



Modifying IPM Components

This chapter provides information about modifying IPM components. IPM components include collectors, source routers, target devices, and operations. Information is provided on viewing, updating, and deleting these components.

This chapter contains the following major sections:

- [Working with Source Routers, page 4-2](#)
- [Working with Target Devices, page 4-6](#)
- [Working with Operations, page 4-12](#)
- [Working with Collectors, page 4-20](#)
- [Adding Components Using Seed Files, page 4-25](#)
- [Changing IP Addresses, page 4-33](#)
- [Setting IPM Database Preferences, page 4-35](#)
- [Setting SNMP Timeout and Retry Environment Variables, page 4-41](#)
- [Setting New IPM Server Process Timeout Values, page 4-45](#)
- [Setting the DISPLAY Variable in Solaris, page 4-48](#)
- [Backing Up or Restoring the IPM Database, page 4-49](#)
- [Changing IPM Database Password, page 4-49](#)

Working with Source Routers

IPM source routers are the routers from which you initiate operations for measuring network performance statistics. Each source router must contain the SA Agent feature and an SNMP agent.

Information about working with source routers is provided in the following subsections:

- [Viewing a List of Configured Source Routers, page 4-2](#)
- [Viewing Source Router Properties, page 4-2](#)
- [Adding a New Source Router, page 4-4](#)
- [Deleting Source Routers, page 4-5](#)

Viewing a List of Configured Source Routers

To view a list of configured source routers, select **Edit > Configuration** from the IPM Main window. The Configuration window ([Figure 2-3](#)) appears. By default, Sources is selected in the navigation pane and the Source Configuration window appears within the Configuration window.

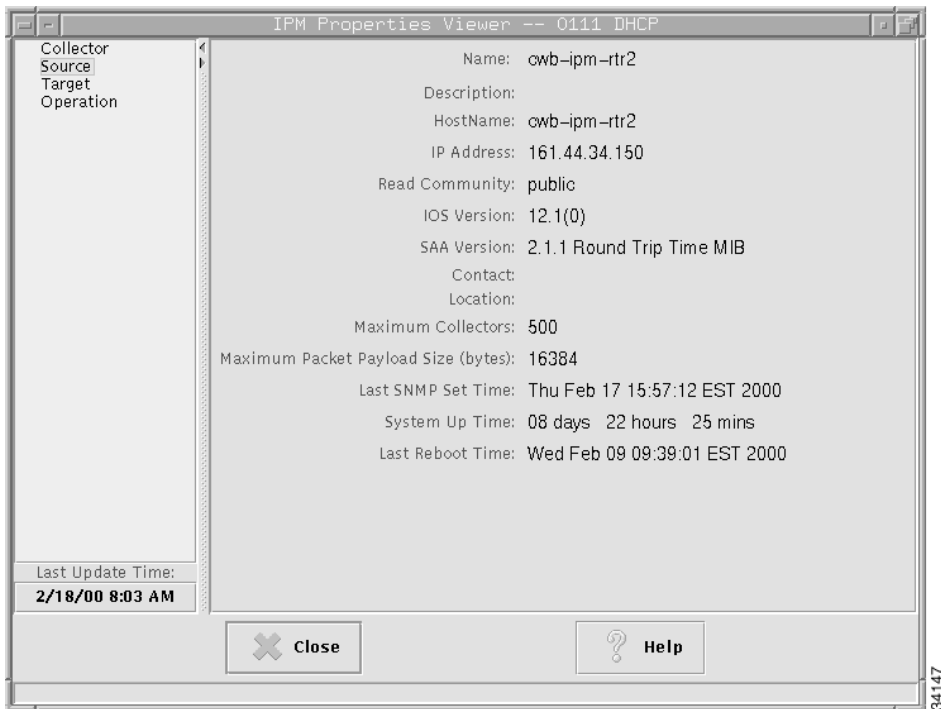
The Source Configuration window displays source routers you have already configured. From this window, you can add a new source router, change the configuration of an existing source, or delete an existing source.

Viewing Source Router Properties

The Source Properties window allows you to view the properties of a defined source router.

To view source router properties:

-
- Step 1** From the IPM Main window, select a collector that uses the source router.
 - Step 2** Select **View > Properties**. The Properties Viewer window appears. By default, the Collector Properties window appears within the Properties Viewer window.
 - Step 3** Click **Source**. The Source Properties window ([Figure 4-1](#)) appears.

Figure 4-1 Source Properties Window

For information about these fields, refer to the “Source Properties Window” topic in the online help.

Adding a New Source Router

Before you can use a router as a source for a collector, you must define the router as an IPM source router.

To add a new source router:

-
- Step 1** (Optional) Verify that the SNMP read community and write community strings are configured properly on the router. Also, if you want to receive traps at your network management system (NMS), verify that the router is configured to send SA Agent-generated traps to your NMS. IPM itself does not receive traps.
- For information about configuring SNMP on the source router, see the “Configuring Your Routers to Send SA Agent-Related Traps” section in the “Preparing to Install” chapter of the *Cisco Internetwork Performance Monitor Installation Guide*.
- Step 2** From the IPM Main window, select **Edit > Configuration**. The Configuration window (Figure 2-3) appears. By default, the Source Configuration window appears within the Configuration window.
- Step 3** In the **Hostname or IP Address** field, enter the IP address or host name of the router on which the source resides. This host name can be from 1 to 64 characters in length.
- Step 4** In the **Read Community** field, enter the SNMP community name for read access to the information maintained by the SNMP agent on the source router. This value can be from 1 to 32 characters in length. Do not include special characters such as ` @ \$ ^ * ' " & |. The default value is “public”.
- Step 5** In the **Write Community** field, enter the SNMP community name for write access to the information maintained by the SNMP agent on the source router. Do not include special characters such as ` @ \$ ^ * ' " & |. This value can be from 1 to 32 characters in length.
- Step 6** In the **Name** field, enter a name to assign to the source router. You can use this field as an alias.
- Step 7** (Optional) In the **Description** field, enter a brief description of the source router.
- Step 8** Click **Add**. IPM attempts to locate the router and determine whether or not it is SNMP-enabled with the correct community string. If the router is successfully located, IPM adds it to the IPM database. If IPM cannot reach the router, IPM displays an error message.



Note If you specify an IP address instead of a host name, and that IP address cannot be resolved by standard address resolution techniques, then IPM displays the IP address for the source router instead of a host name.

Step 9 Click **OK** to close the Configuration window and return to the IPM Main window.

For information about using a seed file to add source routers to IPM, see the [“Adding Components Using Seed Files”](#) section on page 4-25.

Deleting Source Routers

You can delete source routers you no longer need. You can delete more than one source router at a time.



Note If a source router has been configured as part of one or more collectors, you must delete the collectors before you can delete the source router.

To delete a source router:

- Step 1** From the Source Configuration window ([Figure 2-3](#)), select the source router or source routers you want to delete.
 - Step 2** Click **Delete**.
 - Step 3** When the confirmation box appears, click **Yes**. The selected source routers are deleted from the IPM database.
-

Working with Target Devices

IPM targets are destination devices for which you want to gather network performance statistics. A target can be any IP-addressable device, a Cisco router running the SA Agent Responder, or an SNA host.

**Note**

The SA Agent Responder is supported only in Cisco IOS software release 12.1(2)T or later. We strongly recommend software release 12.1 or later.

Information about working with target devices is provided in the following subsections:

- [Viewing a List of Defined Targets, page 4-6](#)
- [Viewing Target Properties, page 4-7](#)
- [Adding a New Target, page 4-9](#)
- [Deleting Targets, page 4-11](#)

Viewing a List of Defined Targets

After you have defined a device as an IPM target, it appears in the list of defined targets in the Target Configuration window.

To view a list of defined targets:

Step 1 In the IPM Main window, select **Edit > Configuration**. The Configuration Window ([Figure 2-3](#)) appears.

Step 2 Click **Targets**. The Target Configuration window ([Figure 2-4](#)) appears.

The Target Configuration window displays a list of all devices defined as IPM targets. From this window, you can define a new target, modify an existing target, or delete a target.

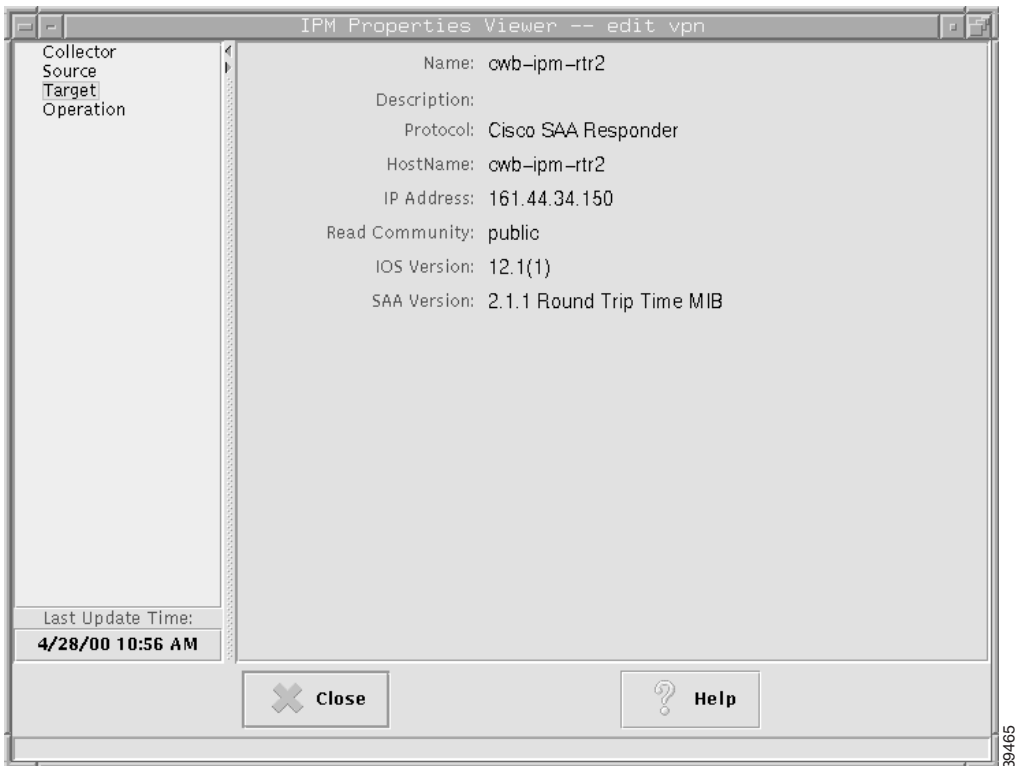
Viewing Target Properties

The Target Properties window allows you to view the properties of a defined target.

To view target properties:

-
- Step 1** From the IPM Main window, select a collector that uses the target device.
 - Step 2** Select **View > Properties**. The Properties Viewer window ([Figure 4-6](#)) appears. By default, the Collector Properties window appears within the Properties Viewer window.
 - Step 3** Click **Target**. The Target Properties window ([Figure 4-2](#)) appears.

Figure 4-2 Target Properties Window



For information about these fields, refer to the “Target Properties Window” topic in the online help.

Adding a New Target

IPM targets are destination devices for which you want to gather data. A target can be any IP-addressable device, an SA Agent Responder, or an SNA host.

To add a new target:

-
- Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window (Figure 2-3) appears. By default, the Source Configuration window appears within the Configuration window.
- Step 2** Click **Targets**. The Target Configuration window (Figure 2-4) appears.
- Step 3** In the **Target Type** field, select the protocol type to be used with this target. The possible values are:
- **IP**—IP/ICMP Echo. Any IP-addressable device. Requires a destination IP address or host name.
 - **Cisco SAA Responder**—Component embedded in a target Cisco router that is running version 12.1 or later of the Cisco IOS software. Its function is to respond to SA Agent request packets from a source router running the SA Agent software. This target type is required for Enhanced UDP operations measuring jitter, or if the target uses the SA Agent (to avoid potential connection problems).

You must enable the SA Agent Responder at the router using the **rtr responder** configuration command.

- **SNA**—SNA LU Type 0 or Type 2 connection to Cisco’s NSPECHO mainframe host application, or SNA SCCP-LU Native Echo. Requires the PU name defined for the SNA PU connection to VTAM.

NSPECHO must be installed on the VTAM mainframe to be used as the target. The NSPECHO application is provided on the IPM product CD. For information about installing NSPECHO, see the “Installing NSPECHO to Measure SNA Response Times” chapter in the *Cisco Internetwork Performance Monitor Installation Guide*.

- Step 4** Based on the **Target Type** you selected, take one of the following actions:
- If you selected **IP**, enter the host name or IP address of the target device in the **Hostname or IP Address** field.
 - If you selected **Cisco SAA Responder**, enter the host name or IP address of the target device in the **Hostname or IP Address** field. In the **Read Community** field, enter the SNMP community name for read access to the information maintained by the SNMP agent on the target device. The default value is **public**.
 - If you selected **SNA**, enter the SNA host name of the target device in the **PU Name** field.
- Step 5** In the **Name** field, enter a name to assign to the target. By default, this field matches the **Hostname, IP Address**, or **PU Name** field, but you can modify the name (for example, to use it as an alias).
- Step 6** (Optional) In the **Description** field, enter a brief description of the target.
- Step 7** Click **Add**. IPM adds the newly defined target to the IPM database.



Note If you specify an IP address instead of a host name and that IP address cannot be resolved by standard address resolution techniques, then IPM assumes that the IP address is valid and does not resolve to a host name.

- Step 8** Click **Close** to close the Configuration window and return to the IPM Main window.
-

For information about using a seed file to add targets to IPM, see the [“Adding Components Using Seed Files”](#) section on page 4-25.

Deleting Targets

You can delete targets you no longer need. You can delete more than one target at a time.

**Note**

Once you have associated a target with a collector, you cannot delete the target without first deleting the collector with which it is associated.

To delete a target:

-
- Step 1** From the Target Configuration window (Figure 2-4), select the target or targets you want to delete.
- Step 2** Click **Delete**.
- Step 3** When the confirmation box appears, click **Yes**. The selected targets are deleted from the IPM database.
-

If you try to delete a target and IPM issues an error message such as **Could not delete the target**, the reason could be:

- The target is being used as a final target by one or more collectors.
- The target is being used as an intermediate hop by one or more Path Echo collectors.

To resolve the problem:

-
- Step 1** Make sure the target is not being used as a final target by any collector. On the IPM Main window, look for the target's name in the Target column. If you find the target's name, you must delete that collector before you can delete the target.
- Step 2** If you still cannot find the target's name, remember that the Path Echo Historical Statistics window shows only the 10 most used paths. To see the rest of the intermediate paths, you must use the IPM Path Usage report. To do so:
- a. On the IPM Server Home Page, select **Configuration Reports > Collectors**. The Collector Information page appears.
 - b. Select the first Path Echo collector in the list and click **Path Usage** in the Details column. The Path Usage page appears.

- c. Click a path to expand it, showing all of its intermediate hops, and look for the target's name. If you find the target's name, you must delete that Path Echo collector before you can delete the target.
 - d. Repeat this procedure for every path under every Path Echo collector.
-

Working with Operations

An IPM operation is an alias for a set of parameters used in measuring performance. Information about working with operations is provided in the following subsections:

- [Viewing a List of Defined Operations, page 4-12](#)
- [Viewing Operation Properties, page 4-14](#)
- [Adding a New Operation, page 4-16](#)
- [Setting Thresholds and Generating Alerts, page 4-16](#)
- [Deleting Operations, page 4-19](#)

Viewing a List of Defined Operations

To view a list of defined operations:

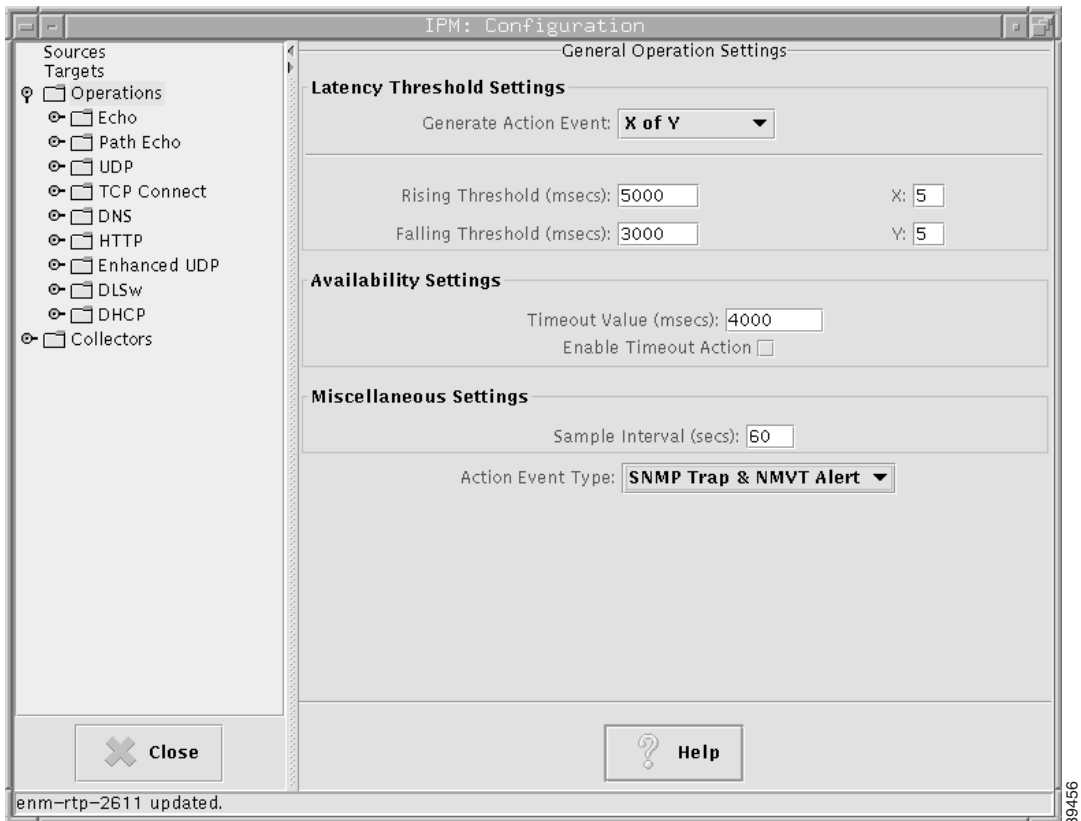
-
- Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration Window ([Figure 2-3](#)) appears.
 - Step 2** Click **Operations**. The list of operations expands to show the types of operations that were defined.
 - Step 3** Click an operation type. The Operation Configuration window ([Figure 4-3](#)) shows the default configuration for the selected operation type and the list of operations expands to show all defined operations of that type.

The Operation Configuration window displays a list of all defined operations. From this window, you can define a new operation, modify an existing operation, or delete an existing operation.

**Note**

When you install IPM, a group of predefined operations is provided. The predefined operations cannot be modified. However, you can use them as templates for creating your own operations. For a listing and brief description of these operations, refer to the [“Defining a Collector”](#) section on page 2-19.

Figure 4-3 Operation Configuration Window

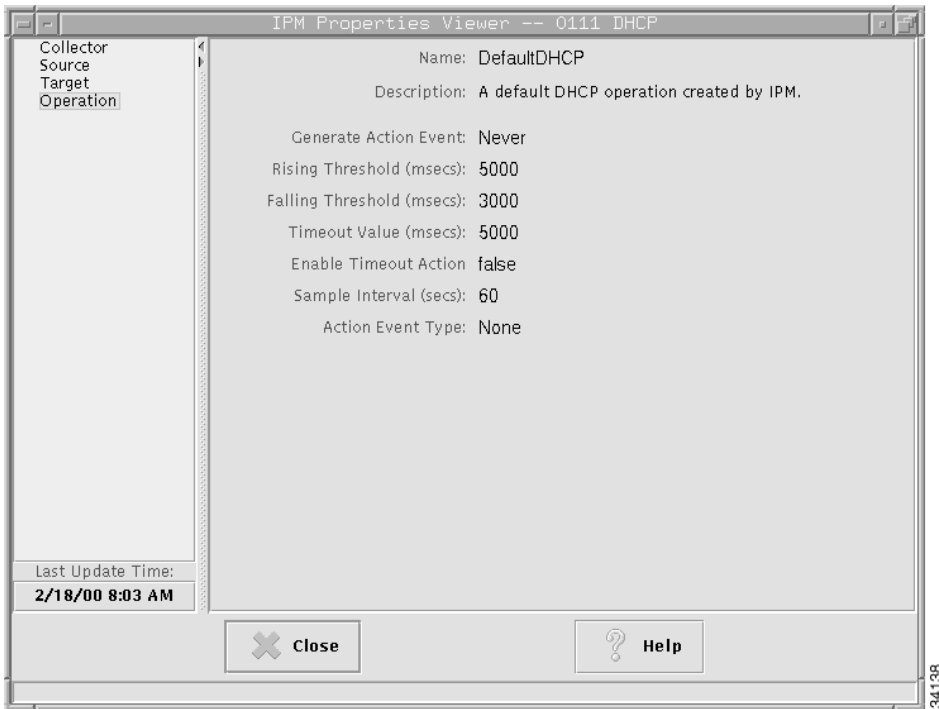


Viewing Operation Properties

The Operation Properties window allows you to view the properties of a defined operation.

To view operation properties:

-
- Step 1** From the IPM Main window, select a collector that uses the operation.
 - Step 2** Select **View > Properties**. The Properties Viewer window ([Figure 4-6](#)) appears. By default, the Collector Properties window appears within the Properties Viewer window.
 - Step 3** Click **Operation**. The Operation Properties window ([Figure 4-4](#)) appears.

Figure 4-4 Operation Properties Window

For information about these fields, refer to the “Operation Properties Window” topic in the online help.

Adding a New Operation

An IPM operation is an alias for a set of parameters used for measuring performance between source router and a target device.

To define an operation:

-
- Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window ([Figure 2-3](#)) appears.
 - Step 2** Click **Operations**. The list of operations expands to show the types of operations that were defined.
 - Step 3** Click an operation type. The Operation Configuration window ([Figure 4-3](#)) shows the default configuration for the selected operation type and the list of operations expands to show all defined operations of that type.
 - Step 4** Set the options for the operation you want to define. Detailed information about defining operations to measure performance for DHCP, DLSw, DNS, HTTP, IP, SNA, TCP, UDP, and Voice over IP is provided in the [“Using IPM to Measure Network Performance”](#) chapter.
 - Step 5** Click **Close** to complete the definition of a monitoring operation. IPM redisplay the Operation window and the new operation is added to the list of defined operations.
-

Setting Thresholds and Generating Alerts

From the Operation Configuration window, you can configure thresholds and event notifications on the source router.

To set thresholds and generate alerts using an operation:

-
- Step 1** Select an existing operation or define a new operation by following the steps in the [“Adding a New Operation”](#) section on page 4-16.
 - Step 2** In the **Generate Action Event** field, select one of the algorithms to be used by IPM to calculate threshold violations. The following values are possible:

- **Never**—Do not calculate threshold violations. This is the default.
- **Immediate**—When the latency exceeds the rising threshold or drops below the falling threshold, immediately perform the action defined by **Action Event Type**.
- **Consecutive**—When the latency exceeds the rising threshold or drops below the falling threshold X times consecutively, perform the action defined by **Action Event Type**. Optionally, specify the number of consecutive occurrences. The default is 5.
- **X of Y**—When the latency exceeds the rising threshold or drops below the falling threshold X out of the last Y times, perform the action defined by **Action Event Type**. Optionally, specify the number of violations that must occur within a specified number. Valid values for both the x-value (X) and y-value (Y) are 1 through 16. The default is 5 for both values.
- **Average**—When the average of the last X completion latency values exceeds the rising threshold or drops below the falling threshold, perform the action defined by **Action Event Type**. Optionally, specify the number of operations to average. The default is the average of the last 5 latency operations. For example, if the collector's rising threshold is 5000 milliseconds and the results of the collector's last 3 attempts are 6000, 6000, and 5000 milliseconds, the average would be $6000 + 6000 + 5000 = 17000/3 > 5000$. The average of these values exceeds the 5000-millisecond threshold, and the action is triggered.

Step 3 In the **Rising** field, enter a rising threshold, in milliseconds. Valid values are between 1 and 99999 milliseconds. The default is 5000 milliseconds. When the latency exceeds the rising threshold, the collector uses the algorithm specified in **Generate Action Event** to determine if a threshold violation has occurred. If a violation occurs, the action defined in **Action Event Type** is taken.

Step 4 In the **Falling** field, enter a falling threshold, in milliseconds. Valid values are between 0 and 99999 milliseconds. The default value is 3000 milliseconds. When the latency falls below the falling threshold, the threshold is reset. Only one event is generated for the time the latency is above the rising threshold.

Step 5 If you specified a **Generate Action Event** of **Consecutive**, **X of Y**, or **Average**, enter a value in the **X** field to be used in calculating the threshold. Valid values are 1 to 16. The default is 5.

Step 6 If you specified a **Generate Action Event** of **X of Y**, enter a value in the **Y** field for the Y value to be used in calculating the threshold. Valid values are 1 to 16. The default is 5.

- Step 7** In the **Timeout Value** field, enter the amount of time, in milliseconds, for the collector to wait for a response to its echo operation. When a timeout occurs, the Timeout counter is incremented. The timeout value must be less than the specified sample interval. Valid values are between 0 and 604800.

The default value is:

- 60000 milliseconds (for TCP Connect operations)
- 9000 milliseconds (for DNS operations)
- 5000 milliseconds (for all other operations)



Note To ensure interoperability with Cisco IOS, the Timeout Values for TCP Connect and DNS operations are fixed at 60000 and 9000 milliseconds, respectively. If you enter some other value, IPM changes the value you enter to the default value.

- Step 8** Enable the **Timeout** option to check for latency reporting operation timeouts based on the timeout value configured for the collector. If you enable the **Timeout** option, the action (specified in **Action Event Type**) is taken when a timeout occurs, or is cleared on this collector.

- Step 9** Enable the **Connection Lost** option to check for connection loss in connection-oriented protocols (LU0, LU2, and SSCP). If you enable the **Connection Lost** option, the action specified in **Action Event Type** is taken when a loss of connection, or a reconnection after a loss, occurs on this collector.

- Step 10** In the **Action Event Type** field, select the action (or combination of actions) for the collector to perform when:

- The **Timeout** option is enabled
- The **Connection Lost** option is enabled
- A threshold is exceeded

For the action type to occur for threshold events, the threshold type must be defined to any value other than **Never**. The possible actions are:

- **Trap**—Send an SNMP trap. Send a trap when a rising threshold is exceeded, a timeout occurs, or a connection loss occurs. Send a second trap when the falling threshold clears, reconnection occurs, or is no longer timing out.

The SNMP traps are sent from the source router to the NMS configured to receive them. IPM itself does not receive or process traps.

- **Alert**—Send an SNA network management vector transport (NMVT) Alert when a rising threshold is exceeded; send an SNA NMVT Resolution when the falling threshold clears.
- **Trap & Alert**—Send both a trap and an NMVT.
- **None**—No action is taken.

Traps and Alerts are sent from the source router to any network management stations that were defined in the source router to receive SA Agent traps or alerts.

- Step 11** Click **OK** to complete the operation definition. IPM adds the new or updated operation to the IPM database.
-

Deleting Operations

You can delete operations you no longer need. You can delete more than one operation at a time.

Collectors that use the deleted operation continue to function correctly.

**Note**

You cannot delete the default operations provided with IPM.

To delete an operation:

- Step 1** From the Configuration window ([Figure 2-3](#)), select the operation or operations you want to delete.
- Step 2** Click **Delete**.
- Step 3** When the confirmation box appears, click **Yes**. The selected operations are deleted from the IPM database.
-

Working with Collectors

A collector is a definition of the source router, the target device, an operation, and the collector schedule. To collect network performance statistics using IPM, you must define a collector.

Information about working with collectors is provided in the following subsections:

- [Viewing a List of Defined Collectors, page 4-20](#)
- [Viewing a Collector State Summary, page 4-21](#)
- [Viewing Collector Properties, page 4-22](#)
- [Adding a New Collector, page 4-23](#)
- [Deleting Collectors, page 4-24](#)

Viewing a List of Defined Collectors

All of the defined collectors are listed in the IPM Main window ([Figure 2-1](#)). Any collectors with start dates and times earlier than the current date and time, and end dates and times later than the current date and time, are considered active collectors.

The following status information appears about each collector in the IPM Main window:

- Collector name
- Source
- Target
- Operation
- Start Time
- Duration
- Type
- Status

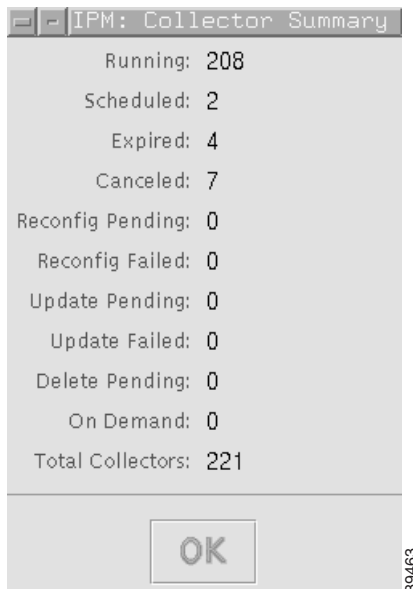
You can sort the collector information displayed in the IPM Main window by clicking on the column titles. By default, the information is sorted based on collector name. Optionally, you can sort the information based on start time, target, or operation type.

Viewing a Collector State Summary

To view a summary of the number of collectors on the server, broken down by current state (Running, Expired, and so on), select **View > Collector State Summary** from the IPM Main window. The Collector State Summary (Figure 4-5) window appears.

For information about these fields, refer to the “Collector State Summary Window” topic in the online help.

Figure 4-5 Collector State Summary Window

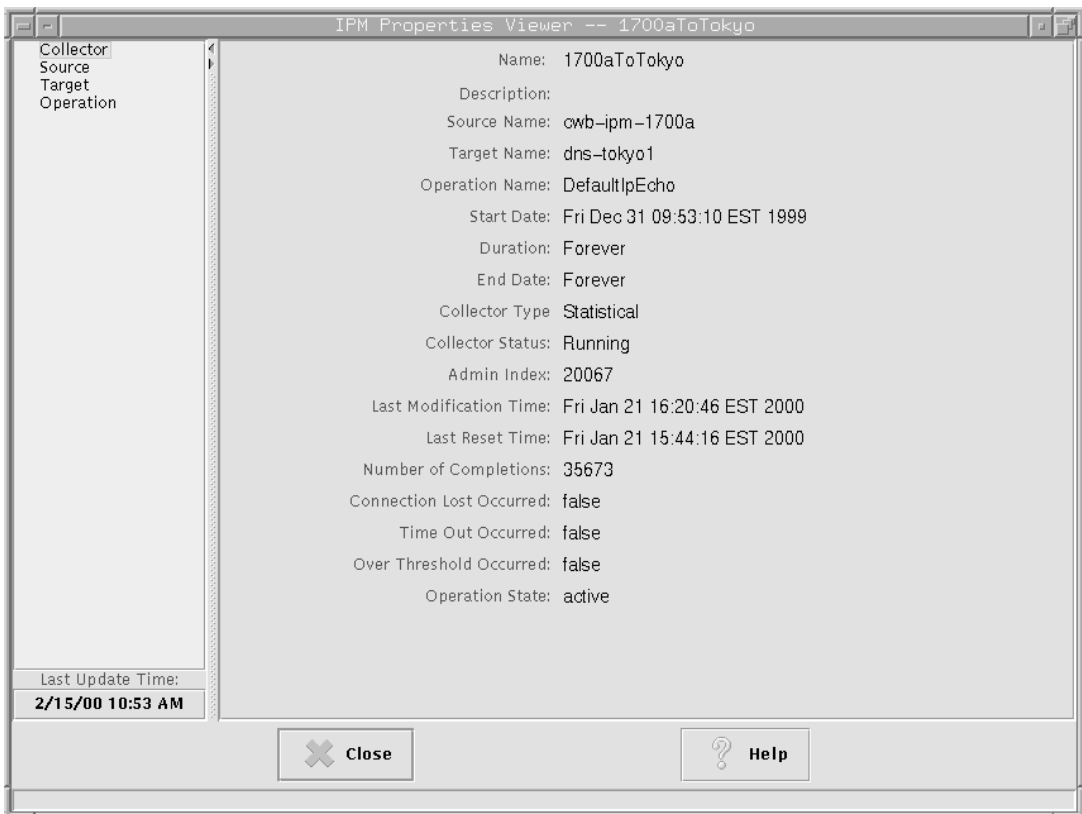


Viewing Collector Properties

To view detailed information about a defined collectors:

- Step 1** From the IPM Main window, select a collector.
- Step 2** Select **View > Properties**. The Properties Viewer window (Figure 4-6) appears. By default, the Collector Properties window appears within the Properties Viewer window.

Figure 4-6 Collector Properties Window



40722



Note If the Collector Properties window is not displayed by default, click **Collector**.

For information about these fields, refer to the “Collector Properties Window” topic in the online help.

Adding a New Collector

Defining a new collector involves selecting a source router, a target, an operation, and a collector schedule.

To define a new collector:

-
- Step 1** From the IPM Main window, select **Edit > Configuration**. The Configuration window ([Figure 2-3](#)) appears. By default, the Source Configuration window appears within the Configuration window.
- Step 2** Click **Collectors**. The Collector Configuration window ([Figure 2-5](#)) appears within the Configuration window.
- Step 3** In the **Name** field, type a name to assign to the collector
- Step 4** (Optional) In the **Description** field, enter a brief description of the collector.
- Step 5** In the **Collector Type** field, enable the **Collect Statistics** option to gather data and store it in the IPM database for future analysis. If this option is not enabled, you can view data in real-time only. Network performance data is not stored in the IPM database. By default, **Collector Type** is set to collect statistics.
- Step 6** Do one of the following:
- To configure the collector without a specific start time or duration so you can postpone starting the collector, click **On Demand**.
 - To define a specific start time and end time, click **Set Date** and enter data in the relevant fields to specify when the collector starts and how long the collector runs. Click **OK**.

For additional information about setting the start time and end time, see the “Set Date Range Window” topic in the online help.

- Step 7** From the **Sources** list, select the router to designate as the source router for collecting data. If you know the name of the router, start typing the name in the **Search** field and the cursor moves to the matching router in the **Sources** list.
- Step 8** From the **Targets** list, select one or more devices to designate as targets. If you know the name of the target, start typing the name in the **Search** field and the cursor moves to the matching target in the **Targets** list.



Note For DNS, DHCP, and HTTP, a target is not required.

- Step 9** From the **Operations** list, select the operation to use for this collector. If you know the name of the operation, start typing the name in the **Search** field and the cursor moves to the matching operation in the **Operations** list.

For a brief description of the predefined operations provided with IPM, see [Table 2-1 on page 2-23](#).



Note IPM does not provide a predefined HTTP operation. Therefore, before you create an HTTP collector, you must first create an HTTP operation. See the [“Adding a New Operation” section on page 4-16](#) for more information.

- Step 10** Click **OK**. IPM adds the newly defined collector to the IPM database.
-

For information about using a seed file to add collectors to IPM, see the [“Adding Components Using Seed Files” section on page 4-25](#).

Deleting Collectors

You can delete collectors you no longer need. When you delete a collector, all data related to that collector is removed from the database, and the collector and the SA Agent entry are removed from the source router. If the selected collector is active, IPM first stops the collector, then deletes it. The collector remains in Delete Pending state until the data is completely deleted from the IPM database. It can take several minutes or more to delete a collector that has a large amount of data stored in the IPM database. You can delete more than one collector at a time.

To delete an IPM collector:

-
- Step 1** From the IPM Main window ([Figure 2-1](#)), select the collector or collectors to delete.
- Step 2** Select **Edit > Delete**.
- Step 3** When the confirmation box appears, click **Yes**. The selected collectors are deleted from the IPM Main window.
-

Adding Components Using Seed Files

In addition to defining source routers, targets, and collectors from their respective Configuration windows, you can define them using seed files. A seed file is a text file containing the information required to define one or more components. This is especially useful if you must add a large number of sources, targets, or collectors quickly.

You must create a separate seed file for each type of component. For example, you cannot mix source router definitions and collector definitions in the same seed file.

The following sections provide detailed information about seed files:

- [Creating a Seed File, page 4-25](#)
- [Loading Components from a Seed File, page 4-31](#)
- [Viewing Seed File Output Files, page 4-32](#)

Creating a Seed File

To create a source router, target, or collector seed file:

-
- Step 1** Using any text editor, create a component-specific seed file following the format described in the [“Seed File Syntax” section on page 4-26](#). Sample seed files for each type of component are shown in the [“Sample Source Router Seed File” section on page 4-28](#), the [“Sample Target Seed File” section on page 4-29](#), and the [“Sample Collector Seed File” section on page 4-30](#).

- Step 2** Save the source router seed file as a text file. The following table lists the default IPM seed file names and directories.

Platform	Default Seed File Name	Default Seed File Directory
Solaris	srcfile.txt	/opt/CSCOipm/etc/source
	trgtfile.txt	/opt/CSCOipm/etc/target
	collfile.txt	/opt/CSCOipm/etc/collector
Windows NT and Windows 2000	srcfile.txt	C:\Program Files\Internetwork Performance Monitor\Server\etc\source
	trgtfile.txt	C:\Program Files\Internetwork Performance Monitor\Server\etc\target
	collfile.txt	C:\Program Files\Internetwork Performance Monitor\Server\etc\collector



Note If you installed IPM in a directory other than the default directory, you must specify that directory instead of */opt* (for Solaris) or *C:\Program Files\Internetwork Performance Monitor* (for Windows NT and Windows 2000).

Seed File Syntax

The top of the seed file contains a comments section for any information you want to note about the file, followed by each component's definition on a separate line.

- In a source router seed file, for each source router you must provide a command, host name, read community string, and write community string.
- In a target seed file, for each target you must provide a command, target type, host name, and for IP or SA Agent Responder targets a read community string.

- In a collector seed file, for each collector you must provide a command, collector name, source router, target device, operation name, start time, duration, and collector type.

You must separate each part of a component's definition with a delimiter. Valid delimiters are spaces, commas (,), semicolons (;), and tabs (\t). Use the same delimiter throughout a given seed file.

Do not begin a component with a comma, semicolon, or tab.

The following example is a valid source router definition, using spaces as delimiters:

```
#a router1 public private
```

If any part of a component's definition contains a space, you must use either a comma or a semicolon as the delimiter between all the parts of that definition. If the host name in the preceding example included a space (for example, router 1), you would use commas or semicolons as delimiters, instead of spaces:

```
#a,router 1,public,private
```

Table 4-1 describes each of the parts of a component's definition.

Table 4-1 Parts of a Component's Definition

Part	Description
Command	<p>Defines whether the source router, target, or collector is added to the IPM database, removed from the IPM database, or whether an existing component entry in the IPM database is updated from the seed file. The following values are possible:</p> <p>A or a—Adds the component to the IPM database.</p> <p>D or d—Removes the component from the IPM database.</p> <p>U or u—Updates an existing component entry in the IPM database from the information provided in the seed file.</p>
Host Name	<p>(Source router and target only) IP address or host name of the router on which the source resides, or of the target device. The host name can be from 1 to 64 characters in length. As an option, you can include an alias for the router by adding a vertical bar () and the alias after the host name.</p>

Table 4-1 Parts of a Component's Definition (continued)

Part	Description
Read Community	(Source router and target only) SNMP community name for read access to the information maintained by the SNMP agent on the source router. This value can be from 1 to 32 characters in length. Do not include special characters such as ` @ \$ ^ * ' " & . This value is usually set to <i>public</i> .
Write Community	(Source router only) SNMP community name for write access to the information maintained by the SNMP agent on the source router. This value can be from 1 to 32 characters in length. Do not include special characters such as ` @ \$ ^ * ' " & . This value is usually set to <i>private</i> .
Target Type	(Target only) The protocol type to be used with this target. Specify one of the following values: 1 —IP. Requires an IP address or host name. 2 —Cisco SAA Responder. Requires an IP address or host name and read community string. 3 —SNA LU0, SNA LU2, or SNA SSCP-LU. Requires a host name.
Collector Name	Name of the collector.
Source	(Collector only) Name of the defined source router to use for this collector. The source router must be defined already in IPM or in a source router seed file.
Target	(Collector only) Name of the defined target device to use for this collector. The target device must be defined already in IPM or in a target seed file.
Operation	(Collector only) Name of the defined operation to use for this collector. The operation must be defined already in IPM.

Sample Source Router Seed File

A sample source router seed file is shown below:

```
#####
#
# This file has example definitions for source routers.
#
# Comments starts with the "#" character
#
# The format of the file is as follows:
#
# <command><delim><hostname[|aliasname]><delim><read community><delim><write community>
```

```

#
# <delim> characters are " ;,\t" "space,semicolon,comma,tab"
#
# <hostname[|aliasname]> : Host name followed by optional aliasName
#                          separated with a '|' ("vertical bar")
#
# The valid commands are 'a|A' for add; 'd|D' for delete; 'u|U' for update;
#
# WARNING: Please assure the permissions on these files
#          do not allow read access to all users due to
#          the inclusions of SNMP community names.
#
#####

#a router1 public private
#a router2 santa claus
#a router3.foobar.com open secret

```

Sample Target Seed File

A sample target seed file is shown below:

```

#####
#
# This file has example definitions for target devices
#
# Comments starts with the "#" character
#
# The format of the file is as follows:
#
# <command><delim><target type><delim><hostname [aliasname]><delim><read community>
#
# <delim> characters are " ;,\t" "space,semicolon,comma,tab"
#
# <hostname[|aliasname]> : Host name followed by optional aliasName
#                          separated with a '|' ("vertical bar")
#
# The valid commands are 'a|A' for add; 'd|D' for delete; 'u|U' for update;
#
# The <target type> is 1 for IP; 2 for CISCO_SAA_RESPONDER; 3 for SNA
#
# For CISCO_SAA_RESPONDER target type, read community string is required.
# and the IOS RTR (SA Agent) Responder must be enabled
#
# WARNING: Please assure the permissions on these files
#          do not allow read access to all users due to

```

Adding Components Using Seed Files

```
#           the inclusions of SNMP community names.
#
#####

#a 1 www.foobar.com
#a 2 ios_router.foobar.com public
#a 3 sna_target.foobar.com
#a 1 server1
#a 2 router1 public
```

Sample Collector Seed File

A sample collector seed file is shown below:

```
#####
#
# This file has example definitions for collectors
#
# Comments starts with the "#" character
#
# The format of the file is as follows:
#
# <command><delim><collName><delim><source><delim><target><delim>
# <operation><delim><startTime><delim><duration><delim><collType>
#
# <delim> characters are " ;, \t "space,semicolon,comma,tab"
#
# The valid commands are 'a|A' for add, 'd|D' for delete, 'u|U' for update;
#
# <collType> is M for Monitored, S for Statistical
#
# <startTime> is in the format MM:DD:YYYY:hh:mm:ss
#
# <startTime> = 1 -> start time will be now
#
# <duration> is in number of hours
#
# <duration> = 0 -> Forever
#
# <startTime> = zero and <duration> = zero -> ON_DEMAND collector
#
# For DHCP, HTTP, and DNS Operation types, the target field must be Unused or unused.
# MyHTTP should be replaced with the name of an HTTP operation you created.
#
# DefaultJitter should be replaced by Default60ByteVoice, Default160ByteVoice,
# DefaultVideo, or DefaultVPN.
```

```
#
#####

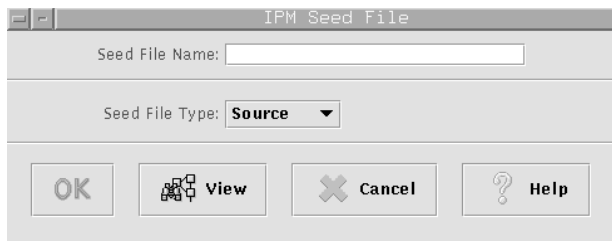
#a coll1 router1.cisco.com target1 DefaultIpEcho 1 12 M
#a coll2 router1.cisco.com target2 DefaultUDPEcho 1 0 S
#a coll3 router1.cisco.com target3 DefaultJitter 1 24 M
#a coll4 router1.cisco.com target4 DefaultDLSw 0 36 S
#a coll5 router2.cisco.com target1 DefaultSnaLu0Echo 1 6 M
#a coll6 router2.cisco.com target2 DefaultSnaLu2Echo 1 12 M
#a coll7 router2.cisco.com target3 DefaultSnaRuEcho 1 24 S
#a coll8 router2.cisco.com target2 DefaultIpPathEcho 10:20:1999:01:00:00 36 M
#a coll9 router.cisco.com Unused DefaultHTTPTConn 1 0 S
#a coll10 router.cisco.com Unused MyHTTP 1 0 S
#a coll11 router.cisco.com Unused DefaultDNS 1 0 S
#a coll12 router.cisco.com Unused DefaultDHCP 1 0 S
#####
```

Loading Components from a Seed File

To load components from a seed file into IPM:

- Step 1** From the IPM Main window, select **File > Open Seed File**. The Seed File window () appears.

Figure 4-7 Seed File Window



- Step 2** In the **Seed File Type** field, select **Source**, **Target**, or **Collector** as the type of seed file to load.
- Step 3** In the **Seed File Name** field, type the name of the source router, target, or collector seed file.

- Step 4** Click **OK**. The source routers, targets, or collectors you defined in the router file are added to the IPM database. When you access the Source Configuration, target Configuration, or Collector Configuration window, the changes you made to the components in the seed file are displayed.

If you do not remember the name of the seed file you want to load, you can view a list of available seed files from the Seed File window. Select **Source**, **Target**, or **Collector** as the Seed File Type and click **View**.

For information about listing, viewing, editing, or loading seed files from the command line, see the [“IPM Command Reference” section on page B-1](#).

Viewing Seed File Output Files

When you add a source router, target, or collector using a seed file, you create an output file that indicates whether the addition of the resource was successful. The output file has the same path and name as the seed file, with the addition of the .out suffix. For example, a seed file named labsrfile.txt generates an output file named labsrfile.txt.out. An output file contains the same information as its seed file, with the addition of messages that indicate whether the addition of the resource was successful. For example, if labsrfile.txt contains the following information:

```
a cwb-ipm-1600a public private
a cwb-ipm-1600b public private
a cwb-ipm-1700a public private
```

Then, if the addition of the resources is successful, the output file labsrfile.txt.out would contain the following information:

```
a cwb-ipm-1600a public private - OK
a cwb-ipm-1600b public private - OK
a cwb-ipm-1700a public private - OK
```

If the resources cannot be added for some reason, `OK` is replaced with an appropriate error message. Possible error messages include:

```
ERROR: BAD VALUE PASSED
ERROR: COLLECTOR LIMIT EXCEEDED
ERROR: COLLECTOR NOT FOUND
ERROR: DATABASE ERROR
ERROR: DUPLICATE ENTRY
```

```
ERROR: DUPLICATE NAME
ERROR: INTERNAL ERROR
ERROR: INVALID COMMAND
ERROR: INVALID ENTRY
ERROR: INVALID IOS VERSION FOR TARGET
ERROR: INVALID PROTOCOL TYPE
ERROR: INVALID RTT TYPE
ERROR: INVALID TARGET FOR THE SELECTED OPERATION
ERROR: LOST CONNECTION TO SNMP SERVER
ERROR: OPERATION NOT FOUND
ERROR: SOURCE NOT FOUND
ERROR: TARGET NOT FOUND
```

Changing IP Addresses

When you physically move routers, servers, or other devices, you might need to change their IP addresses. You might also need to change IP addresses as your network grows. If you have a DNS server, IPM enables you to change an old IP address to a new IP address throughout the IPM database.

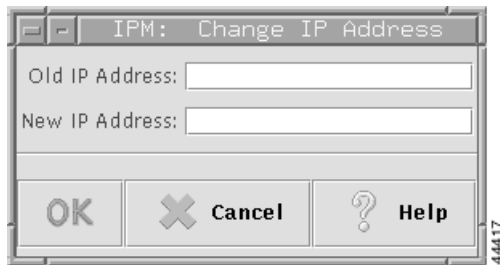


Caution

Changing an IP address changes *every* occurrence of that address in the IPM database, including historical statistics and source and target IP addresses, even if the target is an intermediate hop. Therefore, make sure you want to change *every* occurrence of the IP address in the IPM database before using this procedure.

To change the IP address:

-
- Step 1** Select **Edit > IP Address** from the IPM Main window. The Change IP Address window ([Figure 4-8](#)) appears.

Figure 4-8 Change IP Address Window

- Step 2** In the **Old IP Address** field, enter the old address you want to change. This must be an IP address; it cannot be a host name.
- Step 3** In the **New IP Address** field, enter the new IP address. Do not enter an IP address that already exists in the IPM database. If you do, IPM issues an error message and does not change the old IP address.
- Step 4** Click **OK**. The IP address is changed throughout the IPM database.

The IPM client can seem unresponsive while the IP address is being changed. This is due to the high volume of messages being received by the client during this time.

If you change an IP address, you must wait until the change is complete in the IPM database before making another IP address change.

When you change the IP address of a device, IPM performs two checks. IPM first checks whether the same IP address is used by another device in the IPM database. IPM also checks whether the new IP address is mapped to the same DNS entry as the old IP address, if one existed.

**Note**

You can also change the IP address of a device if it did not have a DNS entry. But the new IP address should map to a DNS entry.

For more detailed information about the Change IP Address window, see the “Change IP Address Window” topic in the online help.

Setting IPM Database Preferences

For collectors that are using a statistical operation, IPM gathers network performance and error statistics from the source router once every hour and stores the data in the IPM database. The collected hourly data is used to calculate daily, weekly, and monthly data.

By default, IPM stores the collected data for the following periods:

- Hourly data for up to 32 days
- Daily data for up to 180 days
- Weekly data forever
- Monthly data forever

The IPM database preferences file allows you to control these parameters and also define the business hours and days. Defined business hours are used in determining the daily, weekly, and monthly averages, whereas business days are used in determining the weekly and monthly averages. The database preferences file also allows you to set the length of time that daily data is retained in the database.

Information about viewing and changing the database preferences is provided in the following sections:

- [Displaying the Current Database Preferences, page 4-35](#)
- [Changing the Database Preferences, page 4-36](#)
- [Database Preferences File Format, page 4-38](#)

Displaying the Current Database Preferences

To display the preferences in the currently running IPM database in Solaris, enter:

```
# cd /opt/CSCOipm/bin
# ./ipm dbprefs view
```

In Windows, enter:

```
cd c:\Program Files\Internetwork Performance Monitor\Server\bin
ipm dbprefs view
```

To display the preferences in the configuration file (which might differ from the preferences in the currently running IPM database), in Solaris, enter:

```
# cd /opt/CSCOipm/bin
# ./ipm dbprefs viewfile
```

In Windows, enter:

```
cd c:\Program Files\Internetwork Performance Monitor\Server\bin
ipm dbprefs viewfile
```

The output from the **view** and **viewfile** versions of this command is formatted differently because **ipm dbprefs view** displays the contents of a *database*, but **ipm dbprefs viewfile** displays the contents of a *file*.

Changing the Database Preferences

To change the IPM database preferences:

-
- Step 1** Edit the IPM database preferences file (*/opt/CSCOipm/etc/ipmDbPref.conf* in Solaris; *c:\Program Files\Internetwork Performance Monitor\server\etc\ipmDbPref.conf* in Windows NT and Windows 2000) using a text editor.
- Step 2** To change the number of days that daily network performance statistics are stored, modify the following line:
- ```
ipm_daily_stats_life=180
```
- Step 3** To set the business hours to be used in calculating averages, you must turn on or off the appropriate hourly interval. The day is divided into increments of one hour, starting at 0:00 a.m. (*ipm\_business\_hour\_0*) and ending at 11:59 p.m. (*ipm\_business\_hour\_23=0*). For the hours you want to include in averages, set the hour interval value to 1.

For example, to store collected statistics over a business day that runs from 8:00 a.m. to 5:00 p.m., you would use the following setting:

```
ipm_business_hour_0=0
ipm_business_hour_1=0
ipm_business_hour_2=0
ipm_business_hour_3=0
ipm_business_hour_4=0
```

```
ipm_business_hour_5=0
ipm_business_hour_6=0
ipm_business_hour_7=0
ipm_business_hour_8=1
ipm_business_hour_9=1
ipm_business_hour_10=1
ipm_business_hour_11=1
ipm_business_hour_12=1
ipm_business_hour_13=1
ipm_business_hour_14=1
ipm_business_hour_15=1
ipm_business_hour_16=1
ipm_business_hour_17=0
ipm_business_hour_18=0
ipm_business_hour_19=0
ipm_business_hour_20=0
ipm_business_hour_21=0
ipm_business_hour_22=0
ipm_business_hour_23=0
```

By default, the business day is defined as 24 hours, 0:00 a.m. to 11:59 p.m.

**Step 4** To set the business days used for calculating weekly and monthly averages, you must turn on or off the appropriate day. Each day of the week is represented by a number as follows:

- Sunday is `ipm_business_day_0`
- Monday is `ipm_business_day_1`
- Tuesday is `ipm_business_day_2`
- Wednesday is `ipm_business_day_3`
- Thursday is `ipm_business_day_4`
- Friday is `ipm_business_day_5`
- Saturday is `ipm_business_day_6`

For the days you want to set as business days, set the day to a value of 1. Days with a value of 0 are not counted as business days.

For example, to set the business days to Monday through Friday, you would use the following setting (the default setting):

```
ipm_business_day_0=0
ipm_business_day_1=1
ipm_business_day_2=1
ipm_business_day_3=1
ipm_business_day_4=1
```

## Setting IPM Database Preferences

```
ipm_business_day_5=1
ipm_business_day_6=0
```

By default, the business week is defined as 7 days, Sunday morning to Saturday evening.

**Step 5** Save your changes to the IPM database preferences file.

**Step 6** Run the database utility program to load your preferences.

In Solaris, enter:

```
cd /opt/CSCOipm/bin
./ipm dbprefs reload
```

In Windows, enter:

```
cd c:\Program Files\Internetwork Performance Monitor\Server\bin
ipm dbprefs reload
```



### Note

You might want to make a backup copy of the database preferences file (*ipmDbPref.conf*) before modifying it.

## Database Preferences File Format

The contents of the default IPM database preferences file (*ipmDbPref.conf*) are shown in the following example. This file is stored in the */opt/CSCOipm/etc* directory in Solaris and in the *c:\Program Files\Internetwork Performance Monitor\server\etc* directory in Windows.

```
##
(C) Copyright 1998 Cisco Systems, Inc.
All Rights Reserved
#
IPM Web Report Preferences
#
The default maximum number of rows returned to the browser
in any web report can be controlled with ipm_max_web_rpt_rows.
#
ipm_max_web_rpt_rows=500
#
#
```

```
IPM Database Preferences
#
This file contains the IPM Database Preferences used for
data aging, data reduction, and web reporting.
#
To change these values, update the values below and run the command:
ipmDbPref.sh -s
#
To display the values currently set in the database, run the command:
ipmDbPref.sh
#
NOTE: Changing these parameters has no effect on daily, weekly and
monthly data that has already been calculated. Only new daily, weekly
and monthly data will use these new settings.
#
The weekly and monthly data are always kept forever.

The ipm_hourly_stats_life setting determines the number of days that IPM
stores hourly statistics information. You can change this to any number
of days.
#
ipm_hourly_stats_life=32
#
#
The ipm_daily_stats_life setting determines the number of days that IPM
stores daily statistics information. You can change this to any number
of days.
#
ipm_daily_stats_life=180
#
The ipm_business_hour_x settings describe which hours of the day IPM
will use when generating daily, weekly and monthly reports. Each hour
of the day, starting with 0 (midnight) and going through 23 (11 PM)
may be included in the reports. However, you will probably want to
restrict the hours included in the reports to normal business hours.
#
The hours are defined as starting at 0 minutes past the hour, and going
through 59 minutes and 59 seconds past the hour.
#
#
Set the value of each ipm_business_hour_x parameter to either 0 or 1.
A value of 1 indicates that IPM will use this hour of the day when
generating daily, weekly and monthly reports. A value of 0 indicates
that IPM will ignore this hour of the day when generating daily, weekly
and monthly reports.
#
For example, setting 'ipm_business_hour_9=1' will cause all data collected
between 9:00AM and 9:59AM on business days to be included in reports.
```

## Setting IPM Database Preferences

```
#
ipm_business_hour_0=1
ipm_business_hour_1=1
ipm_business_hour_2=1
ipm_business_hour_3=1
ipm_business_hour_4=1
ipm_business_hour_5=1
ipm_business_hour_6=1
ipm_business_hour_7=1
ipm_business_hour_8=1
ipm_business_hour_9=1
ipm_business_hour_10=1
ipm_business_hour_11=1
ipm_business_hour_12=1
ipm_business_hour_13=1
ipm_business_hour_14=1
ipm_business_hour_15=1
ipm_business_hour_16=1
ipm_business_hour_17=1
ipm_business_hour_18=1
ipm_business_hour_19=1
ipm_business_hour_20=1
ipm_business_hour_21=1
ipm_business_hour_22=1
ipm_business_hour_23=1
#
The ipm_business_day settings describe which days of the week IPM will
use when generating weekly and monthly reports. Each day of the week
is represented by a number:
#
Sunday is 0
Monday is 1
Tuesday is 2
Wednesday is 3
Thursday is 4
Friday is 5
Saturday is 6
#
Set the value of each ipm_business_day_x parameter to either 0 or 1.
A value of 1 indicates that IPM will use this day of the week when
generating weekly and monthly reports. A value of 0 indicates that IPM
will ignore this day of the week when generating weekly and monthly reports.
#
For example, setting 'ipm_business_day_2=1' will cause all
data collected on Tuesday during business hours to be included in reports.
#
ipm_business_day_0=1
ipm_business_day_1=1
```

```
ipm_business_day_2=1
ipm_business_day_3=1
ipm_business_day_4=1
ipm_business_day_5=1
ipm_business_day_6=1
```

## Setting SNMP Timeout and Retry Environment Variables

An IPM server and source router need not be physically near each other. In fact, they can be thousands of miles apart. However, as the distance increases, so does the time it takes the source router to respond to SNMP requests. If the response time exceeds a predefined timeout value, IPM interprets the delay as an SNMP timeout, which could impact the operation of your collectors.

For example, if you have an IPM server in New York and a source router in Tokyo, SNMP timeouts might prevent you from configuring collectors on the source router. Or you might be able to configure the collectors, but timeouts might result in periods when no statistical data can be collected from the source router.

If you experience this problem, the best solution is to define an additional IPM server that is physically nearer the source router. However, if that is not an option, you can set new values for the SNMP timeout and retry environment variables.



---

**Note**

SNMP environment variables are engineered for all but the most extreme operating conditions. Modifying these variables can adversely affect IPM's performance, resulting in unacceptably long delays in responding to user requests. Unless you are certain that you must, you should not modify these variables.

---

The following environment variables control SNMP timeouts and retries

:

| Variable                   | Description                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPM_SNMP_TIMEOUT           | Time in seconds for the IPM server to wait for a response. The valid range is 1 to 60 seconds. The default is 5 seconds.                                                   |
| IPM_SNMP_RETRIES           | Number of times the IPM server tries again to send a request that has timed out while waiting for a response. The valid range is 1 to 5 retries. The default is 3 retries. |
| IPM_SNMP_TIMEOUT_INCREMENT | Time in seconds to add to the current time-out value for subsequent retries. The valid range is 1 to 60 seconds. The default is 5 seconds.                                 |

Using the default values, IPM waits 50 seconds before determining that an SNMP request cannot be completed—5 seconds for the initial timeout, followed by 3 retries of 10, 15, and 20 seconds each.

If excessive SNMP timeouts are a problem in your network, try slightly increasing the timeout and timeout increment values until the problem is eliminated.

To set new values for these variables, use one of the following procedures:

- [Setting SNMP Environment Variables in Solaris, page 4-42](#)
- [Setting SNMP Environment Variables in Windows NT and Windows 2000, page 4-44](#)

## Setting SNMP Environment Variables in Solaris

To set SNMP environment variables in Solaris, use the following procedure:

- 
- Step 1** Make sure the IPM server is not running. You must set these environment variables while the IPM server is not running. To stop the IPM server, enter:

```
cd /opt/CSCOipm/bin
./ipm stop
```

- Step 2** On your IPM server, use a text editor to open the ipm.env file. In Solaris, the default directory for the ipm.env file is /opt/CSCOipm/etc.



---

**Note** The default directory for installing IPM is /opt. If you installed IPM in a different directory, specify that directory instead of /opt.

---

By default, the variable definitions are commented out in the file:

```
Max value is 60, default is 5, min is 1
#IPM_SNMP_TIMEOUT=5
#export IPM_SNMP_TIMEOUT

Max value is 5, default is 3, min is 1
#IPM_SNMP_RETRIES=3
#export IPM_SNMP_RETRIES

Max value is 60, default is 5, min is 1
#IPM_SNMP_TIMEOUT_INCREMENT=5
#export IPM_SNMP_TIMEOUT_INCREMENT
```

- Step 3** To change a variable definition, remove the comment markers (#) from the definition and change the settings. For example, to change the timeout value to 10 seconds, change the following lines in the file:

```
Max value is 60, default is 5, min is 1
IPM_SNMP_TIMEOUT=10
export IPM_SNMP_TIMEOUT
```

- Step 4** Save your changes and close the file.

- Step 5** Log in as the root user.

- Step 6** Restart the IPM servers by entering:

```
cd /opt/CSCOipm/bin
./ipm restart
```

When the IPM servers start up, they discover the variables and use the new timeout and retry values.

---

## Setting SNMP Environment Variables in Windows NT and Windows 2000

To set SNMP environment variables in Windows:

- Step 1** Make sure the IPM server is not running. You must set these environment variables while the IPM server is not running. To stop the IPM server, enter:

```
cd c:\Program Files\Internetwork Performance Monitor\Server\bin
ipm stop
```

- Step 2** On your IPM server, use a text editor to open the ipm.env file. In Windows, the default directory for the ipm.env file is *c:\Program Files\Internetwork Performance Monitor\server\etc*.



**Note** The default directory for installing IPM is *c:\Program Files\Internetwork Performance Monitor*. If you installed IPM in a different directory, specify that directory instead of *c:\Program Files\Internetwork Performance Monitor*.

By default, the variable definitions are commented out in the file:

```
Max value is 60, default is 5, min is 1
#set IPM_SNMP_TIMEOUT=5

Max value is 5, default is 3, min is 1
#set IPM_SNMP_RETRIES=3

Max value is 60, default is 5, min is 1
#set IPM_SNMP_TIMEOUT_INCREMENT=5
```

- Step 3** To change a variable definition, remove the comment markers (#) from the definition and change the settings. For example, to change the timeout value to 10 seconds, change the following lines in the file:

```
Max value is 60, default is 5, min is 1
set IPM_SNMP_TIMEOUT=10
```

- Step 4** Save your changes and close the file.
- Step 5** Log in as the administrator.

**Step 6** Restart the IPM servers by entering:

```
cd c:\Program Files\Internetwork Performance Monitor\server\bin
ipm restart
```

When the IPM servers start up, they discover the variables and use the new timeout and retry values.

---

## Setting New IPM Server Process Timeout Values

The default timeout value for data collection servers and configuration servers is 120 seconds. This value accommodates the longer startup times encountered when you have a large number of collectors. However, if you have configured more than 1000 collectors on a single IPM server, you might need to increase this timeout value. These timeout values control internal IPM timing; they do not affect communication with source routers.

For each 500 collectors above 1000, add 30 seconds to the default timeout value of 120 seconds for both the data collection server and configuration server. For example, for 1500 collectors change the timeout value to 150 seconds for both servers. If you do not make this change, the Process Manager might timeout while waiting for the data collection server to start up, thus preventing initialization of the configuration server.

To increase the timeout value, allowing sufficient time for the data collection server process to start, use one of the following procedures:

- [Setting Server Timeout Values in Solaris, page 4-45](#)
- [Setting Server Timeout Values in Windows NT and Windows 2000, page 4-47](#)

## Setting Server Timeout Values in Solaris

To set server timeout values in Solaris:

---

**Step 1** On your IPM server, use a text editor to open the ipm.conf file. In Solaris, the default directory for the ipm.conf file is /opt/CSCOipm/etc.



**Note** The default directory for installing IPM is */opt*. If you installed IPM in a different directory, specify that directory instead of */opt*.

The data collection server's timeout value is defined in the following line in the file:

```
DataCollectionServer R MessageLogServer,SNMPServer
/opt/CSCOipm/bin/CWB_ipmData_coll
-ORBagentPort,44342,-PMCserverName,IPMProcessMgr,-PMCname,DataCollecti
onServer,-MLCserverName,IPMMsgLogServer,-MLCname,DataCollectionServer,
-N,IPMDataCollectionServer,-R,/opt/CSCOipm 120
```

The configuration server's timeout value is defined in the following line in the file:

```
ConfigServer R MessageLogServer,SNMPServer,DataCollectionServer
/opt/CSCOipm/bin/CWB_ipmConfigServerd
-ORBagentPort,44342,-PMCserverName,IPMProcessMgr,-PMCname,ConfigServer
,-MLCserverName,IPMMsgLogServer,-MLCname,ConfigServer 120
```

**Step 2** To change the timeout definition for one or both servers, change the number 120 at the end of the appropriate line. For example, to change the timeout value for configuration servers to 240 seconds:

```
ConfigServer R MessageLogServer,SNMPServer,DataCollectionServer
/opt/CSCOipm/bin/CWB_ipmConfigServerd
-ORBagentPort,44342,-PMCserverName,IPMProcessMgr,-PMCname,ConfigServer
,-MLCserverName,IPMMsgLogServer,-MLCname,ConfigServer 240
```

**Step 3** Save your changes and close the file.

**Step 4** Log in as the root user.

**Step 5** Restart the IPM servers by entering:

```
cd /opt/CSCOipm/bin
./ipm restart
```

When the IPM servers start up, they use the new timeout values.

## Setting Server Timeout Values in Windows NT and Windows 2000

To set server timeout values in Windows NT and Windows 2000:

- Step 1** On your IPM server, use a text editor to open the ipm.conf file. In Windows, the default directory for the ipm.conf file is c:\Program Files\Internetwork Performance Monitor\server\pmconf.



**Note** The default directory for installing IPM is *c:\Program Files\Internetwork Performance Monitor*. If you installed IPM in a different directory, specify that directory instead of *c:\Program Files\Internetwork Performance Monitor*.

The data collection server's timeout value is defined in the following line in the file:

```
DataCollectionServer R MessageLogServer,SNMPServer
C:\PROGRA~1\INTERN~1\Server\bin\CWB_ipmData_coll.d
-ORBagentPort,44342,-OAconnectionMaxIdle,8640000,-PMCserverName,IPMPro
cessMgr,-PMCname,DataCollectionServer,-MLCserverName,IPMMsgLogServer,-
MLCname,DataCollectionServer,-N,IPMDataCollectionServer,-R,C:\PROGRA~1
\INTERN~1\Server,-MLCfilterFileName,C:\PROGRA~1\INTERN~1\Server\logs\D
ataCollectionServer.flt 120
```

The configuration server's timeout value is defined in the following line in the file:

```
ConfigServer R MessageLogServer,SNMPServer,DataCollectionServer
C:\PROGRA~1\INTERN~1\Server\bin\CWB_ipmConfigServer.d
-ORBagentPort,44342,-OAconnectionMaxIdle,8640000,-PMCserverName,IPMPro
cessMgr,-PMCname,ConfigServer,-MLCserverName,IPMMsgLogServer,-MLCname,
ConfigServer,-MLCfilterFileName,C:\PROGRA~1\INTERN~1\Server\logs\Confi
gServer.flt 120
```

- Step 2** To change the timeout definition for one or both servers, change the number 120 at the end of the appropriate line. For example, to change the timeout value for configuration servers to 240 seconds:

```
ConfigServer R MessageLogServer,SNMPServer,DataCollectionServer
C:\PROGRA~1\INTERN~1\Server\bin\CWB_ipmConfigServer.d
-ORBagentPort,44342,-OAconnectionMaxIdle,8640000,-PMCserverName,IPMPro
```

```
cessMgr, -PMCname, ConfigServer, -MLCserverName, IPMMsgLogServer, -MLCname,
ConfigServer, -MLCfilterFileName, C:\PROGRA~1\INTERN~1\Server\logs\Confi
gServer.flt 240
```

**Step 3** Save your changes and close the file.

**Step 4** Log in as the administrator.

**Step 5** Restart the IPM servers by entering:

```
cd c:\Program Files\Internetwork Performance Monitor\server\bin
ipm restart
```

When the IPM servers start up, they use the new timeout value.

---

## Setting the DISPLAY Variable in Solaris

The DISPLAY variable is set as part of your login environment on Solaris. However, if you Telnet into a remote workstation, you must set the DISPLAY variable to local display. To do so, enter:

```
setenv DISPLAY local_ws:0.0
```

where *local\_ws* is your local workstation.

If your shell does not support the **setenv** command, use:

```
export DISPLAY=local_ws:0.0
```

If you Telnet into a remote workstation and you do *not* set the DISPLAY variable to local display, you cannot use:

- **ipm**
- **ipm control -rt**
- **ipm debug**
- **ipm pmstatus**
- **ipm start client**

# Backing Up or Restoring the IPM Database

The IPM database is backed up automatically every day at 1:00 a.m. If your database file is corrupted, you can restore the data in the IPM database from the previous day's backed-up data.

To restore the IPM database from a previous back up:

- In Solaris, enter:

```
cd /opt/CSCOipm/bin
./ipm dbrestore
```

- In Windows NT and Windows 2000, enter:

```
cd c:\Program Files\Internetwork Performance Monitor\server\bin
ipm dbrestore
```

**Note**

---

This command can take several hours to complete.

---

**Warning**

---

**Do not interrupt this command. Doing so can corrupt your IPM database.**

---

## Changing IPM Database Password

You can change the IPM database password using the command:

```
ipm dbpassword
```

IPM prompts you to enter the old password. After you enter the old password, you need to enter the new password and confirm it by entering it again.

The password is case sensitive and should be at least four characters long. You cannot use spaces in the password.

When you try to restore an old database after you change the database password and if the password in the old database is different from the new one, then the password in the old database will be modified to the new password and IPM restores the database.

