Accessing SGM Data from a Web Browser

This chapter provides information about accessing SGM data from the SGM server home page, using a Web browser.

This chapter includes the following sections:

Accessing SGM Data from the SGM Server Home Page

From the SGM Server Home Page, you can access many Web pages containing SGM data, including server status, network status, installation logs, message logs, product documentation, Cisco.com, and other information about SGM. You can also download the SGM clients.

To access the SGM Server Home page, use one of the following procedures:

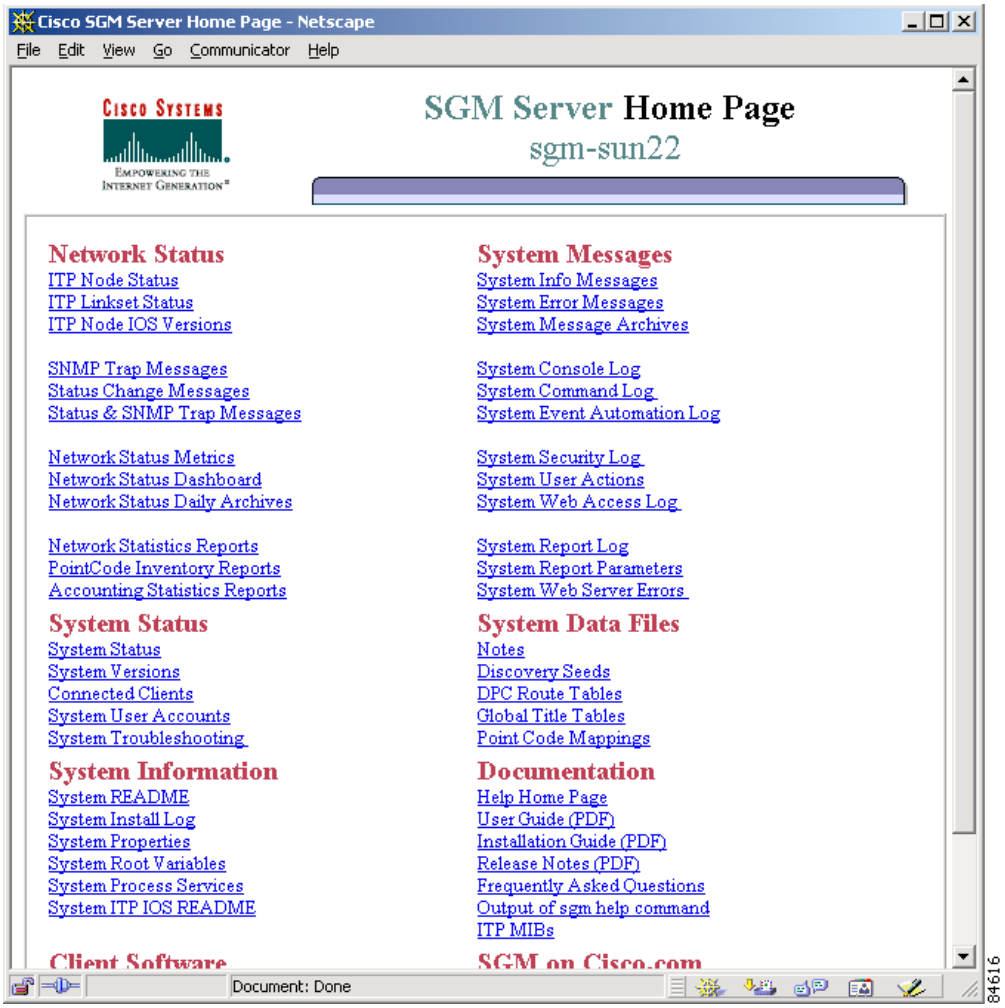
- Select **Web Links>Server Home Page** from the SGM Main Menu.
- Enter the following URL in a Web browser:

  http://*server_name***:***1774*

  Where *server_name* is the name or IP address of the server on which the SGM server is running and *1774* is the Web port being using by SGM. (**1774** is the default port number.) If you do not know the name or Web port of the SGM Web Server, contact the system administrator who installed the SGM server software.
- Select **Home** from the menu bar of any of the SGM Web pages.

The SGM Server Home Page (Figure 7-1) is displayed.

Figure 7-1 SGM Server Home Page



The rest of this chapter provides detailed information about the SGM information you can access from the SGM Server Home Page.

Modifying SGM Web Output (Solaris Only)

SGM enables you to modify the following aspects of its Web output:

- To control how often, in seconds, SGM updates certain Web output, use the **sgm weblogupdate** command. The valid range is 1 second to an unlimited number of seconds. The default value is 300 seconds (5 minutes).
- To set the maximum number of rows for SGM ASCII Web output, such as displays of detailed debugging information, use the **sgm maxasciirows** command. The valid range is 1 row to an unlimited number of rows. The default value is 6000 rows.
- To set the maximum number of rows for SGM HTML Web output, such as displays of statistics reports, status change messages, or SNMP trap messages, use the **sgm maxhtmlrows** command. The valid range is 1 row to an unlimited number of rows. The default value is 500 rows.
- To specify whether SGM is to show real node names or display names in Web pages, enter the **sgm webnames** command:
  - To show the real DNS names of nodes, as discovered by SGM, enter **sgm webnames real**. This is the default setting.
  - To show display names, enter **sgm webnames display**. Display names are new names that you specify for nodes. For more information about display names, see the "Editing a Node" section on page 3-99.
- To specify whether SGM is to display send and receive utilization for linksets and links as percentages or in Erlangs in Web pages, enter the **sgm webutil** command:
  - To display utilization as a percentage, enter **sgm webutil percent**. This is the default setting.
  - To show display utilization in Erlangs, enter **sgm webutil erlangs**.

  See the "Working with SGM Statistics Reports" section on page 3-218 for more information on send and receive utilization for linksets and links.

Each of these commands requires you to be logged in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 3-2, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 4-22.

Viewing Network Status and Statistics Information for SGM

You can view the following SGM network status and statistics information from the SGM Server Home Page:

Viewing Information About Nodes

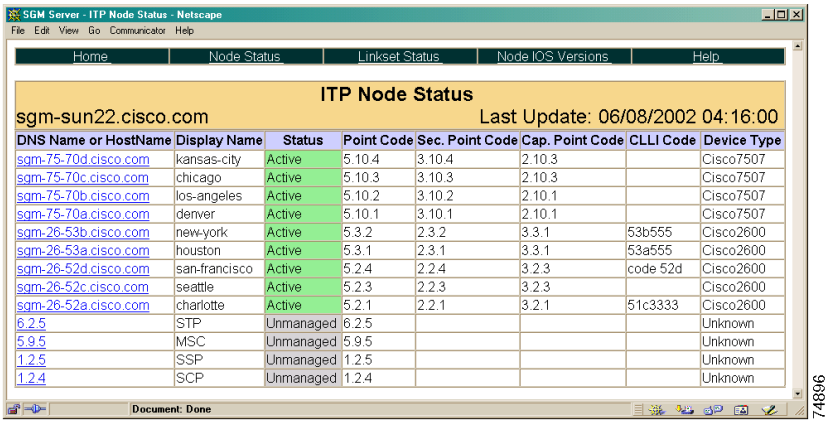
SGM enables you to view the following information about nodes:

Viewing ITP Node Status

The SGM - ITP Node Status page displays information about all discovered nodes, including their names, events, status, and other important information.

To access the SGM - ITP Node Status page, select **ITP Node Status** from the SGM Server Home Page. SGM displays the SGM - ITP Node Status page (Figure 7-2).

Figure 7-2 SGM - ITP Node Status Page



DNS Name or HostName	Display Name	Status	Point Code	Sec. Point Code	Cap. Point Code	CLLI Code	Device Type
sgm-75-70d.cisco.com	kansas-city	Active	5.10.4	3.10.4	2.10.3		Cisco7507
sgm-75-70c.cisco.com	chicago	Active	5.10.3	3.10.3	2.10.3		Cisco7507
sgm-75-70b.cisco.com	los-angeles	Active	5.10.2	3.10.2	2.10.1		Cisco7507
sgm-75-70a.cisco.com	denver	Active	5.10.1	3.10.1	2.10.1		Cisco7507
sgm-26-53b.cisco.com	new-york	Active	5.3.2	2.3.2	3.3.1	53b555	Cisco2600
sgm-26-53a.cisco.com	houston	Active	5.3.1	2.3.1	3.3.1	53a555	Cisco2600
sgm-26-52d.cisco.com	san-francisco	Active	5.2.4	2.2.4	3.2.3	code 52d	Cisco2600
sgm-26-52c.cisco.com	seattle	Active	5.2.3	2.2.3	3.2.3		Cisco2600
sgm-26-52a.cisco.com	charlotte	Active	5.2.1	2.2.1	3.2.1	51c3333	Cisco2600
6.2.5	STP	Unmanaged	6.2.5				Unknown
5.9.5	MSC	Unmanaged	5.9.5				Unknown
1.2.5	SSP	Unmanaged	1.2.5				Unknown
1.2.4	SCP	Unmanaged	1.2.4				Unknown

You can sort the SGM - ITP Node Status table based on the information in one of the columns. See the "Resizing, Sorting, and Hiding Table Columns" section on page 3-178 for more details.

The SGM - ITP Node Status page displays the following information for each node:

- **Server Name (in header)**—Name of the SGM server associated with the node.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **IP Address or DNS Hostname**—DNS name of the node, as discovered by SGM. To see detailed information for the node, click the node name.
- **Display Name**—New name that you specified for the node. If the node has no display name, this field is blank. For more information, see the "Editing a Node" section on page 3-99.

- **Status**—Current status of the node, with a color-coded background. Possible values are:
  - **Active (green)**—The node is currently fully functional.
  - **Discovering (gray)**—The node is being discovered, and SNMP queries have been sent to the device.
  - **Polling (gray)**—The node is being polled.
  - **Unknown (red)**—The node failed to respond to an SNMP request. The node and all associated linksets and links are set to **Unknown**.
  - **Unmanaged (gray)**—One of the following situations exists:
    - The node is known indirectly by SGM. In other words, SGM knows the device exists but there is no known SNMP stack on the device for SGM to query.
    - An SGM user has set the node to **Unmanaged** status, to prevent SGM from polling the node.
  - **Waiting (gray)**—The node is in the Discovery queue but is not currently being discovered.
  - **Warning (yellow)**—The node is active, but one or more associated links or linksets is in **Failed**, **Unavailable**, **Unknown**, or **Warning** status and is not flagged as **Ignored**.
- **Point Code**—Primary point code of the node.
- **Sec. Point Code**—Secondary point code of the node. If the node has no secondary point code, this field is blank.
- **Cap. Point Code**—Capability point code of the node. A capability point code, also called an alias point code, is one that is shared by more than one node, each of which is also assigned a “real” point code. If the node has no capability point code, this field is blank.

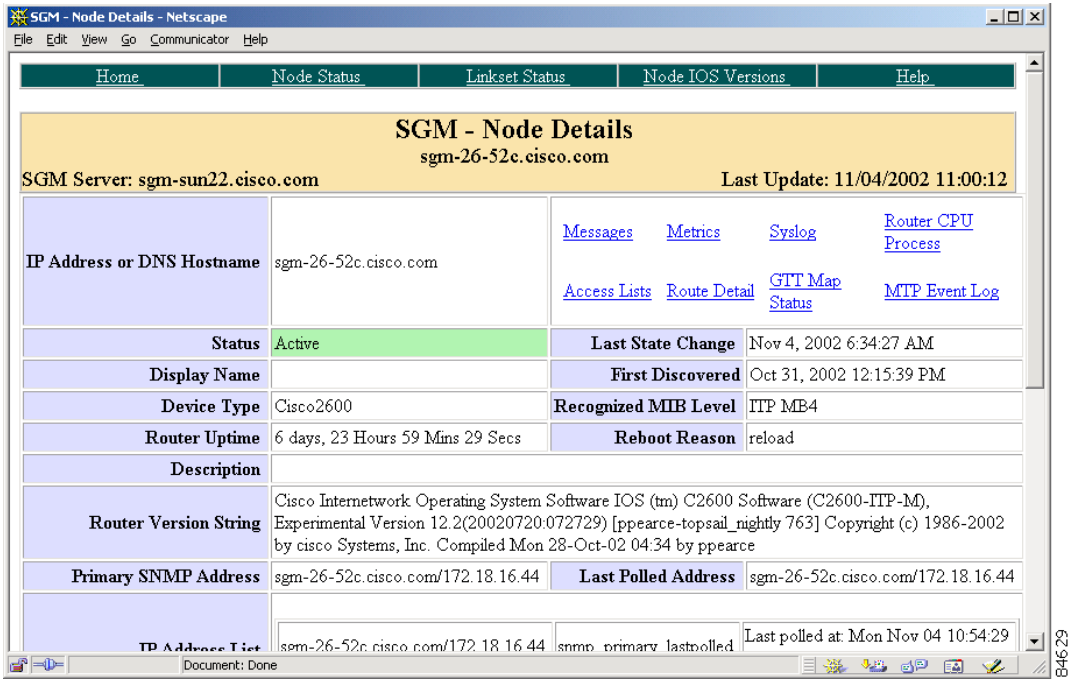
- **CLLI Code**—COMMON LANGUAGE Location Code for the node. A CLLI code is a standardized 11-character identifier that uniquely identifies the geographic location of the node. If the node has no CLLI code configured, this field is blank.
- **Device Type**—Device type of the node. Possible values are:
  - **Cisco2600**—Cisco 2651 series router
  - **Cisco7202**—Cisco 7202 series router
  - **Cisco7204**—Cisco 7204VXR series router
  - **Cisco7206**—Cisco 7206VXR series router
  - **Cisco7507**—Cisco 7507 series router
  - **Cisco7513**—Cisco 7513 series router
  - **IPDevice**—IP device, other than Cisco 2651, 7202, 7204VXR, 7206VXR, 7507, or 7513 series router. You can assign this icon to an unknown node if you know that it is an IP device.
  - **Unknown**—SGM is unable to determine the device type.

Viewing ITP Node Details

The SGM - Node Details page displays detailed information about each discovered node, including its CLLI code, point code, status, and other information.

To access the SGM - Node Details page, click a node name in the SGM - ITP Node Status, SGM - ITP Linkset Status, or SGM - ITP Node IOS Versions page. SGM displays the SGM - Node Details page (Figure 7-3).

Figure 7-3 SGM - Node Details Page



The SGM - Node Details page displays the following information for the selected node:

- **Node Name (in header)**—DNS name of the node, as discovered by SGM.
- **Server Name (in header)**—Name of the SGM server associated with the node.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.

- **IP Address or DNS Hostname**—DNS name of the node, as discovered by SGM.

  To see status change messages and SNMP trap messages associated with the node, click **Messages**.

  To see network status metrics associated with the node, click **Metrics**.

  ITP nodes also provide the following options:

  - To see all messages in the SGM system log for the node, click **Syslog**.
  - To see detailed information about all CPU processes associated with the node, click **Router CPU Process**.
  - To see all access lists associated with the node, click **Access Lists**.
  - To see detailed information about routes associated with the node, click **Route Detail**.
  - To see detailed information about all GTT MAPs associated with the node, click **GTT MAP Status**.
  - To see detailed information about all MTP3 events associated with the node, click **MTP Event Log**.

- **Status**—Current status of the node, with a color-coded background. Possible values are:
  - **Active (green)**—The node is currently fully functional.
  - **Discovering (gray)**—The node is being discovered, and SNMP queries have been sent to the device.
  - **Polling (gray)**—The node is being polled.
  - **Unknown (red)**—The node failed to respond to an SNMP request. The node and all associated linksets and links are set to **Unknown**.
  - **Unmanaged (gray)**—One of the following situations exists:
    - The node is known indirectly by SGM. In other words, SGM knows the device exists but there is no known SNMP stack on the device for SGM to query.
    - An SGM user has set the node to **Unmanaged** status, to prevent SGM from polling the node.

  - **Waiting (gray)**—The node is in the Discovery queue but is not currently being discovered.
  - **Warning (yellow)**—The node is active, but one or more associated links or linksets is in **Failed**, **Unavailable**, **Unknown**, or **Warning** status and is not flagged as **Ignored**.
- **Last State Change**—Date and time that the status of the link last changed.
- **Display Name**—New name that you specified for the node. If the node has no display name, this field is blank. For more information, see the "Editing a Node" section on page 3-99.
- **First Discovered**—Date and time that the node was first discovered by SGM.
- **Device Type**—Device type of the node. Possible values are:
  - **Cisco2600**—Cisco 2651 series router
  - **Cisco7202**—Cisco 7202 series router
  - **Cisco7204**—Cisco 7204VXR series router
  - **Cisco7206**—Cisco 7206VXR series router
  - **Cisco7507**—Cisco 7507 series router
  - **Cisco7513**—Cisco 7513 series router
  - **IPDevice**—IP device, other than Cisco 2651, 7202, 7204VXR, 7206VXR, 7507, or 7513 series router. You can assign this icon to an unknown node if you know that it is an IP device.
  - **Unknown**—SGM is unable to determine the device type.
- **Recognized MIB Level**—MIB conformance level used by the router, such as **ITP MB5**.

Note **Router Version String** and **Recognized MIB Level** might not have a one-to-one correspondence, because multiple router versions can use the same MIB level if there are no changes to the MIBs between versions. For example, router versions **12.2(4)MB5** and **12.2(4)MB6** both use MIB level **ITP MB5**.

- **Router Uptime**—Time the node has been up, in weeks, days, hours, and minutes.
- **Reboot Reason**—Reason for the last reboot of the node.

- **Description**—Description of the node. If the node has no description, this field is blank.
- **Router Version String**—Version of IOS that is installed on the router.
- **Primary SNMP Address**—IP address of the node, used by SNMP to poll the node.
- **Last Polled Address**—Last IP address that was polled for this node.
- **IP Address List**—Drop-down list of all IP addresses associated with this node, including the primary SNMP address and all backup IP addresses.
- **Point Code**—Primary point code of the node.
- **Secondary Point Code**—Secondary point code of the node. If the node has no secondary point code, this field is blank.
- **Capability Point Code**—Capability point code of the node. A capability, or alias, point code is one that is shared by more than one node, each of which is also assigned a "real" point code. If the node has no capability point code, this field is blank.
- **CLLI Code**—COMMON LANGUAGE Location Code for the node. A CLLI code is a standardized 11-character identifier that uniquely identifies the geographic location of the node. If the node has no CLLI code configured, this field is blank.
- **Avg. SGM Poll Response (secs)**—Average time, in seconds, taken by this node to respond to SGM poll requests. For a non-ITP node, this field is left blank.
- **Last SGM Poll Response (secs)**—Time, in seconds, taken by this node to respond to the last SGM poll request. For a non-ITP node, this field is left blank.
- **Last Full Router Poll**—Date and time of the last full poll of the node for ITP-related MIBs (as opposed to a demand poll for just one linkset's worth of data). For a non-ITP node, this field is left blank.
- **Poll Error Time**—Date and time the last error message received by the node. For a non-ITP node, this field is left blank.
- **Poll Error Message**—Last error message received by the node. For a non-ITP node, this field is left blank.
- **Note Timestamp**—Date and time the note associated with this node was last updated. If there is no note associated with this node, this field is blank.

- **Note**—Note associated with this node. If there is no note associated with this node, this field is blank.
- **Internal ID**—Internal ID of the node. The internal ID is a unique ID for every event, link, linkset, and node, assigned by SGM for its own internal use. It can also be useful when the Cisco TAC is debugging problems.
- **QoS**—Quality of service (QoS) class of the node, mapped to the type of service (ToS) or IP differentiated-services-code-point (DSCP).
- **Linksets**—Name and status of all linksets associated with this node. To see detailed information for the linkset, click the linkset name.

Viewing ITP Node IOS Versions

The SGM - ITP Node IOS Versions page displays the version of IOS installed on each ITP node.

To access the SGM - ITP Node IOS Versions page, select **ITP Node IOS Versions** from the SGM Server Home Page.

You can sort the SGM - ITP Node IOS Versions table based on the information in one of the columns. See the "Resizing, Sorting, and Hiding Table Columns" section on page 3-178 for more details.

The SGM - ITP Node IOS Versions page displays the following information for each ITP node:

- **Server Name (in header)**—Name of the SGM server associated with the node.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **IP Address or DNS Hostname**—DNS name of the node, as discovered by SGM.
- **Display Name**—New name that you specified for the node. If the node has no display name, this field is blank. For more information, see the "Editing a Node" section on page 3-99.
- **IOS Version**—Version of IOS installed on the node.

- **Recognized MIB Level**—MIB conformance level used by the router, such as **ITP MB5**.

Note **IOS Version** and **Recognized MIB Level** might not have a one-to-one correspondence, because multiple router versions can use the same MIB level if there are no changes to the MIBs between versions. For example, router versions **12.2(4)MB5** and **12.2(4)MB6** both use MIB level **ITP MB5**.

- **Device Type**—Device type of the node. Possible values are:
  - **Cisco2600**—Cisco 2651 series router
  - **Cisco7202**—Cisco 7202 series router
  - **Cisco7204**—Cisco 7204VXR series router
  - **Cisco7206**—Cisco 7206VXR series router
  - **Cisco7507**—Cisco 7507 series router
  - **Cisco7513**—Cisco 7513 series router
  - **IPDevice**—IP device, other than Cisco 2651, 7202, 7204VXR, 7206VXR, 7507, or 7513 series router. You can assign this icon to an unknown node if you know that it is an IP device.
  - **Unknown**—SGM is unable to determine the device type.

Viewing ITP Node Information - Access Lists

The SGM - ITP Access Lists page displays all access lists associated with the selected node.

To access the SGM - ITP Access Lists page, select a node in the Node or Topology window, then select **Drill Down>Show Access List** from the right-click menu. (This option is not available for a node if the node is in **Unknown** or **Unmanaged** status.)

The SGM - ITP Access Lists page displays the following information for the selected node:

- **Node Name (in header)**—Name of the node for which access lists are being displayed.
- **Server Name (in header)**—Name of the SGM server associated with the node.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Node/Linkset**—Name of the node and linkset for which access lists are being displayed. To see detailed information for the node or linkset, click the node or linkset name.
- **List #**—Access list number configured on the node and applied to the linkset. ITP uses access list numbers 2700 through 2799.
- **Access List**—List of commands in the access list.

Viewing ITP Node Information - CPU Processes

The SGM - CPU Processes page displays detailed information about all CPU processes associated with the selected node.

To access the SGM - CPU Processes page, select a node in the Node or Topology window, then select **Drill Down > Show Router CPU Processes** from the right-click menu. (This option is not available if the node is in **Unknown** or **Unmanaged** status.)

The SGM - CPU Processes page displays the following information for the selected node:

- **Node Name (in header)**—Name of the node for which CPU processes are being displayed.
- **Server Name (in header)**—Name of the SGM server associated with the node.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Node**—Name of the node for which CPU processes are being displayed. To see detailed information for the node, click the node name.
- **CPU**—Number of the CPU for which processes are being displayed.

- **PID**—Process identifier.
- **Name**—Name of the process.
- **Run Time (ms)**—CPU time, in milliseconds, the process has used.
- **Invoked**—Number of times the process has been invoked.
- **Usecs**—Microseconds of CPU time for each process invocation.
- **5 Sec**—Average CPU utilization percentage for the node over the last 5 seconds.
- **1 Min**—Average CPU utilization percentage for the node over the last minute.
- **5 Min**—Average CPU utilization percentage for the node over the last 5 minutes.
- **Mem Alloc**—Bytes of memory allocated by the process.
- **Mem Freed**—Bytes of memory freed by the process, regardless of who originally allocated it.
- **Priority**—Process queue priority. Possible values are:
  - **Low**
  - **Normal**
  - **High**
  - **Critical**

Viewing ITP Node Information - GTT MAP Status

The SGM - GTT MAP Status page displays detailed information about all GTT MAPs associated with the selected node.

To access the SGM - GTT MAP Status page, select a node in the Node or Topology window, then select **Drill Down>Show GTT MAP Status** from the right-click menu. (This option is not available if the node is in **Unknown** or **Unmanaged** status.)

The SGM - GTT MAP Status page displays the following information for the selected node:

- **Node Name (in header)**—Name of the node for which GTT MAPs are being displayed.
- **Server Name (in header)**—Name of the SGM server associated with the node.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Node**—Name of the node for which GTT MAPs are being displayed. To see detailed information for the node, click the node name.
- **Point Code**—Primary point code for the GTT MAP.
- **SSN**—Primary subsystem number (SSN) for the GTT MAP.
- **Point Code Status**—Status of the primary point code. Possible values are:
  - **Allowed**
  - **Prohibited**—Either the point code cannot be reached, or the point code is labeled **Prohibited** by the SCCP protocol.
- **SSN Status**—Status of the primary SSN. Possible values are:
  - **Allowed**
  - **Prohibited**—Either the remote subsystem cannot be reached, or the subsystem is labeled **Prohibited** by the SCCP protocol.
- **Congestion State**—MTP3 congestion level for the primary point code. Possible values are:
  - **No congestion**—Corresponds to **None**. The link is not congested.
  - **Congestion level 1**—Corresponds to **Low**. The link is slightly congested.
  - **Congestion level 2**—Corresponds to **High**. The link is congested.
  - **Congestion level 3**—Corresponds to **Very High**. The link is very congested.

Viewing ITP Node Information - Linkset Status

The SGM - ITP Linkset Statuses for Node page displays status information for all linksets associated with the selected node.

To access the SGM - ITP Linkset Statuses for Node page, select a node in the Node or Topology window, then select **Drill Down > Show All Linkset Statuses** from the right-click menu. (This option is not available if the node is in **Unknown** or **Unmanaged** status.)

The SGM - ITP Linkset Statuses for Node page displays the following information for the selected node:

- **Node Name (in header)**—Name of the node for which linkset statuses are being displayed.
- **Server Name (in header)**—Name of the SGM server associated with the node.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Linkset**—Linkset associated with the node. To see detailed information for the linkset, click the linkset name.
- **Status**—Current status of the linkset, with a color-coded background. Possible values are:
  - **Active (green)**—The linkset is currently fully functional.
  - **Unavailable (red)**—An error is preventing traffic from flowing on this linkset.
  - **Shutdown (blue)**—A router administrator has set the linkset to prevent traffic from flowing. When a linkset is set to **Shutdown**, all its associated links are set to **Failed** by Cisco IOS.
  - **Unknown (red)**—Either the node associated with this linkset has failed to respond to an SNMP request, or SGM found that the linkset no longer exists.
  - **Warning (yellow)**—The linkset is active, but one or more links in the linkset is congested or is in **Failed**, **Unknown**, or **Warning** status, and is not flagged as **Ignored**. At least one link is available and can carry traffic.

  There is no **Unshut** or **No Shut** status.

Viewing ITP Node Information - MTP3 Event Log Messages

The SGM - MTP3 Event Log page displays the most recent MTP3 events associated with the selected node or event.

To access the SGM - MTP3 Event Log page, select a node in the Node or Topology window, or an event in the Event Window, then select **Drill Down>Show MTP3 Event Log Messages** from the right-click menu. SGM displays the SGM - MTP3 Event Log page.

You can sort the SGM - MTP3 Event Log table based on the information in one of the columns. See the "Resizing, Sorting, and Hiding Table Columns" section on page 3-178 for more details.

The SGM - MTP3 Event Log table displays the following information for the selected node:

- **Server Name (in header)**—Name of the SGM server associated with the node or event.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Node**—Name or IP address of the node. To see detailed information for the node, click the node name.
- **Index**—Event number, assigned to the event by SGM.
- **Event**—Message text for the event.

Viewing ITP Node Information - Route Detail

The SGM - Route Detail page displays detailed information about routes associated with the selected node.

To access the SGM - Route Detail page and display information about routes for all destination point codes for a node, select a node in the Node or Topology window, then select **Drill Down>Show Route Detail** from the right-click menu. (This option is not available if the node is in **Unknown** or **Unmanaged** status.)

To access the SGM - Route Detail page and display information about routes for a single destination point code for a node, select a node in the Node or Topology window, then select **Drill Down>Show Route to Point Code** from the right-click menu, then enter a specific point code when prompted. (This option is not available if the node is in **Unknown** or **Unmanaged** status.)

The SGM - Route Detail page displays the following information for the selected node:

- **Node Name (in header)**—Name of the node for which route detail is being displayed.
- **Server Name (in header)**—Name of the SGM server associated with the node.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Node**—Name of the node for which route detail is being displayed. To see detailed information for the node, click the node name.
- **Destination**—Destination point code and mask length for packets on the selected node.

  The destination point code is the point code to which a given packet is routed.

  The mask length is the number of significant leading bits in the point code. The mask length is always 14 for ITU and 24 for ANSI.
- **Access**—Status of the destination. Possible values are:
  - **Accessible**
  - **Inaccessible**
  - **Restricted**
- **Cost**—Cost of the route to the destination, relative to other routes. The valid costs range from **1** (lowest cost and highest priority) through **9** (highest cost and lowest priority).
- **QoS**—Quality of service (QoS) class of the route, as configured by the network administrator. Valid QoS classes range from **1** through **7**; **ALL** indicates that the route accepts all QoS classes.
- **Linkset**—Destination linkset associated with the destination point code. The destination linkset is also known as the output linkset. To see detailed information for the linkset, click the linkset name.

- **Status**—Current status of the linkset, with a color-coded background. Possible values are:
  - **Active (green)**—The linkset is currently fully functional.
  - **Unavailable (red)**—An error is preventing traffic from flowing on this linkset.
  - **Shutdown (blue)**—A router administrator has set the linkset to prevent traffic from flowing. When a linkset is set to **Shutdown**, all its associated links are set to **Failed** by Cisco IOS.
  - **Unknown (red)**—Either the node associated with this linkset has failed to respond to an SNMP request, or SGM found that the linkset no longer exists.
  - **Warning (yellow)**—The linkset is active, but one or more links in the linkset is congested or is in **Failed**, **Unknown**, or **Warning** status, and is not flagged as **Ignored**. At least one link is available and can carry traffic.

  There is no **Unshut** or **No Shut** status.
- **Non-Adj. State**—Accessibility of the destination from the adjacent point code at the remote end of the linkset. Possible values are:
  - **Allowed**—Traffic is allowed on the route without restriction.
  - **Prohibited**—Traffic is prohibited on the route.
  - **Restricted**—Traffic is restricted on the route.
  - **Unknown**—Accessibility cannot be determined.
- **Route State**—Status of the route, derived from **Status** and **Non-Adj. State**:
  - If **Status** is **Shutdown**, **Unavailable**, **Unknown**, or **Warning**, then **Route State** is also **Unavailable**.
  - If **Status** is **Active** and **Non-Adj. State** is **Allowed** or **Unknown**, then **Route State** is **Available**.
  - If **Status** is **Active** and **Non-Adj. State** is **Restricted**, then **Route State** is also **Restricted**.
  - If **Status** is **Active** and **Non-Adj. State** is **Prohibited**, then **Route State** is **Unavailable**.

Viewing ITP Node Information - Syslog Messages

The SGM - Router Syslog page displays all messages in the SGM system log for the selected node.

To access the SGM - Router Syslog page, use one of the following procedures:

- Select a node in the Node or Topology window, then select **Drill Down>Show Syslog Messages** from the right-click menu. SGM displays the SGM - Router Syslog page, populated with the most recent syslog messages for the selected node.
- Select **Syslog** in the SGM - Node Details page. SGM displays the SGM - Router Syslog page, populated with the most recent syslog messages for the selected node.
- Select an event in the Event Window, then select **Drill Down>Show Syslog Messages** from the right-click menu. SGM displays the SGM - Router Syslog page, populated with the most recent syslog messages for the node associated with the selected event.

None of the above options is available if the node is in **Unknown** or **Unmanaged** status.

The SGM - Router Syslog page displays the following information for the selected node:

- **Node Name (in header)**—Name of the node for which syslog messages are being displayed.
- **Server Name (in header)**—Name of the SGM server associated with the node.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Node**—Name of the node for which syslog messages are being displayed. To see detailed information for the node, click the node name.
- **Timestamp**—Date and time of the syslog message

- **Severity**—Severity of the syslog message. Possible values are:
  - **Alert**—Messages that require immediate action.
  - **Critical**—Critical conditions.
  - **Debug**—Debug messages, log FTP commands, and WWW URLs.
  - **Emergency**—System unusable messages.
  - **Error**—Error messages.
  - **Info**—Information messages.
  - **Notice**—Normal but significant conditions.
  - **Warning**—Warning messages.
- **Facility**—Name of the facility that generated the syslog message, such as SYS, SNMP, CS7MTP3, or CS7PING.
- **Name**—Short text identifier for the message type. A facility name in conjunction with a message name uniquely identifies a syslog message type.
- **Message**—Text of the syslog message.

Viewing the Network Status Node Dashboard

The SGM - Node Dashboard page lists all discovered nodes, and provides links to messages and metrics for each node.

To access the SGM - Node Dashboard page, select **Network Status Dashboard** from the SGM Server Home Page, then click **Node Dashboard**.

To see status change messages and SNMP trap messages associated with a given node, click **Messages**.

To see network status metrics associated with a given node, click **Metrics**.

ITP nodes also provide the following options:

- To see detailed information about all CPU processes associated with a given node, click **Router CPU Process**.
- To see all messages in the SGM system log associated with a given node, click **Syslog**.
- To see all access lists associated with a given node, click **Access Lists**.
- To see detailed information about routes associated with a given node, click **Route Detail**.

- To see detailed information about all GTT MAPs associated with a given node, click **GTT MAP Status**.
- To see detailed information about all MTP events associated with a given node, click **MTP Event Log**.

You can sort the table based on the information in the **Nodes** column. See the "Resizing, Sorting, and Hiding Table Columns" section on page 3-178 for more details.

Viewing Information About Linksets

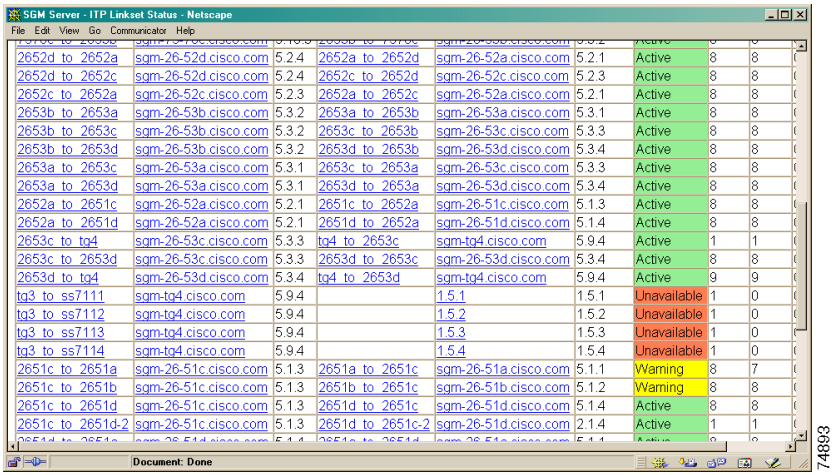
SGM enables you to view the following information about linksets:

Viewing ITP Linkset Status

The SGM - ITP Linkset Status page displays information about the linksets that have been discovered by SGM.

To access the SGM - ITP Linkset Status page, select **ITP Linkset Status** from the SGM Server Home Page. SGM displays the SGM - ITP Linkset Status page (Figure 7-4).

Figure 7-4 SGM - ITP Linkset Status Page



2652d_to_2652a	sgm-26-52d.cisco.com	5.2.4	2652a_to_2652d	sgm-26-52a.cisco.com	5.2.1	Active	8	8
2652d_to_2652c	sgm-26-52d.cisco.com	5.2.4	2652c_to_2652d	sgm-26-52c.cisco.com	5.2.3	Active	8	8
2652c_to_2652a	sgm-26-52c.cisco.com	5.2.3	2652a_to_2652c	sgm-26-52a.cisco.com	5.2.1	Active	8	8
2653b_to_2653a	sgm-26-53b.cisco.com	5.3.2	2653a_to_2653b	sgm-26-53a.cisco.com	5.3.1	Active	8	8
2653b_to_2653c	sgm-26-53b.cisco.com	5.3.2	2653c_to_2653b	sgm-26-53c.cisco.com	5.3.3	Active	8	8
2653b_to_2653d	sgm-26-53b.cisco.com	5.3.2	2653d_to_2653b	sgm-26-53d.cisco.com	5.3.4	Active	8	8
2653a_to_2653c	sgm-26-53a.cisco.com	5.3.1	2653c_to_2653a	sgm-26-53c.cisco.com	5.3.3	Active	8	8
2653a_to_2653d	sgm-26-53a.cisco.com	5.3.1	2653d_to_2653a	sgm-26-53d.cisco.com	5.3.4	Active	8	8
2652a_to_2651c	sgm-26-52a.cisco.com	5.2.1	2651c_to_2652a	sgm-26-51c.cisco.com	5.1.3	Active	8	8
2652a_to_2651d	sgm-26-52a.cisco.com	5.2.1	2651d_to_2652a	sgm-26-51d.cisco.com	5.1.4	Active	8	8
2653c_to_tg4	sgm-26-53c.cisco.com	5.3.3	tg4_to_2653c	sgm-tg4.cisco.com	5.9.4	Active	1	1
2653c_to_2653d	sgm-26-53c.cisco.com	5.3.3	2653d_to_2653c	sgm-26-53d.cisco.com	5.3.4	Active	8	8
2653d_to_tg4	sgm-26-53d.cisco.com	5.3.4	tg4_to_2653d	sgm-tg4.cisco.com	5.9.4	Active	9	9
tg3_to_ss7111	sgm-tg4.cisco.com	5.9.4		1.5.1	1.5.1	Unavailable	1	0
tg3_to_ss7112	sgm-tg4.cisco.com	5.9.4		1.5.2	1.5.2	Unavailable	1	0
tg3_to_ss7113	sgm-tg4.cisco.com	5.9.4		1.5.3	1.5.3	Unavailable	1	0
tg3_to_ss7114	sgm-tg4.cisco.com	5.9.4		1.5.4	1.5.4	Unavailable	1	0
2651c_to_2651a	sgm-26-51c.cisco.com	5.1.3	2651a_to_2651c	sgm-26-51a.cisco.com	5.1.1	Warning	8	7
2651c_to_2651b	sgm-26-51c.cisco.com	5.1.3	2651b_to_2651c	sgm-26-51b.cisco.com	5.1.2	Warning	8	8
2651c_to_2651d	sgm-26-51c.cisco.com	5.1.3	2651d_to_2651c	sgm-26-51d.cisco.com	5.1.4	Active	8	8
2651c_to_2651d-2	sgm-26-51c.cisco.com	5.1.3	2651d_to_2651c-2	sgm-26-51d.cisco.com	2.1.4	Active	1	1

You can sort the SGM - ITP Linkset Status table based on the information in one of the columns. See the "Resizing, Sorting, and Hiding Table Columns" section on page 3-178 for more details.

The SGM - ITP Linkset Status page displays the following information for each linkset:

- **Server Name (in header)**—Name of the SGM server associated with the linkset.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Linkset Name**—Name of the linkset. To see detailed information for the linkset, click the linkset name.
- **Node**—Name of node for the linkset. To see detailed information for the node, click the node name.
- **Point Code**—Point code of the primary node for the linkset.
- **Adjacent Linkset Name**—Name of adjacent linkset. To see detailed information for the linkset, click the linkset name.
- **Adjacent Node**—Name of adjacent node for the linkset. To see detailed information for the node, click the node name.
- **Adjacent Point Code**—Point code of the adjacent node for the linkset.

- **Status**—Current status of the linkset, with a color-coded background. Possible values are:
  - **Active (green)**—The linkset is currently fully functional.
  - **Unavailable (red)**—An error is preventing traffic from flowing on this linkset.
  - **Shutdown (blue)**—A router administrator has set the linkset to prevent traffic from flowing. When a linkset is set to **Shutdown**, all its associated links are set to **Failed** by Cisco IOS.
  - **Unknown (red)**—Either the node associated with this linkset has failed to respond to an SNMP request, or SGM found that the linkset no longer exists.
  - **Warning (yellow)**—The linkset is active, but one or more links in the linkset is congested or is in **Failed**, **Unknown**, or **Warning** status, and is not flagged as **Ignored**. At least one link is available and can carry traffic.

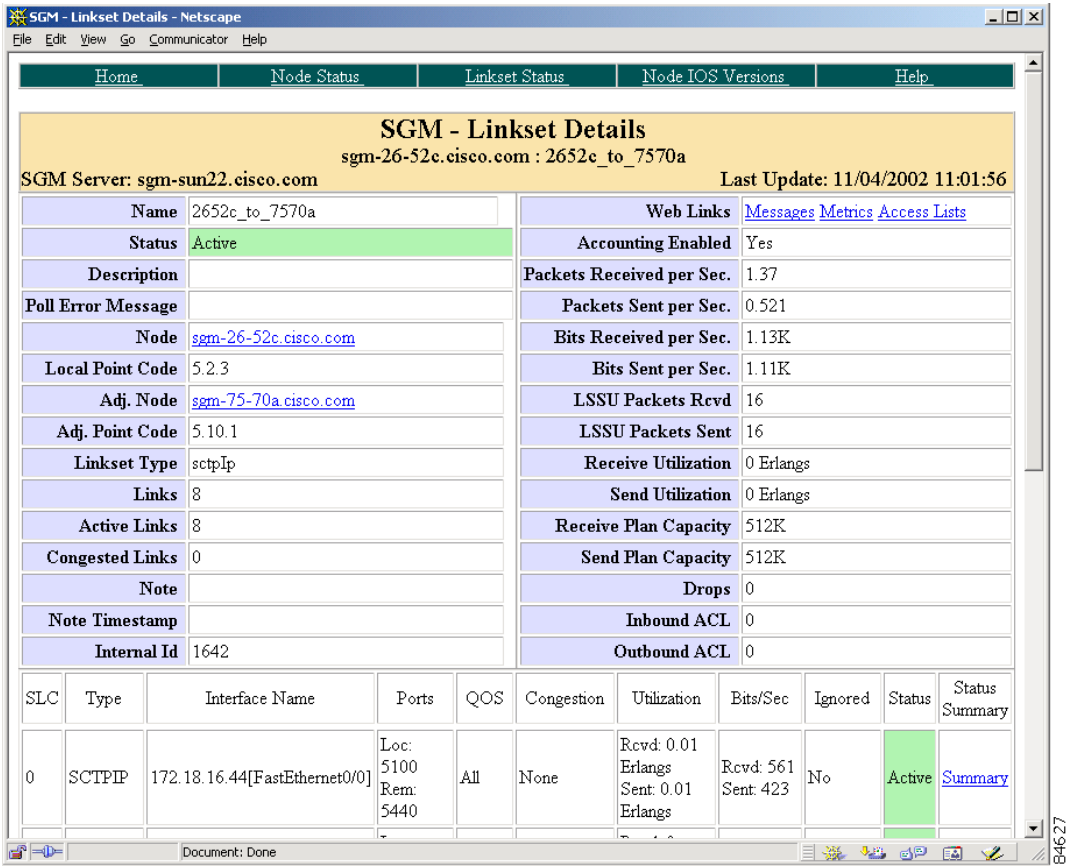
  There is no **Unshut** or **No Shut** status.
- **# Links**—Total number of links in the linkset.
- **Active Links**—Number of links in the linkset that are **Active**.
- **Congested Links**—Number of links in the linkset that are **Congested**.

Viewing ITP Linkset Details

The SGM - Linkset Details page displays detailed information about all discovered linksets, including their associated nodes, links, events, status, and other information.

To access the SGM - Linkset Details page, click a linkset name in the SGM - ITP Linkset Status page. SGM displays the SGM - Linkset Details page (Figure 7-5).

Figure 7-5 SGM - Linkset Details Page



The SGM - Linkset Details page displays the following information for the selected linkset:

- **Node Name and Linkset Name (in header)**—DNS name of the node, as discovered by SGM, and linkset name.
- **Server Name (in header)**—Name of the SGM server associated with the linkset.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.

- **Name**—Name of the linkset.

  To see status change messages and SNMP trap messages associated with the linkset, click **Messages**.

  To see network status metrics associated with the linkset, click **Metrics**.

  To see all access lists associated with the linkset, click **Access Lists**.

- **Status**—Current status of the linkset, with a color-coded background. Possible values are:
  - **Active (green)**—The linkset is currently fully functional.
  - **Unavailable (red)**—An error is preventing traffic from flowing on this linkset.
  - **Shutdown (blue)**—A router administrator has set the linkset to prevent traffic from flowing. When a linkset is set to **Shutdown**, all its associated links are set to **Failed** by Cisco IOS.
  - **Unknown (red)**—Either the node associated with this linkset has failed to respond to an SNMP request, or SGM found that the linkset no longer exists.
  - **Warning (yellow)**—The linkset is active, but one or more links in the linkset is congested or is in **Failed**, **Unknown**, or **Warning** status, and is not flagged as **Ignored**. At least one link is available and can carry traffic.

  There is no **Unshut** or **No Shut** status.

- **Description**—Description of the linkset. If the linkset has no description, this field is blank.
- **Poll Error Message**—Last error message received by the linkset.
- **Node**—Name of primary node for the linkset. To see detailed information for the node, click the node name.
- **Local Point Code**—Point code of the primary node for the linkset.
- **Adj. Node**—Name of adjacent node for the linkset. To see detailed information for the adjacent node, click the node name.
- **Adj. Point Code**—Point code of the adjacent node for the linkset.

- **Linkset Type**—Type of linkset, which SGM determines by examining the links defined in the linkset. Possible linkset types are:
  - **HSL**—The links in this linkset use the SS7-over-ATM (Asynchronous Transfer Mode) high-speed protocol.
  - **SCTPIP**—The links in this linkset use the Stream Control Transmission Protocol (SCTP) IP transport protocol.
  - **Serial**—The links in this linkset use the serial SS7 signaling protocol.
  - **Mixed**—The links in this linkset are of two or more types. (This arrangement is not recommended.)
  - **Other**—No links have been defined for this linkset.
- **Links**—Total number of links in the linkset.
- **Active Links**—Number of links in the linkset that are **Active**.
- **Congested Links**—Number of links in the linkset that are **Congested**.
- **Note**—Note associated with this linkset. If there is no note associated with this linkset, this field is blank.
- **Note Timestamp**—Date and time the note associated with this linkset was last updated. If there is no note associated with this linkset, this field is blank.
- **Internal ID**—Internal ID of the linkset. The internal ID is a unique ID for every event, link, linkset, and node, assigned by SGM for its own internal use. It can also be useful when the Cisco TAC is debugging problems.
- **Accounting Enabled**—Indicates whether the collection of SS7 accounting statistics is enabled for the linkset.
- **Packets Received Per Sec.**—Number of packets received by the linkset per second.

  This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.
- **Packets Sent Per Sec.**—Number of packets sent by the linkset per second.

  This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.
- **Bits Received Per Sec.**—Number of bits received by the linkset per second.

  This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.

- **Bits Sent Per Sec.**—Number of bits sent by the linkset per second.

  This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.

- **LSSU Packets Received**—Total number of SS7 Message Transfer Part Layer 2 (MTP2) Links Status Signal Unit (LSSU) packets received by the linkset.
- **LSSU Packets Sent**—Total number of LSSU packets sent by the linkset.
- **Receive Utilization**—Amount of the linkset's receive capacity being used, as a percentage or in Erlangs, calculated using the following formula:

  Receive Utilization = (Bits Received Per Sec.)/Planned Capacity

  Planned Capacity is the planned capacity of the linkset in bits per second.

  - For a linkset of type **Serial**, **Planned Capacity** is the available bandwidth for the linkset.
  - For a linkset of type **SCTPIP** or of type **Mixed**, **Planned Capacity** is set on the router using the **plan-capacity** CS7 linkset configuration command.
    If **Planned Capacity** is not set on the router for this linkset, this field displays the phrase **Planned Capacity for Router Not Set**.
  - For a linkset of type **Other**, this field displays the phrase **Planned Capacity for Router Not Set**.

  This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.

  If the planned receive capacity is not set for the link, this field displays **Set Plan Capacity on Router**.

- **Send Utilization**—Amount of the linkset's send capacity being used, as a percentage or in Erlangs, calculated using the following formula:

  Send Utilization = (Bits Sent Per Sec.)/Planned Capacity

  Planned Capacity is the planned capacity of the linkset in bits per second.

  - For a linkset of type **Serial**, **Planned Capacity** is the available bandwidth for the linkset.
  - For a linkset of type **SCTPIP** or of type **Mixed**, **Planned Capacity** is set on the router using the **plan-capacity** CS7 linkset configuration command.
    If **Planned Capacity** is not set on the router for this linkset, this field displays the phrase **Planned Capacity for Router Not Set**.
  - For a linkset of type **Other**, this field displays the phrase **Planned Capacity for Router Not Set**.

  This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.

  If the planned send capacity is not set for the link, this field displays **Set Plan Capacity on Router**.

- **Receive Plan Capacity**—Planned capacity of the linkset to receive, in bits per second.
  - For a linkset of type **Serial** or **HSL**, available bandwidth for the linkset.
  - For a linkset of type **SCTPIP** or **Mixed**, set on the router using the **plan-capacity** CS7 linkset configuration command.

    If **Receive Plan Capacity** is not set on the router for this linkset, this field displays the value **0**.
  - For a linkset of type **Other**, this field always displays the value **0**.

- **Send Plan Capacity**—Planned capacity of the linkset to send, in bits per second.
  - For a linkset of type **Serial** or **HSL**, available bandwidth for the linkset.
  - For a linkset of type **SCTPIP** or **Mixed**, set on the router using the **plan-capacity** CS7 linkset configuration command.

    If **Send Plan Capacity** is not set on the router for this linkset, this field displays the value **0**.
  - For a linkset of type **Other**, this field always displays the value **0**.
- **Drops**—Total number of packets that have been dropped by the linkset.
- **Inbound ACL**—Inbound IP access control list (ACL) for the linkset. If there is no inbound ACL for the linkset, this field displays **0**.
- **Outbound ACL**—Outbound ACL for the linkset. If there is no outbound ACL for the linkset, this field displays **0**.

The SGM - Linkset Details page also displays the following information about links associated with the selected linkset:

- **SLC**—Identifier for the link, assigned by SGM.
- **Type**—Type of link. Possible link types are:
  - **HSL**—The link uses the SS7-over-ATM (Asynchronous Transfer Mode) high-speed protocol.
  - **SCTPIP**—The link uses the Stream Control Transmission Protocol (SCTP) IP transport protocol.
  - **Serial**—The link uses the serial SS7 signaling protocol.

- **Interface Name**—For serial and HSL links, this field displays the interface name of the link.

  For SCTP links, this field displays the primary IP address and interface name of the link. The primary IP address is the first CS7 local IP address configured in the router. For example, if the following IP addresses are configured in the router:

  ```
  cs7 local-peer 4180
    local-ip 128.3.0.77
    local-ip 128.3.0.254
  ```

  Then SGM uses **128.3.0.77** as the primary IP address. If at any time that IP address is deleted from the router configuration, or if a new IP address is added to the beginning of the list, SGM detects the change and automatically updates this field to reflect the new primary IP address.

  If the link has no interface name, this field is blank.

- **Ports**—Local and remote ports for the link.
- **QoS**—Quality of service (QoS) class of the link.
- **Congestion**—Indicates whether there is congestion on the link. A link is congested if it has too many packets waiting to be sent. This condition could be caused by the failure of an element in your network.

  Possible values for the **Congestion** field are:

  - **None**—The link is not congested.
  - **Low**—The link is slightly congested.
  - **High**—The link is congested.
  - **Very High**—The link is very congested.

  Low, **High**, and **Very High** correspond roughly to equivalent ANSI, China standard, and ITU congestion levels.

- **Utilization**—Receive Utilization (Rcvd) and Send Utilization (Sent) for the link, expressed as either a utilization percentage or a number of Erlangs.

  This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.

  If the planned send or receive capacity is not set for the link, this field displays **Set Plan Capacity on Router**.

- **Bits/Sec**—Number of bits received (Rcvd) and sent by the link per second.

  This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.

- **Ignored**—Indicates whether the link has been flagged as **Ignored** (that is, whether the link is to be included when aggregating and displaying SGM status information).

- **Status**—Current status of the link, with a color-coded background. Possible values are:

  - **Active (green)**—The link is currently fully functional.
  - **Blocked (red)**—Either the node associated with this link has failed to respond to an SNMP request, or SGM found that the link no longer exists.
  - **Failed (red)**—An error is preventing traffic from flowing on this link, or the associated linkset has been set to **Shutdown** status.

    A link can be **Failed** from an MTP3 perspective, but control messages might still be sent or received on the link, resulting in changing packet/second and bit/second rates. The rates might also be different at each end of the link, depending on the reason for the failure and the timing related to each endpoint.
  - **InhibitLoc (blue)**—A local router administrator has set the link to prevent traffic from flowing.
  - **InhibitRem (blue)**—A remote router administrator has set the link to prevent traffic from flowing.
  - **Shutdown (blue)**—A router administrator has set the link to prevent traffic from flowing.

  - **Unknown (red)**—Either the node associated with this link has failed to respond to an SNMP request, or SGM found that the link no longer exists.

    When you physically delete a link, the **Status** field displays **Unknown** until you delete the link from the SGM database.

  - **Warning (yellow)**—The link is active and traffic is flowing, but one or more situations has occurred:

    - The link is congested.

    - The link has exceeded the defined **Receive Utilization %** or **Send Utilization %**.

    - One or more of the local or remote IP addresses defined for SCTP is not active.

  There is no **Unshut** or **No Shut** status.

- **Status Summary**—Opens the SGM - Link Status Summary Web Page.

Viewing ITP Linkset Information - Access Lists

The SGM - ITP Access Lists page displays all access lists associated with the selected linkset.

To access the SGM - ITP Access Lists page, select a linkset in the Linkset or Topology window, then select **Drill Down>Show Access List** from the right-click menu.

The SGM - ITP Access Lists page displays the following information for the selected linkset:

- **Node Name (in header)**—Name of the node for which access lists are being displayed.
- **Server Name (in header)**—Name of the SGM server associated with the linkset.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Node/Linkset**—Name of the node and linkset for which access lists are being displayed. To see detailed information for the node or linkset, click the node or linkset name.

- **List #**—Access list number configured on the node and applied to the linkset. ITP uses access list numbers 2700 through 2799.
- **Access List**—List of commands in the access list.

Viewing the Network Status Linkset Dashboard

The SGM - Linkset Dashboard page lists all discovered linksets, and provides links to messages and metrics for each linkset.

To access the SGM - Linkset Dashboard page, select **Network Status Dashboard** from the SGM Server Home Page, then click **Linkset Dashboard**.

To see status change messages and SNMP trap messages associated with a given linkset, click **Messages**.

To see network status metrics associated with a given linkset, click **Metrics**.

To see all access lists associated with a given linkset, click **Access Lists**.

You can sort the table based on the information in the **Linksets** column. See the "Resizing, Sorting, and Hiding Table Columns" section on page 3-178 for more details.

Viewing Information About Links

SGM enables you to view the following information about links:

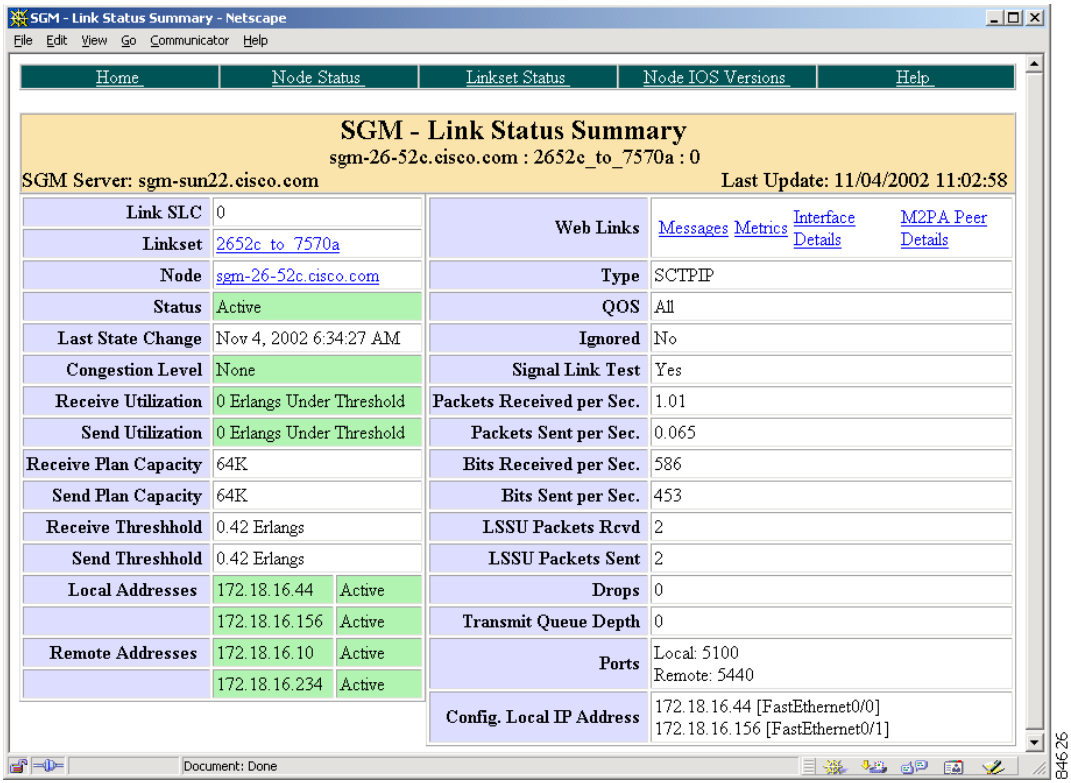
- Viewing ITP Link Status, page 7-37
- Viewing Interface Details for a Link, page 7-42
- Viewing M2PA Peer Details for a Link, page 7-45
- Viewing the Network Status Link Dashboard, page 7-49

Viewing ITP Link Status

The SGM - Link Status Summary page displays status information for a single link.

To access the SGM - Link Status Summary page, click a linkset name in the SGM - ITP Linkset Status page to display the SGM - Linkset Details page, then click **Summary** beside a link at the bottom of the page. SGM displays the SGM - Link Status Summary page (Figure 7-6).

Figure 7-6 SGM - Link Status Summary Page



The SGM - Link Status Summary page displays the following information for the selected link:

- **Node Name, Linkset Name, and SLC (in header)**—Name of the node and linkset associated with the link, and the SLC of the link.
- **Server Name (in header)**—Name of the SGM server associated with the link.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Link SLC**—Signaling link code (SLC) ID for the link.

  To see status change messages and SNMP trap messages associated with the link, click **Messages**.

  To see network status metrics associated with the link, click **Metrics**.

  To see detailed interface information for the link, click **Interface Details**. (This field is displayed only if the selected link has a status of **Active** or **Warning** and is connected to an ITP device.)

  To see detailed M2PA peer information for the link, click **M2PA Peer Details**. (This field is displayed only if the selected link has a status of **Active** or **Warning** and is connected to an ITP device.)
- **Linkset**—Name of the linkset associated with the link. To see detailed information for the linkset, click the linkset name.
- **Node**—Name of the node associated with the link. To see detailed information for the node, click the node name.
- **Type**—Type of link. Possible link types are:
  - **HSL**—The link uses the SS7-over-ATM (Asynchronous Transfer Mode) high-speed protocol.
  - **SCTPIP**—The link uses the Stream Control Transmission Protocol (SCTP) IP transport protocol.
  - **Serial**—The link uses the serial SS7 signaling protocol.

- **Status**—Current status of the link, with a color-coded background. Possible values are:
  - **Active (green)**—The link is currently fully functional.
  - **Blocked (red)**—Either the node associated with this link has failed to respond to an SNMP request, or SGM found that the link no longer exists.
  - **Failed (red)**—An error is preventing traffic from flowing on this link, or the associated linkset has been set to **Shutdown** status.

    A link can be **Failed** from an MTP3 perspective, but control messages might still be sent or received on the link, resulting in changing packet/second and bit/second rates. The rates might also be different at each end of the link, depending on the reason for the failure and the timing related to each endpoint.
  - **InhibitLoc (blue)**—A local router administrator has set the link to prevent traffic from flowing.
  - **InhibitRem (blue)**—A remote router administrator has set the link to prevent traffic from flowing.
  - **Shutdown (blue)**—A router administrator has set the link to prevent traffic from flowing.
  - **Unknown (red)**—Either the node associated with this link has failed to respond to an SNMP request, or SGM found that the link no longer exists.

    When you physically delete a link, the **Status** field displays **Unknown** until you delete the link from the SGM database.
  - **Warning (yellow)**—The link is active and traffic is flowing, but one or more situations has occurred:

    - The link is congested.

    - The link has exceeded the defined **Receive Utilization %** or **Send Utilization %**.

    - One or more of the local or remote IP addresses defined for SCTP is not active.

  There is no **Unshut** or **No Shut** status.
- **QoS**—Quality of service (QoS) class of the link.
- **Last State Change**—Date and time that the status of the link last changed.

- **Ignored**—Indicates whether the link is **Ignored** (that is, whether the link is to be included when aggregating and displaying SGM status information).
- **Congestion Level**—Indicates whether there is congestion on the link. A link is congested if it has too many packets waiting to be sent. This condition could be caused by the failure of an element in your network.

  Possible values for the **Congestion** field are:

  - **None**—The link is not congested.
  - **Low**—The link is slightly congested.
  - **High**—The link is congested.
  - **Very High**—The link is very congested.

  Low, **High**, and **Very High** correspond roughly to equivalent ANSI, China standard, and ITU congestion levels.
- **Signal Link Test**—Indicates whether the link acknowledged a Signal Link Test Message (SLTM), which tests the link's ability to carry data.
- **Receive Utilization**—Amount, expressed as either a utilization percentage or a number of Erlangs, that the link is under (**UnderThreshold**) or over (**OverThreshold**) its configured receive utilization threshold.
- **Packets Received Per Sec.**—Number of packets received by the link per second. This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.
- **Send Utilization**—Amount, expressed as either a utilization percentage or a number of Erlangs, that the link is under (**UnderThreshold**) or over (**OverThreshold**) its configured send utilization threshold.
- **Packets Sent Per Sec.**—Number of packets sent by the link per second. This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.

- **Receive Plan Capacity**—Planned capacity of the link to receive, in bits per second.
  - For a link of type **Serial** or **HSL**, available bandwidth for the link.
  - For a link of type **SCTPIP** or **Mixed**, set on the router using the **plan-capacity** CS7 link configuration command.

    If **Receive Plan Capacity** is not set on the router for this link, this field displays the value **0**.
  - For a link of type **Other**, this field always displays the value **0**.
- **Bits Received Per Sec.**—Number of bits received by the link per second. This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.
- **Send Plan Capacity**—Planned capacity of the link to send, in bits per second.
  - For a link of type **Serial** or **HSL**, available bandwidth for the link.
  - For a link of type **SCTPIP** or **Mixed**, set on the router using the **plan-capacity** CS7 link configuration command.

    If **Send Plan Capacity** is not set on the router for this link, this field displays the value **0**.
  - For a link of type **Other**, this field always displays the value **0**.
- **Bits Sent Per Sec.**—Number of bits sent by the link per second. This field initially displays the phrase **Waiting for second poll**. After two polling cycles, SGM populates this field with actual calculated rates.
- **Receive Threshold**—Indicates when a cItpSpLinkRcvdUtilChange is to be generated for the link, as a percent of its total receive capacity. For example, if Receive Plan **Capacity** is **64000** bits per second, and Receive Threshold % is **50**, then a cItpSpLinkRcvdUtilChange notification is generated when the link reaches 50% of 64000, or 32000 bits per second.
- **LSSU Packets Received**—Total number of SS7 Message Transfer Part Layer 2 (MTP2) Links Status Signal Unit (LSSU) packets received by the link.
- **Send Threshold**—Indicates when a cItpSpLinkSentUtilChange is to be generated for the link, as a percent of its total send capacity. For example, if Send Plan **Capacity** is **64000** bits per second, and Send Threshold % is **50**, then a cItpSpLinkSentUtilChange notification is generated when the link reaches 50% of 64000, or 32000 bits per second.

- **LSSU Packets Sent**—Total number of LSSU packets sent by the link.
- **Local Addresses**—Local IP addresses associated with the link, and their status.
- **Remote Addresses**—Remote IP addresses associated with the link, and their status.
- **Drops**—Total number of packets that have been dropped by the link.
- **Transmit Queue Depth**—Number of packets waiting to be sent on by the link.
- **Ports**—Local and remote ports for the link.
- **Config. Local IP Address**—Configured local IP address associated with the link.

Viewing Interface Details for a Link

The SGM - Interface Details page displays detailed interface information for a link, with one column of information for each of the link's interfaces.

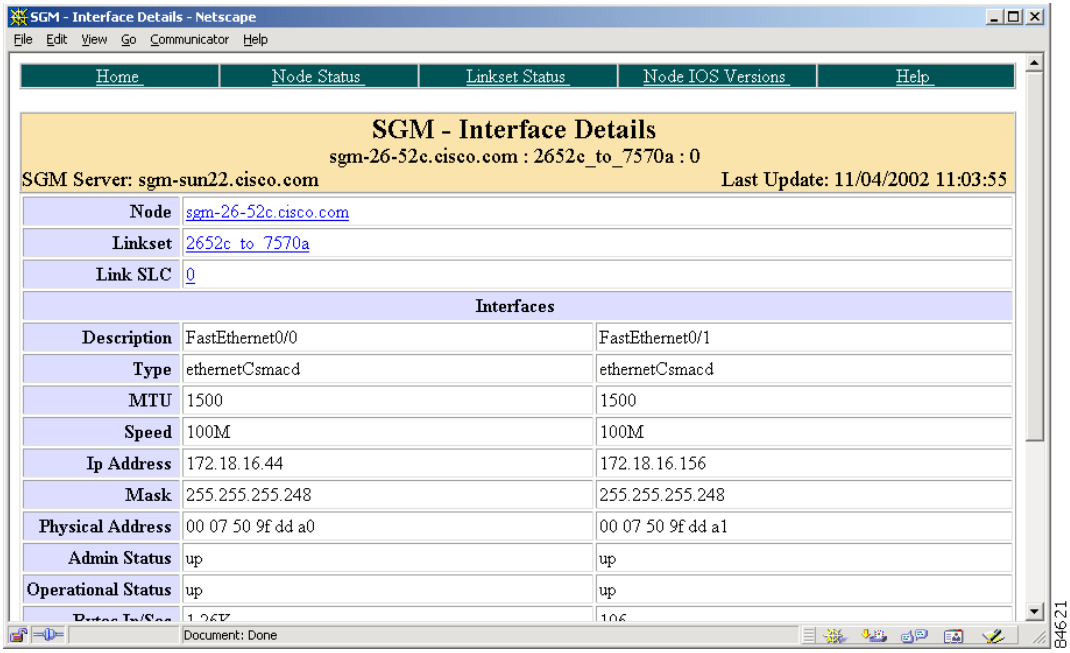
To access the SGM - Interface Details page, use the following procedure:

Step 1 Click a linkset name in the SGM - ITP Linkset Status page to display the SGM - Linkset Details page.

Step 2 Click **Summary** beside a link at the bottom of the page to display the SGM - Link Status Summary page.

Step 3 Click **Interface Details** to display the SGM - Interface Details page (Figure 7-7).

Figure 7-7 SGM - Interface Details Page



The SGM - Interface Details table displays the following information for the selected link:

- **Node Name, Linkset Name, and SLC (in header)**—Name of the node and linkset associated with the link, and the SLC of the link.
- **Server Name (in header)**—Name of the SGM server associated with the link.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Node**—Name of the node associated with the link. To see detailed information for the node, click the node name.
- **Linkset**—Name of the linkset associated with the link. To see detailed information for the linkset, click the linkset name.
- **Link SLC**—Signaling link code (SLC) ID for the link. To see detailed information for the link, click the link name.

- **Description**—Text string containing information about the interface.
- **Type**—Type of interface, such as Ethernet.
- **MTU**—Size, in bytes, of the largest datagram that can be sent or received on the interface.
- **Speed (Bits/Sec)**—Estimate, in bits per second, of the interface's current bandwidth. If the interface does not vary in bandwidth, or if no accurate estimate can be made, this field displays the nominal bandwidth.
- **IP Address**—IP address corresponding to the media-dependent "physical" address. If the interface does not have such an address (for example, a serial line), this field displays **N/A**.
- **Mask**—Subnet mask corresponding to the media-dependent "physical" address. If the interface does not have such an address (for example, a serial line), this field displays **N/A**.
- **Physical Address**—Address of the interface at the protocol layer immediately "below" the network layer in the protocol stack. If the interface does not have such an address (for example, a serial line), this field displays **N/A**.
- **Admin Status**—Desired state of the interface. Possible values are:
  - **up**
  - **down**
  - **testing**
- **Operational Status**—Current operational state of the interface. Possible values are:
  - **up**
  - **down**
  - **testing**
  - **unknown**
  - **dormant**
- **Bytes In**—Number of bytes received on the interface per second, including framing characters.
- **Bytes Out**—Number of bytes sent on the interface per second, including framing characters.

- **Packets In**—Number of packets delivered to a higher-layer protocol.
- **Packets Out**—Total number of packets that higher-level protocols requested to be sent to the network, including those that were discarded or not sent.
- **Discards In**—Number of inbound packets that were discarded, even though no errors were detected to prevent their delivery to a higher-layer protocol. For example, a packet might be discarded to free buffer space.
- **Discards Out**—Number of outbound packets that were discarded, even though no errors were detected to prevent their delivery to a higher-layer protocol. For example, a packet might be discarded to free buffer space.
- **Errors In**—Number of inbound packets that contained errors that prevented their delivery to a higher-layer protocol.
- **Errors Out**—Number of outbound packets that were not sent because of errors.

Viewing M2PA Peer Details for a Link

The SGM - M2PA Peer Details page displays detailed SCTP association information for a link.

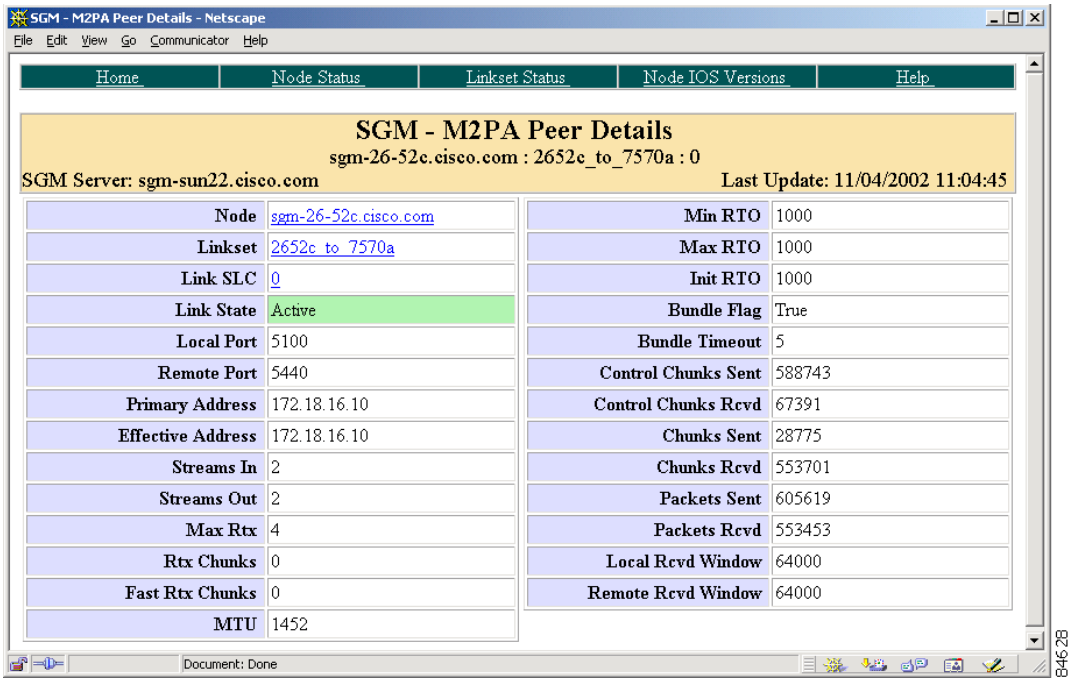
To access the SGM - M2PA Peer Details page, use the following procedure:

Step 1 Click a linkset name in the SGM - ITP Linkset Status page to display the SGM - Linkset Details page.

Step 2 Click **Summary** beside a link at the bottom of the page to display the SGM - Link Status Summary page.

Step 3 Click **M2PA Peer Details** to display the SGM - M2PA Peer Details page (Figure 7-8).

Figure 7-8 SGM - M2PA Peer Details Page



The SGM - M2PA Peer Details table displays the following information for the selected link:

- **Node Name, Linkset Name, and SLC (in header)**—Name of the node and linkset associated with the link, and the SLC of the link.
- **Server Name (in header)**—Name of the SGM server to which this SCTP association belongs.
- **Last Update (in header)**—Date and time the information on the page was last updated by SGM.
- **Node**—Name of the node to which this SCTP association belongs.
- **Linkset**—Name of the linkset to which this SCTP association belongs.
- **Link SLC**—Signaling link code (SLC) ID to which this SCTP association corresponds.

- **Link State**—Current status of the link to which this SCTP association corresponds, with a color-coded background. Possible values are:
  - **Active (green)**—The link is currently fully functional.
  - **Blocked (red)**—Either the node associated with this link has failed to respond to an SNMP request, or SGM found that the link no longer exists.
  - **Failed (red)**—An error is preventing traffic from flowing on this link, or the associated linkset has been set to **Shutdown** status.

    A link can be **Failed** from an MTP3 perspective, but control messages might still be sent or received on the link, resulting in changing packet/second and bit/second rates. The rates might also be different at each end of the link, depending on the reason for the failure and the timing related to each endpoint.
  - **InhibitLoc (blue)**—A local router administrator has set the link to prevent traffic from flowing.
  - **InhibitRem (blue)**—A remote router administrator has set the link to prevent traffic from flowing.
  - **Shutdown (blue)**—A router administrator has set the link to prevent traffic from flowing.
  - **Unknown (red)**—Either the node associated with this link has failed to respond to an SNMP request, or SGM found that the link no longer exists.

    When you physically delete a link, the **Status** field displays **Unknown** until you delete the link from the SGM database.
  - **Warning (yellow)**—The link is active and traffic is flowing, but one or more situations has occurred:

    – The link is congested.

    – The link has exceeded the defined **Receive Utilization %** or **Send Utilization %**.

    – One or more of the local or remote IP addresses defined for SCTP is not active.

  There is no **Unshut** or **No Shut** status.
- **Local Port**—Local port number for the SCTP association.
- **Remote Port**—Remote port number for the SCTP association.
- **Primary Address**—Designated primary IP address for the SCTP association.

- **Effective Address**—IP address currently being used by the SCTP association.
- **Streams In**—Inbound streams as negotiated when the SCTP association was started.
- **Streams Out**—Outbound streams as negotiated when the SCTP association was started.
- **Max Rtx**—Maximum number of data retransmissions in the SCTP association context.
- **Rtx Chunks**—Number of data chunks retransmitted to the peer in the current SCTP association.
- **Fast Rtx Chunks**—Total number of SCTP chunks retransmitted in the current SCTP association, using the fast-recovery retransmission mechanism specified in SCTP.
- **MTU**—Maximum transmission unit (MTU) size to be used by this SCTP association. This is the smallest MTU size supported by any of the IP addresses used by the SCTP association.
- **Min RTO**—Minimum timeout value, in milliseconds, permitted by the SCTP implementation for the retransmission timeout (RTO).
- **Max RTO**—Maximum timeout value, in milliseconds, permitted by the SCTP implementation for the RTO.
- **Init RTO**—Initial timeout value, in milliseconds, permitted by the SCTP implementation for the RTO.
- **Bundle Flag**—Indicates whether the SCTP protocol allows chunks to be bundled into a single datagram as follows. Valid values are:
  - **true (1)**—Chunks are bundled.
  - **false (2)**—Chunks are not bundled.
- **Bundle Timeout**—Time, in milliseconds, to wait to allow data chunks to accumulate so that they can be transmitted in the same datagram.
- **Control Chunks Sent**—Number of control chunks sent by this SCTP association.
- **Control Chunks Recv**—Number of control chunks received by this SCTP association.
- **Chunks Sent**—Number of chunks sent by this SCTP association.

- **Chunks Recv**—Number of chunks received by this SCTP association.
- **Packets Sent**—Number of IP datagrams sent by this SCTP association.
- **Packets Recv**—Number of IP datagrams received by this SCTP association.
- **Local Recv Window**—Current local receive window size for this SCTP association.
- **Remote Recv Window**—Current local send window size for this SCTP association.

Viewing the Network Status Link Dashboard

The SGM - Link Dashboard page lists all discovered links, and provides links to messages and metrics for each link.

To access the SGM - Link Dashboard page, select **Network Status Dashboard** from the SGM Server Home Page, then click **Link Dashboard**.

To see status change messages and SNMP trap messages associated with a given link, click **Messages**.

To see network status metrics associated with a given link, click **Metrics**.

To see detailed interface information for a given link, click **Interface Details**. (This field is displayed only if the selected link has a status of **Active** or **Warning** and is connected to an ITP device.)

To see detailed SCTP association information for a given link, click **M2PA Peer Details**. (This field is displayed only if the selected link has a status of **Active** or **Warning** and is connected to an ITP device.)

You can sort the table based on the information in the **Links** column. See the "Resizing, Sorting, and Hiding Table Columns" section on page 3-178 for more details.

Viewing Status Change and SNMP Trap Messages

SGM enables you to view the following status change and SNMP trap messages:

- Viewing Status Change and SNMP Trap Messages for SGM, page 7-50
- Viewing Status Change Messages for SGM, page 7-52
- Viewing SNMP Trap Messages for SGM, page 7-54

- Viewing All Archived Status Change and SNMP Trap Messages, page 7-55
- Modifying Network Status Message Colors, page 7-56

Viewing Status Change and SNMP Trap Messages for SGM

The Network Status - Last Status Change and Trap Messages page displays status change messages and SNMP trap messages in the SGM network log.

To access the Network Status - Last Status Change and Trap Messages page and display all status change and trap messages, use one of the following procedures:

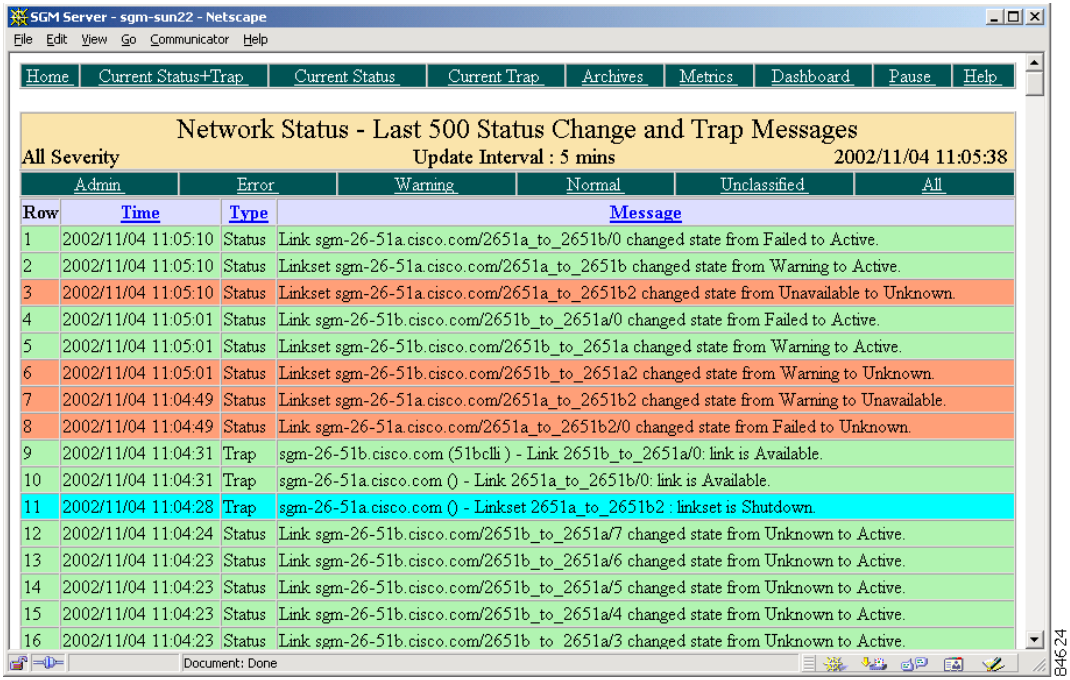
- Select **Web Links>Status & Trap Messages>All** from the SGM Main Menu.
- Select **Status & SNMP Trap Messages** from the SGM Server Home Page.

To access the Network Status - Last Status Change and Trap Messages page and display status change and trap messages for a specific node, linkset, or event, use one of the following procedures:

- Select a node, linkset, or event in a window, then select **Web Links>Status & Trap Messages>Selected Item** from the SGM Main Menu.
- Right-click a node, linkset, or event in a window, then select **Web Links>Status and Trap Messages** from the right-click menu.

SGM displays the Network Status - Last Status Change and Trap Messages page (Figure 7-9).

Figure 7-9 Network Status - Last Status Change and Trap Messages Page



The Network Status - Last Status Change and Trap Messages page displays the following information for each message:

- **Severity (in header)**—Message severity currently being displayed.
- **Update Interval (in header)**—Interval between updates for the page.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Row—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged.
- **Type—**Type of message:
  - **Status**—Status change message
  - **Trap**—SNMP trap message
- **Message—**Text of the message.

To sort the messages by time, type, or alphabetically by message text, click the **Time**, **Type**, or **Message** header.

By default, SGM displays status change and SNMP trap messages of all types on the Network Status - Last Status Change and Trap Messages page. However, menu options are provided that enable you to display only messages of a specific type on the page. To display only messages of a specific type, select one of the following options:

- **Admin—**Displays only administrative messages. SGM displays administrative messages with a cyan background.
- **Error—**Displays only error messages. SGM displays error messages with a coral background.
- **Warning—**Displays only warning messages. SGM displays warning messages with a yellow background.
- **Normal—**Displays only normal messages. SGM displays normal messages with a light green background.
- **Unclassified—**Displays only messages that do not fall into one of the above classifications. SGM displays unclassified messages with a white background.
- **All—**Displays all status change and SNMP trap messages.

The list of messages displayed in the Last Status Change and Trap Messages table is continually refreshed as new messages are received.

- To pause the message display, select **Pause** from the menu bar.
- To resume the message display, select **Resume** from the menu bar.

Viewing Status Change Messages for SGM

The Network Status - Last Status Change Messages page displays status change messages in the SGM network log.

To access the Network Status - Last Status Change Messages page and display all status change messages, use one of the following procedures:

- Select **Web Links>Status Change Messages>All** from the SGM Main Menu.
- Select **Status Change Messages** from the SGM Server Home Page.

To access the Network Status - Last Status Change Messages page and display status change messages for a specific node, linkset, or event, use one of the following procedures:

- Select a node, linkset, or event in a window, then select **Web Links>Status Change Messages>Selected Item** from the SGM Main Menu.
- Right-click a node, linkset, or event in a window, then select **Web Links>Status Change Messages** from the right-click menu.

The Network Status - Last Status Change Messages page displays the following information for each message:

- **Severity (in header)**—Message severity currently being displayed.
- **Update Interval (in header)**—Interval between updates for the page.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Row—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged.
- **Message—**Text of the message.

To sort the messages by time or alphabetically by message text, click the **Time** or **Message** header.

By default, SGM displays status change messages of all types on the Network Status - Last Status Change Messages page. However, menu options are provided that enable you to display only messages of a specific type on the page. To display only messages of a specific type, select one of the following options:

- **Admin—**Displays only administrative messages. SGM displays administrative messages with a cyan background.
- **Error—**Displays only error messages. SGM displays error messages with a coral background.
- **Warning—**Displays only warning messages. SGM displays warning messages with a yellow background.
- **Normal—**Displays only normal messages. SGM displays normal messages with a light green background.

- **Unclassified—**Displays only messages that do not fall into one of the above classifications. SGM displays unclassified messages with a white background.
- **All—**Displays all status change messages.

The list of messages displayed in the Last Status Change Messages table is continually refreshed as new messages are received.

- To pause the message display, select **Pause** from the menu bar.
- To resume the message display, select **Resume** from the menu bar.

Viewing SNMP Trap Messages for SGM

The Network Status - Last SNMP Trap Messages page displays SNMP trap messages in the SGM network log.

To access the Network Status - Last SNMP Trap Messages page and display all SNMP trap messages, use one of the following procedures:

- Select **Web Links>SNMP Trap Messages>All** from the SGM Main Menu.
- Select **SNMP Trap Messages** from the SGM Server Home Page.

To access the Network Status - Last SNMP Trap Messages page and display SNMP trap messages for a specific node, linkset, or event, use one of the following procedures:

- Select a node, linkset, or event in a window, then select **Web Links>SNMP Trap Messages>Selected Item** from the SGM Main Menu.
- Right-click a node, linkset, or event in a window, then select **Web Links>SNMP Trap Messages** from the right-click menu.

The Network Status - Last SNMP Trap Messages page displays the following information for each message:

- **Severity (in header)**—Message severity currently being displayed.
- **Update Interval (in header)**—Interval between updates for the page.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Row—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged.
- **Message—**Text of the message.

To sort the messages by time or alphabetically by message text, click the **Time** or **Message** header.

By default, SGM displays SNMP trap messages of all types on the Network Status - Last SNMP Trap Messages page. However, menu options are provided that enable you to display only messages of a specific type on the page. To display only messages of a specific type, select one of the following options:

- **Admin—**Displays SNMP trap administrative messages. SGM displays administrative messages with a cyan background.
- **Error—**Displays SNMP trap error messages. SGM displays error messages with a coral background.
- **Warning—**Displays SNMP trap warning messages. SGM displays warning messages with a yellow background.
- **Normal—**Displays normal SNMP trap messages. SGM displays normal messages with a light green background.
- **Unclassified—**Displays SNMP trap messages that do not fall into one of the above classifications. SGM displays unclassified messages with a white background.
- **All—**Displays all SNMP trap messages.

The list of messages displayed in the Last SNMP Trap Messages table is continually refreshed as new messages are received.

- To pause the message display, select **Pause** from the menu bar.
- To resume the message display, select **Resume** from the menu bar.

Viewing All Archived Status Change and SNMP Trap Messages

The Network Status Archives - Status and SNMP Trap Messages page displays all archived status change and SNMP trap messages.

To access the Network Status Archives - Status and SNMP Trap Messages page, use one of the following procedures:

- Select **Web Links>Network Status Archives** from the SGM Main Menu.
- Select **Network Status Archives** from the SGM Server Home Page.

On the Network Status Archives - Status and SNMP Trap Messages page, messages are archived by time stamp. SGM automatically archives the messages at 11:59 PM each night; each archived file contains messages from a single calendar day.

To view archived messages, click a time stamp. SGM displays the message archive, with columns and features as described in the "Viewing Status Change and SNMP Trap Messages for SGM" section on page 7-50.

Modifying Network Status Message Colors

By default, SGM displays network status messages with the following background colors:

- **Admin—**cyan background
- **Error—**coral background
- **Normal—**light green background
- **Warning—**yellow background
- **Unclassified—**white background

For information about customizing the background colors for network status messages, see the "Modifying the SGM Event Configuration File (Solaris Only)" section on page 5-25.

Viewing Network Status Metrics

The Network Status Messages - Messages page displays a number of metrics for SGM, based on the number of messages of each type and severity received by SGM.

To access the Network Status Messages - Messages page and display all metrics, use one of the following procedures:

- Select **Web Links>Network Status Metrics>All** from the SGM Main Menu.
- Select **Network Status Metrics** from the SGM Server Home Page.

To access the Network Status Messages - Messages page and display metrics for a specific node, linkset, or event, use one of the following procedures:

- Select a node, linkset, or event in a window, then select **Web Links > Network Status Metrics > Selected Item** from the SGM Main Menu.
- Right-click a node, linkset, or event in a window, then select **Web Links > Network Status Metrics** from the right-click menu.

The Network Status Messages - Messages page displays both raw numbers and calculated metrics for the following information:

- Total number of messages of each type and severity received by SGM.
- Messages sorted by severity.
- Messages sorted by type (status change messages and SNMP trap messages)
- Status change messages sorted by severity.
- SNMP trap messages sorted by severity.
- Names of all files processed by SGM.
- Beginning and ending date and time for the displayed metrics.

Viewing Network Statistics Reports for Links and Linksets

You can view the following SGM network statistics reports for links and linksets from the SGM Server Home Page:

- Linkset Statistics Hourly Summary Reports
- Linkset Statistics Daily Summary Reports
- Link Statistics Hourly Summary Reports
- Link Statistics Daily Summary Reports
- Five Day Link Utilization Report
- Hourly Network Statistics Export Files
- Daily Network Statistics Export Files
- Rolling Network Statistics Export Files
- Custom Network Statistics Export Files

For more information, see the "Viewing SGM Network Statistics Reports" section on page 3-228.

Viewing Accounting Statistics Reports

You can view the following SGM accounting statistics reports from the SGM Server Home Page:

- Accounting Statistics Daily Detail Reports
- Daily Accounting Statistics Export Files
- Custom Network Statistics Export Files

For more information, see the "Viewing SGM Accounting Statistics Reports" section on page 3-248.

Viewing Point Code Inventory Reports

You can view the following SGM point code inventory reports from the SGM Server Home Page:

- Current Point Code Inventory
- Daily Point Code Inventory Daily Reports
- Daily Point Code Inventory Export Files

For more information, see the "Viewing SGM Point Code Inventory Reports" section on page 3-275.

Viewing Statistics Report Logs

You can view the following SGM network and accounting statistics report logs from the SGM Server Home Page:

- SGM System Reports Logs
- SGM System Report Parameters and Timers

For more information, see the "Viewing SGM Statistics Reports Logs" section on page 3-279.

Viewing SGM System Messages

You can view the following SGM system messages from the SGM Server Home Page.

Note These messages are all related to the SGM system itself, not to your network.

Viewing SGM Error Messages

The System Messages - Last Error Messages page displays error messages stored in the SGM system log. These messages can be useful when diagnosing and correcting SGM operational problems.

To access the System Messages - Last Error Messages page, use one of the following procedures:

- Select **System Error Messages** from the SGM Server Home Page.
- Select **Error** from the menu bar of any SGM System Messages Web page.

The Last Error Messages table provides the following information for each message:

- **Period (in header)**—Collection period of the table, such as **Since Server Restart**.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Row—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged. To sort the messages by time, click the **Time** header.
- **Source—**Source for the message, with the format *process.host.id*, where:
  - *process* is the process that logged the message.
  - *host* is the host name of the process that logged the message.
  - *id* is an SGM ID that uniquely identifies the process that logged the message, in the event that there are two or more clients running on the same device, connected to the same SGM server.
- **Task—**Task, or thread, that logged the message.
- **Message—**Text of the message. To sort the messages alphabetically by message text, click the **Message** header.

To sort the messages by time or alphabetically by message text, click the **Time** or **Message** header.

Viewing SGM Info Messages

The System Messages - Last Info Messages page displays informational messages stored in the SGM system log. These messages can be useful when diagnosing and correcting SGM operational problems.

To access the System Messages - Last Info Messages page, select **Info** from the menu bar of any SGM System Messages Web page.

The Last Info Messages table provides the following information for each message:

- **Period (in header)**—Collection period of the table, such as **Since Server Restart**.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Row—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged. To sort the messages by time, click the **Time** header.
- **Source—**Source for the message, with the format *process.host.id*, where:
  - *process* is the process that logged the message.
  - *host* is the host name of the process that logged the message.
  - *id* is an SGM ID that uniquely identifies the process that logged the message, in the event that there are two or more clients running on the same device, connected to the same SGM server.
- **Task—**Task, or thread, that logged the message.
- **Message—**Text of the message. To sort the messages alphabetically by message text, click the **Message** header.

To sort the messages by time or alphabetically by message text, click the **Time** or **Message** header.

Viewing SGM Action Messages

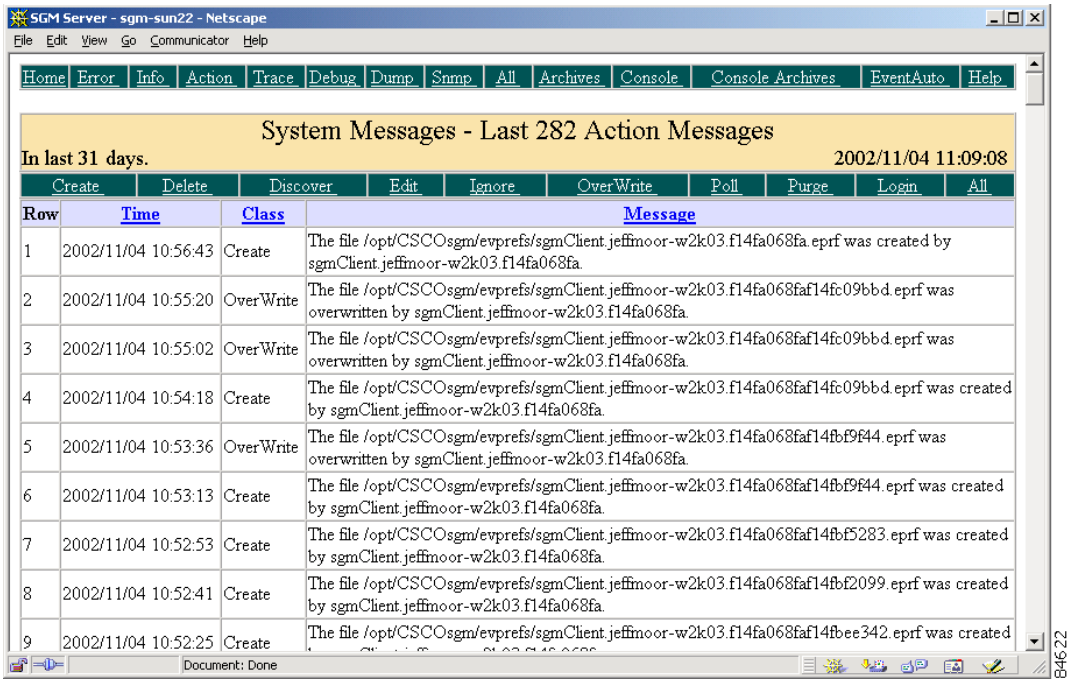
The System Messages - Last Action Messages page displays action messages stored in the SGM system log. These messages can be useful when diagnosing and correcting SGM operational problems, and when monitoring audit trails of user actions.

To access the System Messages - Last Action Messages page, use one of the following procedures:

- Select **Web Links>User Audit>User Actions** from the SGM Main Menu.
- Select **User Actions** from the SGM Server Home Page.
- Select **Action** from the menu bar of any SGM System Messages Web page.

SGM displays the System Messages - Last Action Messages page (Figure 7-10).

Figure 7-10 System Messages - Last Action Messages Page



The Last Action Messages table provides the following information for each message:

- **Period (in header)**—Collection period of the table, such as **Since Server Restart**.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Row—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged.
- **Class—**Class of the message. Possible classes are:
  - **Create**—Creation event, such as the creation of a seed file.
  - **Delete**—Deletion event, such as the deletion of a node or linkset.
  - **Discover**—Discovery event, such as Discovery beginning.
  - **Edit**—Edit event. A user has edited an event, linkset, or node.
  - **Ignore**—Ignore event. A user has flagged a link or linkset as **Ignored**.
  - **Login**—Login event. A user has logged in to SGM.
  - **LoginDisable**—LoginDisable event. SGM has disabled a user's User-Based Access authentication as a result of too many failed attempts to log in to SGM.
  - **LoginFail**—LoginFail event. An attempt by a user to log in to SGM has failed.
  - **OverWrite**—OverWrite event. An existing file, such as a seed file or route file, has been overwritten.
  - **Poll**—Poll event, such as an SNMP poll.
  - **Purge**—Purge event. A user has requested Discovery with **Delete Existing Data** selected, and SGM has deleted the existing SGM database.
- **Message—**Text of the message.

To sort the messages by time, class, or alphabetically by message text, click the **Time**, **Class**, or **Message** header.

By default, SGM displays action messages of all classes on the System Messages - Last Action Messages page. However, menu options are provided that enable you to display only messages of a specific class on the page. To display only messages of a specific class, select one of the following options:

- **All**—Opens the System Messages - Last Action Messages Web page, which displays all action messages.
- **Create**—Opens the System Messages - Last Action - Create Messages Web page, which displays only Create action messages.
- **Delete**—Opens the System Messages - Last Action - Delete Messages Web page, which displays only Delete action messages.
- **Discover**—Opens the System Messages - Last Action - Discover Messages Web page, which displays only Discover action messages.
- **Edit**—Opens the System Messages - Last Action - Edit Messages Web page, which displays only Edit action messages.
- **Ignore**—Opens the System Messages - Last Action - Ignore Messages Web page, which displays only Ignore action messages.
- **Login**—Opens the System Messages - Last Action - Login Messages Web page, which displays only Login action messages.
- **OverWrite**—Opens the System Messages - Last Action - OverWrite Messages Web page, which displays only OverWrite action messages.
- **Poll**—Opens the System Messages - Last Action - Poll Messages Web page, which displays only Poll action messages.
- **Purge**—Opens the System Messages - Last Action - Purge Messages Web page, which displays only Purge action messages.

Viewing SGM Trace Messages

The System Messages - Last Trace Messages page displays trace messages stored in the SGM system log. These messages can be useful when diagnosing and correcting SGM operational problems.

To access the System Messages - Last Trace Messages page, select **Trace** from the menu bar of any SGM System Messages Web page.

The Last Trace Messages table provides the following information for each message:

- **Period (in header)**—Collection period of the table, such as **Since Server Restart**.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Index—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged.
- **Source—**Source for the message, with the format *process.host.id*, where:
  - *process* is the process that logged the message.
  - *host* is the host name of the process that logged the message.
  - *id* is an SGM ID that uniquely identifies the process that logged the message, in the event that there are two or more clients running on the same device, connected to the same SGM server.
- **Task—**Task, or thread, that logged the message.
- **Message—**Text of the message.

Viewing SGM Debug Messages

The System Messages - Last Debug Messages page displays debug messages stored in the SGM system log. These messages can be useful when diagnosing and correcting SGM operational problems.

To access the System Messages - Last Debug Messages page, select **Debug** from the menu bar of any SGM System Messages Web page.

Note The **Debug** option is displayed only when enabled at the request of Cisco TAC.

The Last Debug Messages table provides the following information for each message:

- **Period (in header)**—Collection period of the table, such as **Since Server Restart**.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Index—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged.
- **Source—**Source for the message, with the format *process.host.id*, where:
  - *process* is the process that logged the message.
  - *host* is the host name of the process that logged the message.
  - *id* is an SGM ID that uniquely identifies the process that logged the message, in the event that there are two or more clients running on the same device, connected to the same SGM server.
- **Task—**Task, or thread, that logged the message.
- **Message—**Text of the message.

Viewing SGM Dump Messages

The System Messages - Last Dump Messages page displays dump messages stored in the SGM system log. These messages can be useful when diagnosing and correcting SGM operational problems.

To access the System Messages - Last Dump Messages page, select **Dump** from the menu bar of any SGM System Messages Web page.

Note The **Dump** option is displayed only when enabled at the request of Cisco TAC.

The Last Dump Messages table provides the following information for each message:

- **Period (in header)**—Collection period of the table, such as **Since Server Restart**.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Index—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged.
- **Source—**Source for the message, with the format *process.host.id*, where:
  - *process* is the process that logged the message.
  - *host* is the host name of the process that logged the message.
  - *id* is an SGM ID that uniquely identifies the process that logged the message, in the event that there are two or more clients running on the same device, connected to the same SGM server.
- **Task—**Task, or thread, that logged the message.
- **Message—**Text of the message.

Viewing SGM SNMP Messages

The System Messages - Last SNMP Messages page displays SNMP messages stored in the SGM system log. These messages can be useful when diagnosing and correcting SGM operational problems.

Note These are not SNMP trap messages. These are debugging messages from internal, low-level SNMP encoding and decoding routines.

To access the System Messages - Last SNMP Messages page, select **SNMP** from the menu bar of any SGM System Messages Web page.

Note The **SNMP** option is displayed only when enabled at the request of Cisco TAC.

The Last SNMP Messages table provides the following information for each message:

- **Period (in header)**—Collection period of the table, such as **Since Server Restart**.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Index—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged.
- **Source—**Source for the message, with the format *process.host.id*, where:
  - *process* is the process that logged the message.
  - *host* is the host name of the process that logged the message.
  - *id* is an SGM ID that uniquely identifies the process that logged the message, in the event that there are two or more clients running on the same device, connected to the same SGM server.
- **Task—**Task, or thread, that logged the message.
- **Message—**Text of the message.

Viewing All Current SGM Messages

The System Messages - Last All Messages page displays all current messages in the SGM system log.

To access the System Messages - Last All Messages page, select **All Messages**.

The Last All Messages table provides the following information for each message:

- **Period (in header)**—Collection period of the table, such as **Since Server Restart**.
- **Timestamp (in header)**—Date and time the information on the page was last updated by SGM.
- **Index—**Message number, assigned to the message by SGM.
- **Time—**Date and time the message was logged.
- **Type**—Type of message. Possible types are:
  - **Action**
  - **Debug**
  - **Dump**
  - **Error**
  - **Info**
  - **SNMP**
  - **Trace**
- **Source—**Source for the message, with the format *process.host.id*, where:
  - *process* is the process that logged the message.
  - *host* is the host name of the process that logged the message.
  - *id* is an SGM ID that uniquely identifies the process that logged the message, in the event that there are two or more clients running on the same device, connected to the same SGM server.
- **Task—**Task, or thread, that logged the message.
- **Message—**Text of the message.

Viewing All Archived SGM Messages

The System Message Archives - All Messages page displays all archived messages in the SGM system logs, including error messages, informational messages, trace messages, debug messages, dump messages, and SNMP messages.

To access the System Message Archives - All Messages page, use one of the following procedures:

- Select **System Message Archives** from the SGM Server Home Page.
- Select **Archives** from the menu bar of any SGM System Messages Web page.

On the System Message Archives - All Messages page, messages are archived by time stamp. Each archived file contains all SGM system messages for a single session for the server to which you are connected, and which is currently running the SGM server. (If you restart the server, SGM creates a new file.)

To view archived messages, click a time stamp. SGM displays the archived messages.

Viewing the SGM System Console Log

The SGM System Console Log page displays the contents of the SGM system console log file for the server to which you are connected, and which is currently running the SGM server. The console log file contains unexpected error and warning messages from the SGM server, such as those that might occur if the SGM server cannot start.

To access the SGM System Console Log page, use one of the following procedures:

- Select **System Console Log** from the SGM Server Home Page.
- Select **Console** from the menu bar of any SGM System Messages Web page.

Viewing All Archived SGM System Console Log Messages

The Console Archives - All Messages page displays all archived SGM system console log messages for the server to which you are connected, and which is currently running the SGM server. The archived console logs contain unexpected error and warning messages from the SGM server, such as those that might occur if the SGM server cannot start.

To access the Console Archives - All Messages page, select **Console Archives** from the menu bar of any SGM System Messages Web page.

On the Console Archives - All Messages page, messages are archived by time stamp. Each archived file contains all SGM system console log messages for a single session for the server to which you are connected, and which is currently running the SGM server. (If you restart the server, SGM creates a new file.)

To view archived messages, click a time stamp. SGM displays the archived messages.

Viewing the SGM System Command Log

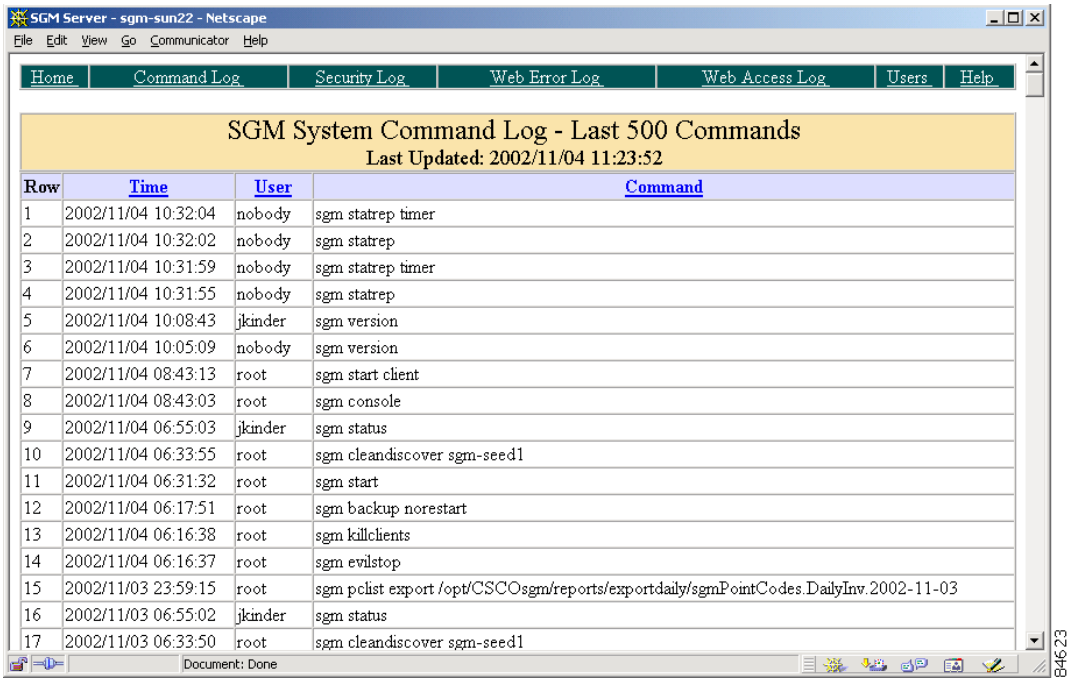
The SGM System Command Log - Last Commands page displays the contents of the SGM system command log file for the server to which you are connected, and which is currently running the SGM server. The system command log lists all **sgm** commands that have been entered for the SGM server, the time each command was entered, and the user who entered the command.

To access the SGM System Command Log - Last Commands page, use one of the following procedures:

- Select **Web Links > User Audit > Command Log** from the SGM Main Menu.
- Select **System Command Log** from the SGM Server Home Page.
- Select **Command Log** from the menu bar of any SGM System Messages Web page.

SGM displays the SGM System Command Log - Last Commands page (Figure 7-11).

Figure 7-11 SGM Command Page - Last Commands Page



The Last Commands table provides the following information for each command:

- **Last Updated (in header)**—Date and time the information on the page was last updated by SGM.
- **Row—**Command number, assigned to the command by SGM.
- **Time—**Date and time the command was entered.
- **User**—User who entered the command.
- **Command—**Text of the command.

To sort the commands by time, by user, or alphabetically by command text, click the **Time**, **User**, or **Command** header.

Viewing the SGM System Event Automation Log

The SGM System Event Automation Log page displays the contents of the SGM system event automation log file for the server to which you are connected, and which is currently running the SGM server. The system event automation log lists all messages generated by scripts launched by event automation.

The default path and filename for the system event automation log file is */opt/CSCOsgm/logs/eventAutomationLog.txt*. If you installed SGM in a directory other than */opt*, then the system event automation log file is located in that directory.

To access the SGM System Event Automation Log page, use one of the following procedures:

- Select **System Event Automation Log** from the SGM Server Home Page.
- Select **EventAuto** from the menu bar of any SGM System Messages Web page.

Viewing the SGM System Security Log

The SGM System Security Log - Last Entries page displays the contents of the SGM system security log file for the server to which you are connected, and which is currently running the SGM server. The system security log lists all SGM security events that have occurred for the SGM server, the time each event occurred, the user and command that triggered the event, and the text of any associated message.

The default path and filename for the system security log file is */opt/CSCOsgm/logs/sgmSecurityLog.txt*. If you installed SGM in a directory other than */opt*, then the system security log file is located in that directory.

To access the SGM System Security Log - Last Entries page, use one of the following procedures:

- Select **Web Links > User Audit > Security Log** from the SGM Main Menu.
- Select **System Security Log** from the SGM Server Home Page.
- Select **Security Log** from the menu bar of any SGM System Messages Web page.

The Last Security Entries table provides the following information for each entry:

- **Last Updated (in header)**—Date and time the information on the page was last updated by SGM.
- **Row—**Entry number, assigned to the entry by SGM.
- **Time—**Date and time the security event occurred.
- **User**—User who triggered the security event.
- **Message—**Text of the security event message.
- **Command—**Text of the command that triggered the security event.

To sort the entries by time, user, or alphabetically by message or command text, click the **Time**, **User**, **Message**, or **Command** header.

Viewing the SGM System Web Server Error Log

The SGM System Web Server Error Log - Last Messages page displays the contents of the SGM system Web server error log file for the server to which you are connected, and which is currently running the SGM server. The system Web server error log lists all SGM system Web error messages that have been logged for the SGM Web server.

To access the SGM System Web Server Error Log - Last Messages page, select **Web Server Errors** from the SGM Server Home Page, or enter the **sgm weberrorlog** command. (You must be logged in as the root user or as a super user to use the **sgm weberrorlog** command.)

The SGM System Web Server Error Log - Last Messages page provides the following information:

- **Last Updated (in header)**—Date and time the information on the page was last updated by SGM.
- **Row**—Message number, assigned to the message by SGM.
- **Message**—Text of the Web server error message.

Viewing the SGM System Web Access Log

The SGM System Web Access Log - Last Messages page displays the contents of the SGM system Web access log file for the server to which you are connected, and which is currently running the SGM server. The system Web access log lists all SGM system Web access messages that have been logged for the SGM server. This provides an audit trail of all access to the SGM server via the Web interface.

To access the SGM System Web Access Log - Last Messages page, select **Web Access Log** from the SGM Server Home Page, or enter the **sgm webaccesslog** command. (You must be logged in as the root user or as a super user to use the **sgm webaccesslog** command.)

The SGM System Web Access Log - Last Messages page provides the following information:

- **Last Updated (in header)**—Date and time the information on the page was last updated by SGM.
- **Row**—Message number, assigned to the message by SGM.
- **Message**—Text of the Web error message.

Viewing System Status Information for SGM

You can view the following SGM system status information from the SGM Server Home Page:

- Viewing Status Information for SGM, page 7-75
- Viewing Version Information for SGM, page 7-76
- Viewing SGM Client Information, page 7-76
- Viewing SGM User Account Information, page 7-76
- Viewing the Troubleshooting Log for SGM (Solaris Only), page 7-78

Viewing Status Information for SGM

The SGM System Status page displays the status of all SGM servers, local clients, and processes. To access the SGM System Status page, select **System Status**. (SGM might take a few seconds to display this page.)

Viewing Version Information for SGM

The SGM System Versions page displays version information for all SGM servers, clients, and processes. To access the SGM System Versions page, select **System Versions**. (SGM might take a few seconds to display this page.)

Viewing SGM Client Information

The SGM System Connected Clients page lists all SGM clients that are currently connected to the SGM server. It also lists all Solaris users that are logged in to the SGM server.

To access the SGM System Connected Clients page, use one of the following procedures:

- Select **Web Links > User Audit > Connected Clients** from the SGM Main Menu.
- Select **Connected Clients** from the SGM Server Home Page.
- Select **Clients** from the menu bar of any SGM System Status Web page.

Viewing SGM User Account Information

The SGM User Accounts page displays information about all user accounts that have been defined for the SGM server. If no user accounts have been defined, SGM displays the message, "User Database is Empty."

To access the SGM User Accounts page, use one of the following procedures:

- Select **Web Links > User Audit > User Accounts** from the SGM Main Menu.
- Select **System User Accounts** from the SGM Server Home Page.
- Select **Users** from the menu bar of any SGM System Status Web page.

The SGM User Accounts page provides the following information:

- **Server Name (in header)**—Name of the SGM server for which user accounts are being displayed.
- **User**—SGM user for whom a User-Based Access account has been set up.
- **Last Login**—Date and time the user last logged in to SGM.

- **Level Name**—Authentication level for the user. Valid levels are:
  - Basic User
  - Power User
  - Network Operator
  - Network Administrator
  - System Administrator
- **Level Number**—Authentication level for the user, expressed as a number. Valid levels are:
  - **1**—Basic User
  - **2**—Power User
  - **3**—Network Operator
  - **4**—Network Administrator
  - **5**—System Administrator
- **Status**—Current status of the user's account. Valid status settings are:
  - **Account Enabled**—The account has been enabled and is functioning normally.
  - **Account Disabled**—The account has been disabled for one of the following reasons:

    – A System Administrator disabled the account. See the descriptions of the **sgm disablepass** and **sgm disableuser** commands in the "SGM Command Reference" for more information.

    – SGM disabled the account as a result of too many failed attempts to log in using the account. See the description of the **sgm badlogindisable** command in the "SGM Command Reference" for more information.

    – SGM disabled the account because it was inactive for too many days. See the description of the **sgm inactiveuserdays** command in the "SGM Command Reference" for more information.

To sort the SGM User Accounts page based on the contents of any column, click the column header.

Viewing the Troubleshooting Log for SGM (Solaris Only)

The SGM System Troubleshooting page displays the troubleshooting information that is stored in the */opt/CSCOsgm/tmp/cisco_sgm_tshoot.log* file on the SGM server. This log, which is updated each time the SGM System Troubleshooting page is accessed or the **sgm tac** command is run, contains information that might be requested by Cisco customer support personnel.

To view troubleshooting information for SGM, select **System Troubleshooting**.

Note SGM might take several minutes to create and display the troubleshooting log, and the resulting log might be several MB, depending on the size of the network and system logs.

Viewing System Data Files for SGM

You can view the following SGM system data files from the SGM Server Home Page:

- **ITP SNMP MIBs**—Displays a list of the MIBs on the server to which you are connected, and which is currently running the SGM server. To access the ITP SNMP MIBs page, select **ITP MIBs** from the menu bar of any SGM System Files Web Page.
- **SGM System Files - Discovery Seeds**—Displays a list of the seed files that have been created on this SGM server. To access the SGM System Files - Discovery Seeds page, select **Discovery Seeds** from the SGM Server Home Page.
- **SGM System Files - GTT**—Displays a list of the GTT files that have been created on this SGM server. To access the SGM System Files - GTT page, select **Global Title Tables** from the SGM Server Home Page. Click a GTT file name to view its contents.
- **SGM System Files - Network Views**—Displays a list of the network view files that have been created on this SGM server. To access the SGM System Files - Network Views page, select **Views** from the menu bar of any SGM System Files Web Page.

- **SGM System Files - Notes**—Displays a list of the note files that have been created on this SGM server. The notes are listed by the name of the node or linkset, or by the internal ID of the event. To access the SGM System Files - Notes page, select **Notes** from the SGM Server Home Page. Click a node name, linkset name, or event ID to view the contents of the note.
- **SGM System Files - Point Code Mappings**—Displays a list of point codes mapped to node names on this SGM server. To access the SGM System Files - Point Code Mappings page, select **Point Code Mappings** from the SGM Server Home Page.

  You can also view the SGM point code mappings file, *pcinfo.conf*, using the **sgm pcinfo view** command. To edit the file, use the **sgm pcinfo edit** command. See the "SGM Commands and Descriptions" section on page B-2 for more information on the use of these commands.
- **SGM System Files - Routes**—Displays a list of the route table files that have been created on this SGM server. To access the SGM System Files - Routes page, select **DPC Route Tables** from the SGM Server Home Page. Click a route table file name to view its contents.

  In the route table file, linksets are listed with the format **L***number***:***name*, where:

  - **L** indicates that the line is for a linkset.
  - *number* is the linkset number.
  - *name* is the name of the linkset.

  In the route table file, routes are listed with the format R*code*:*bits*:I*number*:*cost*:*qos*, where:

  - **R** indicates that the line is for a route.
  - *code* is the destination point code in hexadecimal format.
  - *bits* is the number of bits in the mask, in hexadecimal format. For example, e indicates that there are 14 bits in the mask (7.255.7 = 111.11111111.111).
  - **I** indicates the information for the route.
  - *number* is the linkset number to use, which matches one of the linkset numbers from the above list.

  - *cost* is the cost or priority of the route to the destination, relative to other routes. The valid costs range from 1 (lowest cost and highest priority) through 9 (highest cost and lowest priority).
  - *qos* is the quality of service (QoS) class of the route, as configured by the network administrator. A value of **ff** means the QoS is not set.

- **SGM System Files - Server Event Automation Sounds**—Displays a list of event automation sound files on this SGM server. To access the SGM System Files - Server Event Automation Sounds page, select **Sounds** from the menu bar of any SGM System Files Web Page.

Viewing System Information for SGM

You can view the following SGM system information from the SGM Server Home Page:

- **SGM Install Log**—Displays the contents of the SGM system installation log. The installation log contains messages and other information recorded during installation, which can be useful when troubleshooting problems. To access the SGM System Install Log page, select **System Install Log**.
- **SGM ITP IOS README**—Displays the versions of IOS with which SGM is compatible. To access the SGM System ITP IOS README page, select **System ITP IOS README** from the SGM Server Home Page.
- **SGM Process Services**—Displays the processes that are started and managed by the SGM Process Manager. To access the SGM System Process Services page, select **System Process Services**, or enter the **sgm services** command. (You must be logged in as the root user or as a super user to use the **sgm services** command.)
- **SGM README**—Contains late-breaking information about SGM that might not be found in the other product documentation. To access the SGM System README page, select **System README**.

- **SGM Root Variables**—Displays the contents of the */etc/CSCOsgm.sh* file, which determines the root location of the SGM server and client installation. To access the SGM System Root Variables page, select **System Root Variables**, or enter the **sgm rootvars** command.
- **SGM System Properties**—Displays SGM server and client properties that control various SGM configuration parameters. To access the SGM System Properties page, select **System Properties**.

Viewing the SGM Technical Documentation

From the SGM Server Home Page, you can view the following SGM technical documentation:

- To access the Cisco Signaling Gateway Manager Help System, select **Help Home Page**.
- To view Frequently Asked Questions (FAQs) about SGM, select **Frequently Asked Questions**.
- To view the entire SGM Installation Guide as a PDF file on the Web, select **Installation Guide**.
- To view the entire SGM User Guide as a PDF file on the Web, select **User Guide**.
- To view the entire SGM Release Notes as a PDF file on the Web, select **Release Notes**.
- To view help for SGM commands, select **Output of sgm help command** from the SGM Server Home Page.

Downloading the SGM Client from the Web

You can access the SGM client installation software for Linux, Solaris, and Windows from the SGM Server Home Page. This access is useful if you do not have the CD-ROM, or if you prefer to download the software using your Web browser. Once you have downloaded the SGM client installation software to your workstation, you must install the software on your local system.

For more information about installing the SGM client software using a Web server, see the "Installing SGM on Solaris" and "Installing SGM on Windows" chapters of the *Cisco Signaling Gateway Manager Installation Guide*.

- To access the SGM Client for Solaris page, select **Download Solaris Client**.
- To access the SGM Client for Windows page, select **Download Windows Client**.
- To access the SGM Client for Linux page, select **Download Linux Client**. (The SGM client for Linux is not a supported feature of SGM. Use it under advisement.)

Downloading the SGM Server's SSL Certificate from the Web

If you have implemented Secure Sockets Layer (SSL) support in your SGM system, you can download the SGM server's signed SSL certificate to all remote SGM clients that connect to the server using SSL.

To access the SGM Server SSL Certificate page, select **Server SSL Certificate** from the SGM Server Home Page.

For more information about downloading the certificate, or about enabling SSL in SGM, see the "Implementing SSL Support in SGM" section on page 4-24.

Accessing Software Updates and Additional Information

You can access the following additional information about SGM from the SGM Server Home Page:

- To read Cisco literature associated with SGM, including product data sheets, Q and As, and helpful presentations, select **SGM Home Page** from the SGM Server Home Page.
- To view information about SGM or any other Cisco product available on Cisco.com (also known as Cisco Connection Online), use one of the following procedures:
  - Select **Web Links>Cisco.com** from the SGM Main Menu.
  - Select **Cisco Home Page** from the SGM Server Home Page.
- To access the Network Management Software page, which includes the latest downloads for SGM, select **Network Management Software Center** from the SGM Server Home Page.
- To access software updates for SGM from Cisco.com for FTP, select **Engineering Software Updates**. The SGM Software Home page is displayed.

Displaying the Router Home Page

SGM enables you to display the home page of a selected router in a new Web browser window.

To view a router's home page, use one of the following procedures:

- Select a node, or a linkset associated with the node, in the Node, Linkset, or Topology window, then select **Web Links>Router Homepage** from the SGM Main Menu.
- Right-click a node in the Node or Topology window, then select **Web Links>Router Homepage** from the right-click menu.