Working Config** window opens, with the text of the working config displayed.

Working configs can be created or modified in any of three ways:

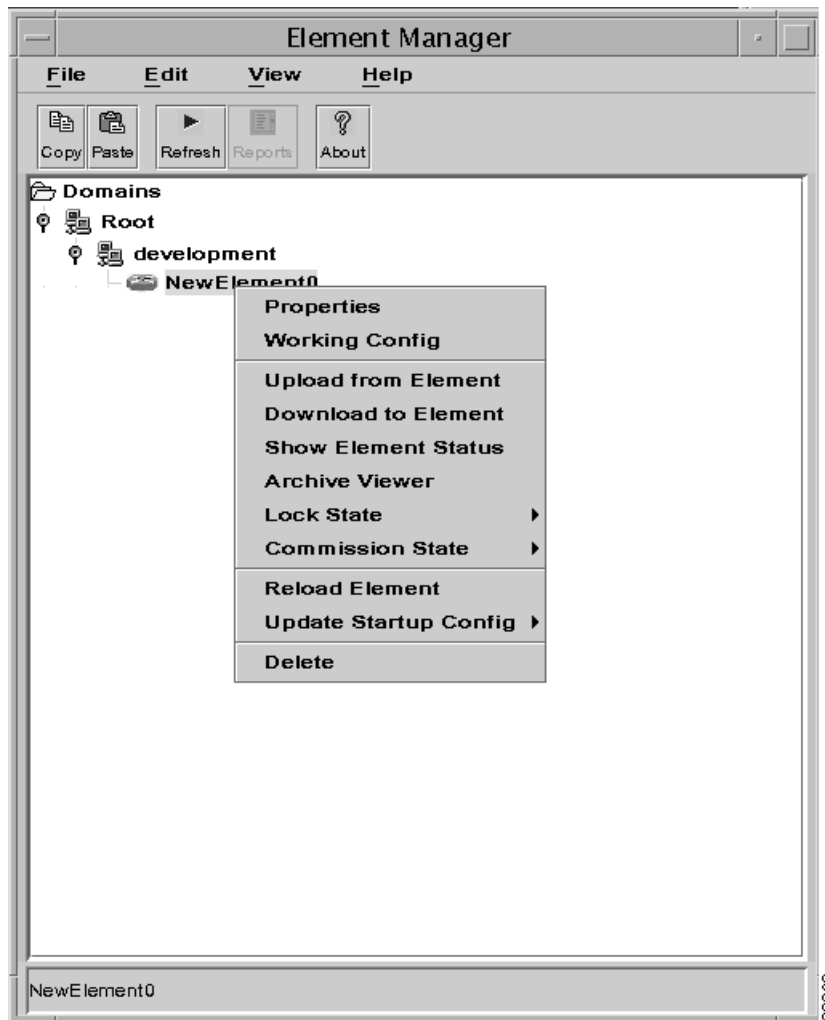
- **Template Config Builder**—when you select the **Commit** command on the **Config** menu, the configuration is written to the database as a working config. (For more information, see the chapter "Managing Templates.")
- **Configuration File window**—you can enter text directly into this window, either from the keyboard or by cutting and pasting from a text editor.
- **Upload from a device**—if a device you have added to your domain is already a running device, you can right-click on it in the **Element Manager** window and choose the **Upload from Element** command.

If you choose the **Import** button at the bottom of configuration **File** window, an **Import Config** window opens.

Working with Devices

Once a network element exists in a domain and you have created a working config, you can use the floating options menu that opens when you right-click the mouse to manage the uploading and downloading of configurations. This can be done either from or to an individual device or from or to multiple devices.

Figure 5-19 Element Manager: options menu



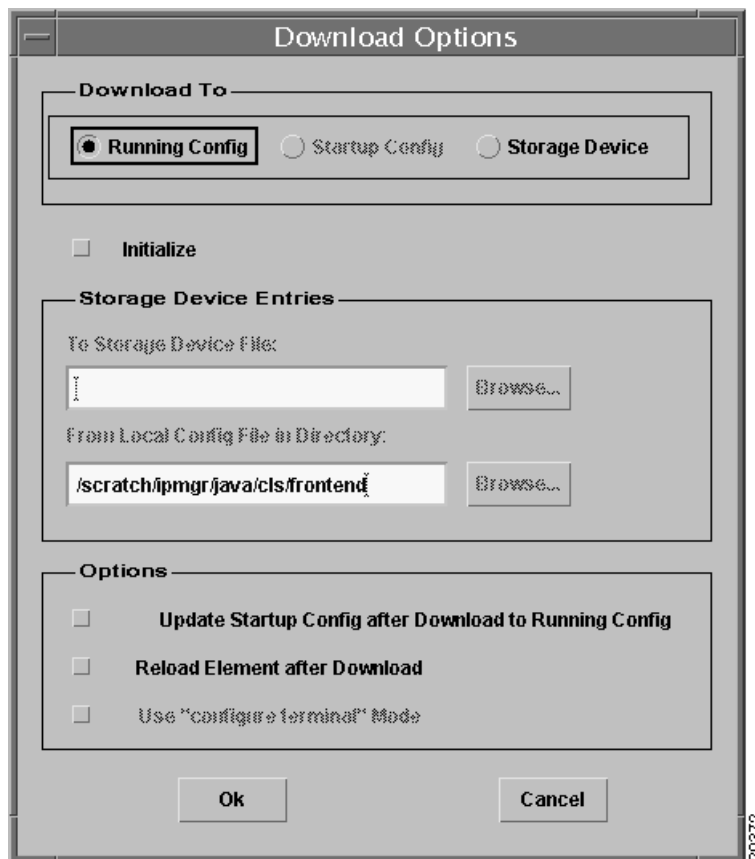
Note The Cisco IP Manager software does not provide any auto-rollback features. Downloads are irreversible unless you have manually saved the previous configurations, prior to the download. To roll back, you must then reimport the saved configurations into the **Working Config** window and download again.

Downloading to a Device

To transmit an existing working config to the device, right-click on the device name in the data tree and choose the **Download to Element** command from the floating menu.

The **Download Options** window opens.

Figure 5-20 Element Manager: Download Options window



Choose the destination of the download operation by clicking the **Running Config**, **Startup Config**, or **Storage Device** button in the **Download To** control group. Other options on the dialog are enabled or disabled according to your **Download To** selection.

Note If you download to flash storage on a GSR device (Cisco 12008 router) that uses Cisco IOS version 11.2(14)GS3, the operation fails. You can download to the specific slot number (for example, slot 0) instead.

If you are configuring a new router for the first time, select the **Initialize** checkbox. (To perform this operation, you must previously have selected the **Console** connect method in the General tab of the **Element Properties** dialog.) You can initialize a device only when the **Running Config** download option is selected; the checkbox is disabled if you are downloading to the **Startup Config**. If you check the **Initialize** option, the **Use “configure terminal” Mode** option is automatically checked (and that mode used) and the option grayed out. You then cannot uncheck this option if you are initializing a device.

Download to Running Config

Select any combination of the following checkboxes in the **Options** group:

- **Update Startup Config after Download to Running Config**—available for selection only when **Running Config** is selected in the **Download To** group; lets you choose whether or not the device's startup configuration is updated after the running configuration has been downloaded.
- **Reload Element after Download**—forces the device to reboot after the configuration has been downloaded (available when **Running Config** or **Startup Config** is selected).
- **Use “configure terminal” mode**—forces the use of **configure terminal** mode (line-by-line transfer) instead of **configure network** mode (TFTP) for the download operation; available only when **Running Config** is selected.

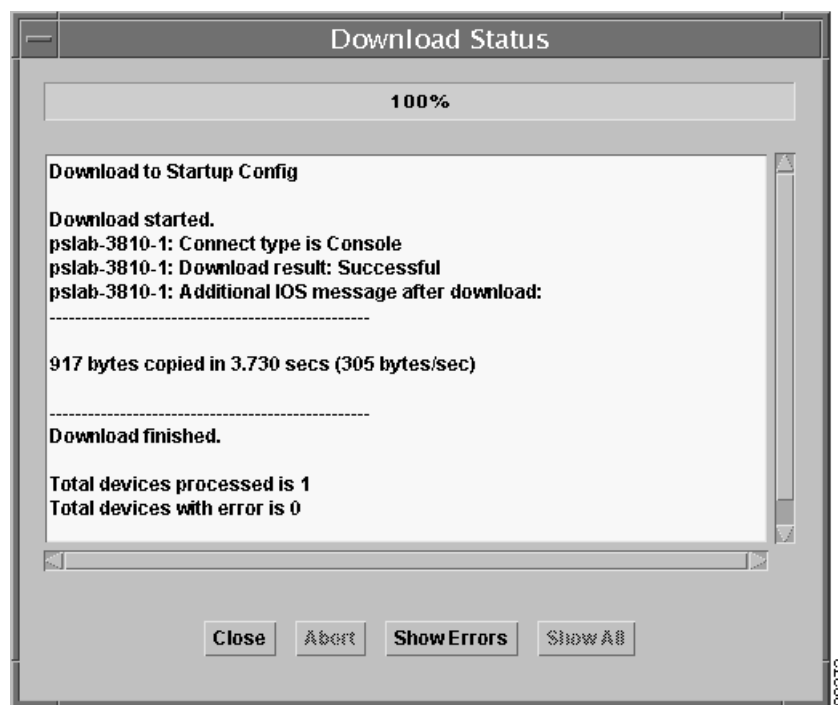
Download to Startup Config

When you are downloading to the startup configuration, only the following option is available:

- **Reload Element after Download**—forces the device to reboot after the configuration has been downloaded (available when **Running Config** or **Startup Config** is selected).

When you have made your selections, click the **OK** button to download the working configuration to the device. The **Download Status** window opens.

Figure 5-21 Element Manager: Download Status window



Click the **Show Errors** button to filter out positive responses from the messages displayed. This allows you to focus on problems that need to be resolved. (Not everything is filtered out of the response window; start, stop, and summary messages about the download operation still appear.)

The **Show All** button reverts to the full display.

Be sure to read all messages completely. Text could have been generated by the Cisco IP Manager GUI application or NEMServer, the Cisco IOS parser, or by the device itself. Sometimes, adjacent messages may appear to contradict each other.

In the following example, it appears at first glance that the **Reload** operation succeeded, but further analysis shows that it did not.

In the first part of the status report, the Cisco IP Manager GUI application reports that the NEMServer has successfully issued the Cisco IOS command **Reload**. This is followed by the subsequent information that the router has returned the message “The date and time must be set first.” This is a fatal error, and the Cisco IP Manager adds the information that, though the command was successfully issued, the operation failed.

```
pslab-2505: Reload successful.
pslab-2505: Additional IOS message after reload:
-----

IOS Reload command succeeded, but reload operation failed:

    "The date and time must be set first"

-----

Reload finished.
```

The message concludes with the information from the NEMServer that the **Reload** attempt is finished.

You should read all messages carefully to determine whether an operation was successfully completed.

Download to Storage Device

You can download a configuration file to a storage device associated with an element by clicking the **Storage Device** button. When you select this option, the **To Storage Device File** and **From Local Config File in Directory** fields are enabled. Specify a file name in the **To Storage Device File** field; the configuration file is then downloaded to the specified storage device in the element. (You specified this storage device in the General tab of the **Element Properties** dialog, as shown earlier under “General Tab.”) You can use any convenient name here, such as `test`.

The **From Local Config File in Directory** field specifies the source file name entry for the configuration file to be downloaded to the storage device. You can specify directly the file name to be downloaded or leave this field blank. If you leave this field blank, Cisco IP Manager selects the configuration file from the default directory or the selected directory, and appends the element name with `.cfg` (`elementname.cfg`). The specific name usually gets generated at the time of upload (if you enabled the option in the dialog to store the configuration file). You can use this procedure for group operations.

Note If you leave the field blank, you must have a valid configuration file (the element name appended with `.cfg`) in the selected directory.

Downloading to Multiple Devices

You can download working configurations to multiple devices in the **Element Manager** window. Select all of the devices you want to configure, then right-click the mouse to open a floating options menu.

Select the **Download to Elements** command. The **Download Options** window described previously opens. When you click the **OK** button, the working configurations for the selected devices download, with the results of each download operation recorded in the **Download Status** window.

You can halt the download process at any time, by choosing the **Abort** button at the bottom of this window. This terminates the download *after* completing the operation in progress. You cannot stop a download operation for a single element.

The messages in the window tell you whether the download operation succeeded or failed for each device.

Uploading from a Device

Right-click on a device name and select **Upload from Element** from the menu that appears. The **Upload Options** window opens. Select source of the upload operation by clicking the **Running Config**, **Startup Config**, or **Storage Device** button in the **Upload From** control group. Options on the dialog are enabled or disabled according to your **Upload from** selection. Then select any combination of the following checkboxes:

- **Non-Tftp Transfer**—this option is disabled when you click the **Storage Device** button.
- **Copy to Working Config**
- **Show Content in Window**—opens a separate **Upload Config File** window, which displays the contents of the configuration (checked by default when window is opened).
- **Export to Local Directory**—enter a path to a valid, existing directory in which you have **write** permission, or use the **Browse** button to locate a destination directory. The configuration is saved to a file using the device's name and the file extension `cfg`.

Note If banner text contains the character # or > (which are used by Cisco IOS as part of a prompt), an upload using non-TFTP transfer mode may result in only a partial configuration being uploaded. We recommend that you use the TFTP transfer mode in this case.

If you click the **Storage Device** button, the **Storage Device File** field is enabled; you can choose the name of a file stored in the storage device of the element. That could be the element's flash memory, or whatever other device you specified in the General tab of the **Element Properties** dialog, as shown earlier under "General Tab." You can use a name that you specified in "Download to Storage Device."

When you have set the options as desired, click the **OK** button to upload the configuration.

The **Upload Status** window opens and a Telnet session is initiated with the device. When the operation is completed, the status of the attempt to upload is displayed in the window's message area. Other than the title in the title bar, this window is identical to the **Download Status** window.

Uploading from Multiple Devices

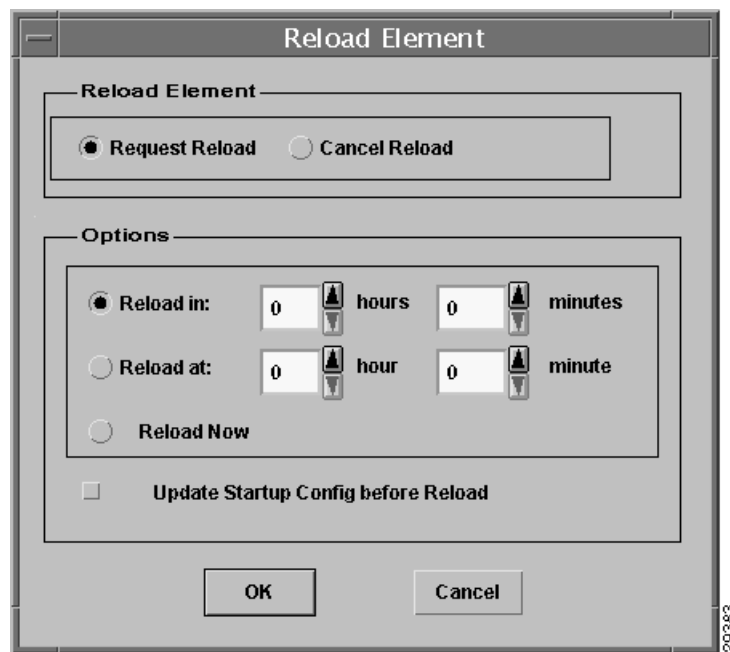
To upload configurations from multiple elements, select the elements from the data tree in the **Element Manager** window and right-click the mouse to open a floating options menu. Choose the **Upload from Elements** command to open the **Upload Options** window.

Reload Element

To force a reboot of the device, right-click on a device name in the **Element Manager** window's data tree and select the **Reload Element** option from the menu that opens. The **Element Reload** window opens.

Note The **Reload Element** commands do not support SNMP.

Figure 5-22 Element Manager: Reload Element window



If you want to update the device's startup configuration from the working configuration, click the **Update Startup Config before Reload** checkbox before forcing the reload operation.

You can choose to reload after a specified interval of time (using the format specified in the dialog), at a specified time of the current day (using 24-hour notation in the **hour** field), or immediately, by choosing one of the following buttons:

- **Reload in**
- **Reload at**
- **Reload Now**

Or, you can click the **Cancel Reload** button to cancel a previously set reload request.

Click the **OK** button to implement your selections.

Update Startup Config

To copy the device's running configuration into its startup configuration RAM, right-click on a device name in the **Element Manager** window's data tree. Select the **Update Startup Config** command from the menu, then select the **Update** command to copy the running configuration to the startup configuration, or select **Erase** to just erase the existing startup configuration.

A confirmation message appears. Click **Yes** to complete the operation.

Show Element Status

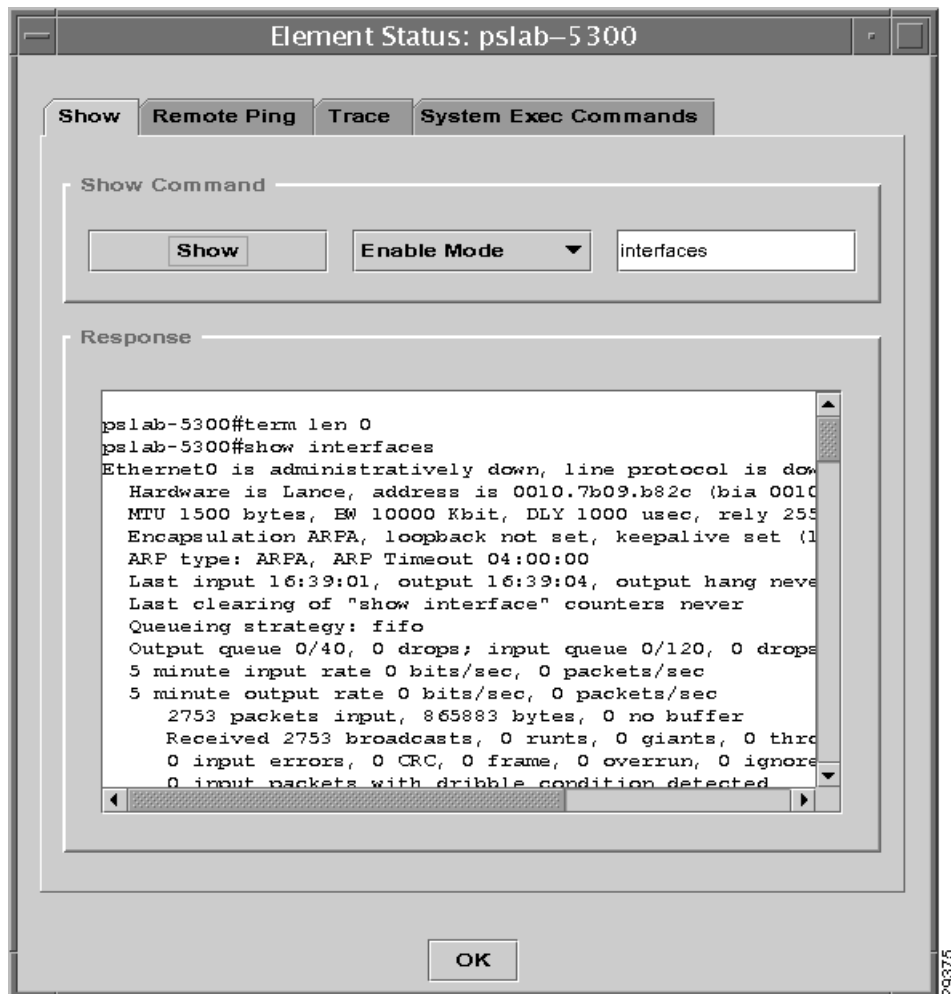
The **Element Status** window, opened by right-clicking on a device and choosing the **Show Element Status** command, executes **Show** and **Ping** commands, and performs **Trace** and **System Exec Commands**.

Note The **Show Element Status** commands do not support SNMP.

Show

Choose the **Show** tab on the **Element Status** window to execute a Cisco IOS **Show** command.

Figure 5-23 Element Manager: Element Status window—Show tab



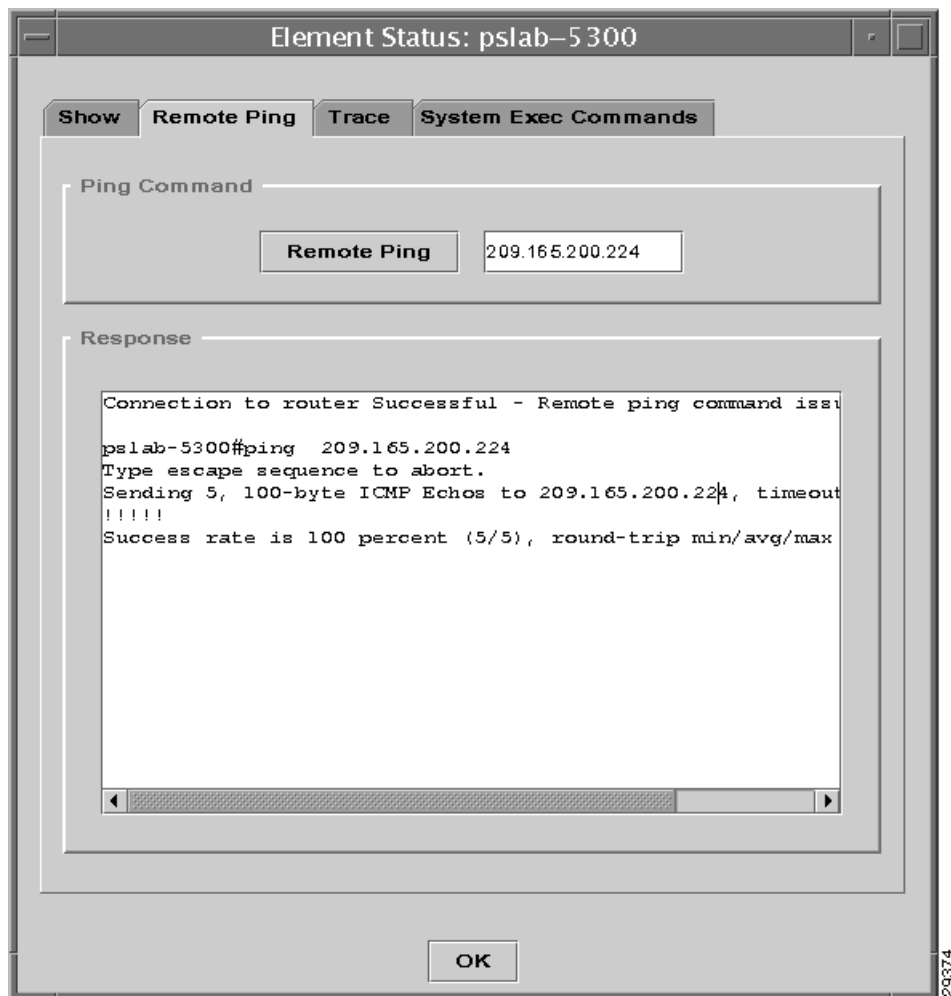
Enter into the editable text field the particular **Show** command you want to send to the device, plus any arguments required. (Do not enter the word `show`; it is supplied when you click the **Show** button.)

Select either **Enable Mode** or **Normal Mode** from the drop-down list, then click the **Show** button. The response is displayed in the **Response** window. For example, Figure 5-23 shows the results of the `Show interfaces` command.

Remote Ping

Choose the **Remote Ping** tab to send a **Ping** command from the router to any device, to verify that the router can communicate with that device.

Figure 5-24 Element Manager: Element Status window—Remote Ping tab



Enter the IP address of the target device into the editable text field, and click the **Remote Ping** button. The reply is displayed in the **Response** window. If the selected router supports host names, you can enter either the IP address or the host name of the target device.

Trace

Choose the **Trace** tab to issue a Cisco IOS `trace` command to determine the routes that packets will actually take when traveling to the destination you specified. The format of the command issued is:

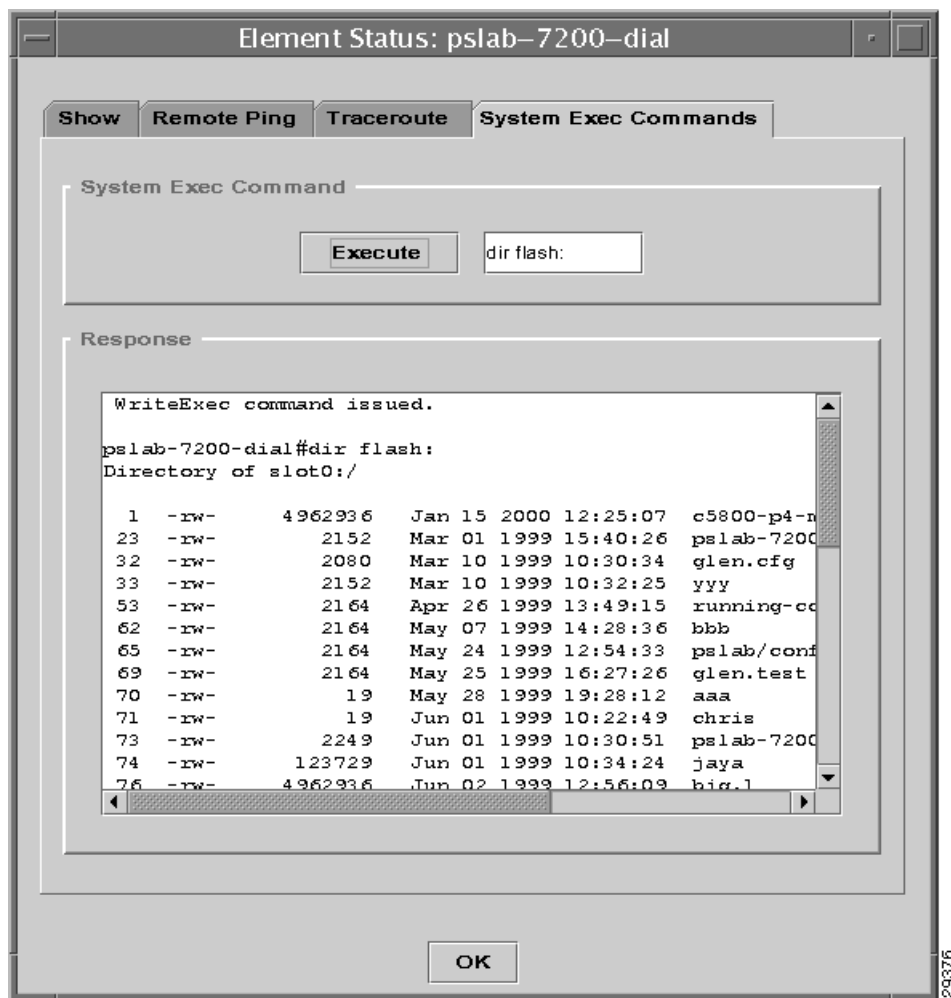
```
trace [protocol] [destination]
```

where *protocol* is one of `appletalk`, `clns`, `ip` (the default), or `vines`, and *destination* is a destination (IP) address.

System Exec Commands

Choose the **System Exec Commands** tab to issue any valid Cisco IOS command. You would use this tab to execute a command that doesn't expect user interaction (which uploads or downloads, for example, `do`).

Figure 5-25 Element Manager: Element Status window—System Exec Commands tab



Enter a command into the field to the right of the **Execute** button, and then click the **Execute** button. The results of the command appear in the **Response** window. For example, Figure 5-25 shows the results of the `dir flash:` command (which shows all the files under `flash`).

Leaving the Element Status Window

To close the **Element Status Window**, click the OK button.

Archiving Elements

To view archive information about an element and to perform operations on stored configurations, right-click on the element and select the **Archive Viewer** option. For more about the operations you can perform, refer to Chapter 8, “Archive Administration.”

When you download a configuration, the Element Manager creates a new version to store in the archive; you can view each version, compare versions, and so on, as also described in Chapter 8, “Archive Administration.”

Deleting Domains and Elements

To delete a domain or an element, right-click on its name in the data tree and choose the **Delete** command from the floating menu that opens. Or, select multiple domains and devices then right-click on any one of the selected names and choose the **Delete** command. When deleting multiple items, a confirmation dialog is displayed; click the **OK** button to confirm. If the deleted items remain in the **Element Manager** window’s data tree, choose the **Refresh All** command (or select the parent node and choose the **Refresh Selection** command) from the **View** menu.

A domain must be empty before you can delete it.

