Monitoring with the Multicast Manager Tool

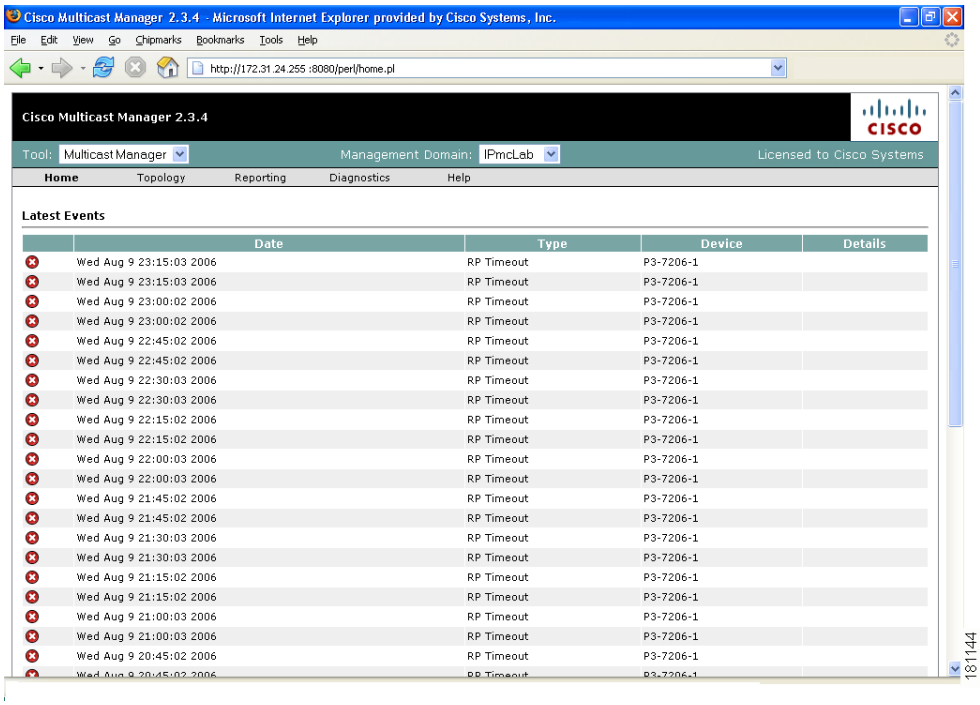
This chapter covers:

Viewing the Multicast Manager Home Page

When you log into the CMM, the Multicast Manager Home Page opens. To access this page from within the CMM, select the **Multicast Manager** tool, then select **Home**.

The **Home** page shows the last 20 events (see the "Latest Events" section on page 3-5).

Figure 3-1 Multicast Manager Home Page

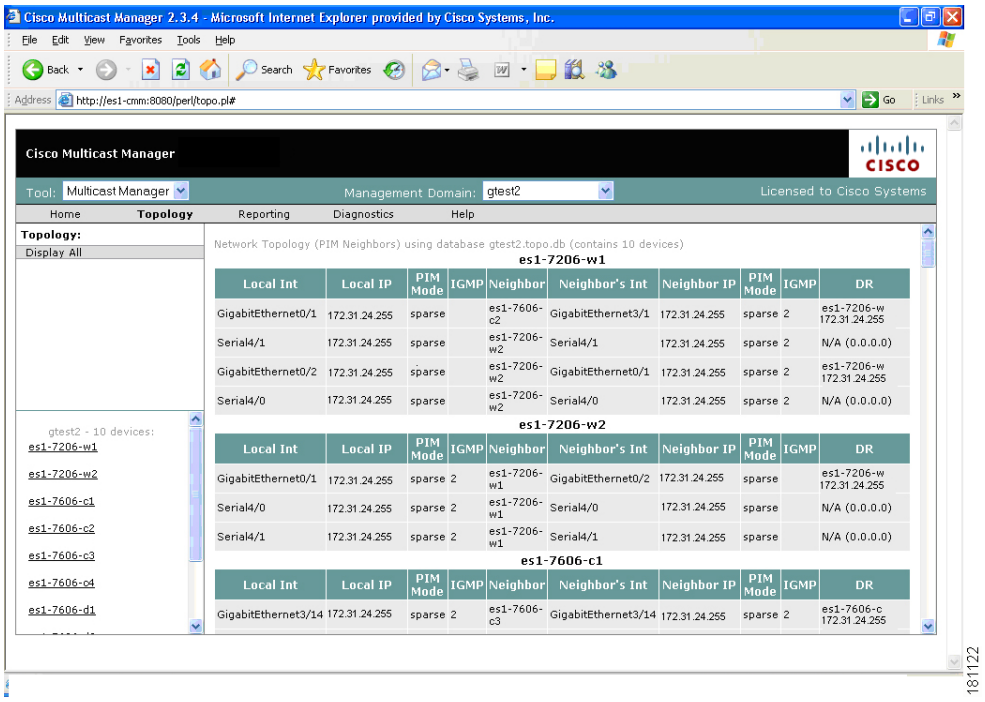


Viewing Topology

Using **Topology**, you can display routers and their multicast information in the database, on an individual basis, or by showing the complete database.

To see the complete database, select **Display All**. Router names appear at the top of each table.

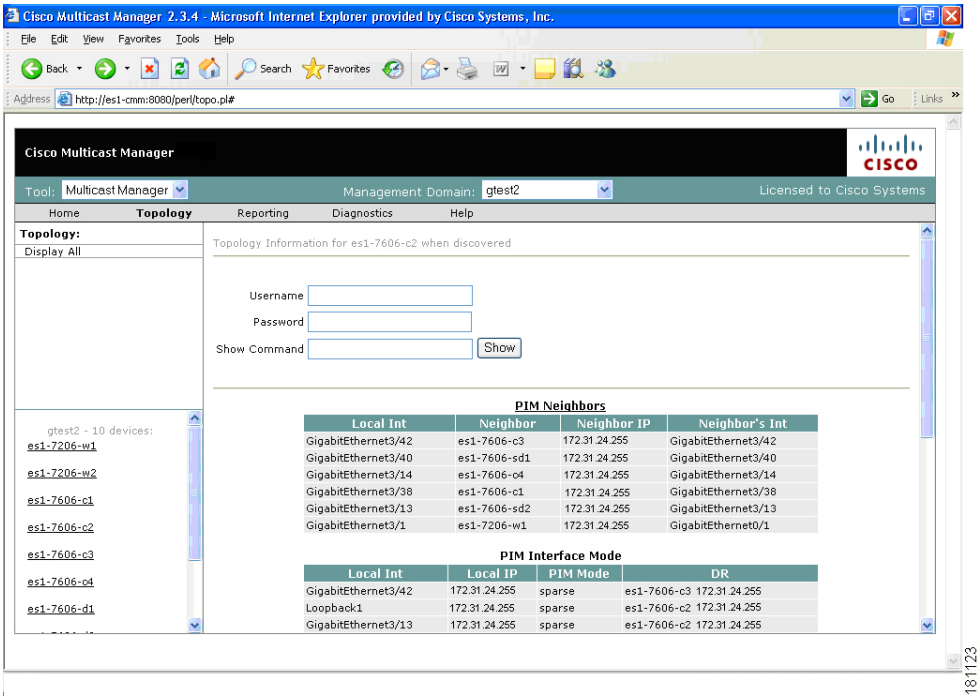
Figure 3-2 Topology Display All



Field	Description
Local Int	Interfaces running multicast.
Local IP	IP address of the interfaces.
PIM Mode	PIM Mode, can be sparse or dense.
IGMP	IGMP version.
Neighbor	PIM neighbor name.
Neighbor's INT	PIM neighbor's interface.
Neighbor IP	PIM neighbor's IP address.
PIM Mode	PIM neighbor's mode, can be sparse or dense.
IGMP	IGMP version of PIM neighbor.
DR	DR information.

To see topology for an individual router, click a router from the list pane at lower left.

Figure 3-3 Topology for an Individual Router

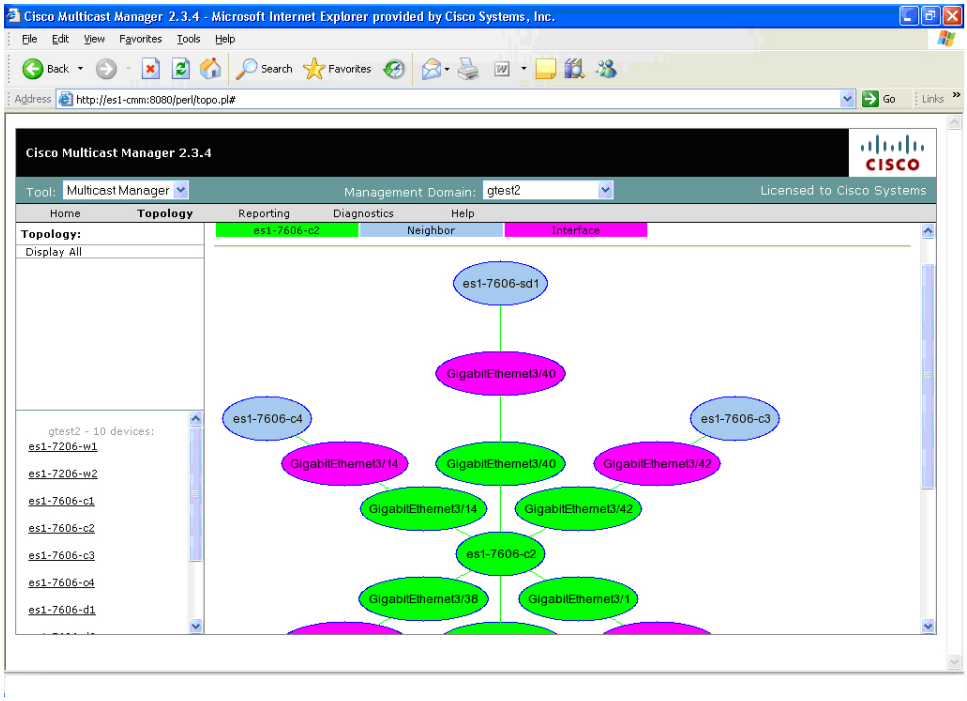


Field or Button	Description
Username	Enter your username.
Password	Enter your password.
Show Command	Enter any show commands on the router.
Show	Click **Show** to run the selected command.
PIM Neighbors	PIM neighbor name.

Note For details on the table columns within this window, see the descriptions for the Topology Display All window.

To see a topological display of the routers, select **PIM Neighbors**.

Figure 3-4 PIM Neighbors



On the PIM Neighbors page:

- Green = Router that was selected and its local interfaces
- Purple = PIM neighbor's interfaces of this router's PIM neighbors
- Blue = Names of the PIM neighbors of the selected router

Managing Reports

To start managing reports, within the **Multicast Manager** tool, click on **Reporting**.

Within Reporting, you can view:

- A record of the latest SNMP traps sent
- Historical graphs or trends
- Routers in the database IOS versions

Reporting Options
Latest Events, page 3-5
RP Polling Report, page 3-5
RP Group Threshold Report, page 3-6
RPF Failures, page 3-7
Group Gone Report, page 3-8
S,G Threshold Report, page 3-8
Layer 2 PPS Threshold Report, page 3-9

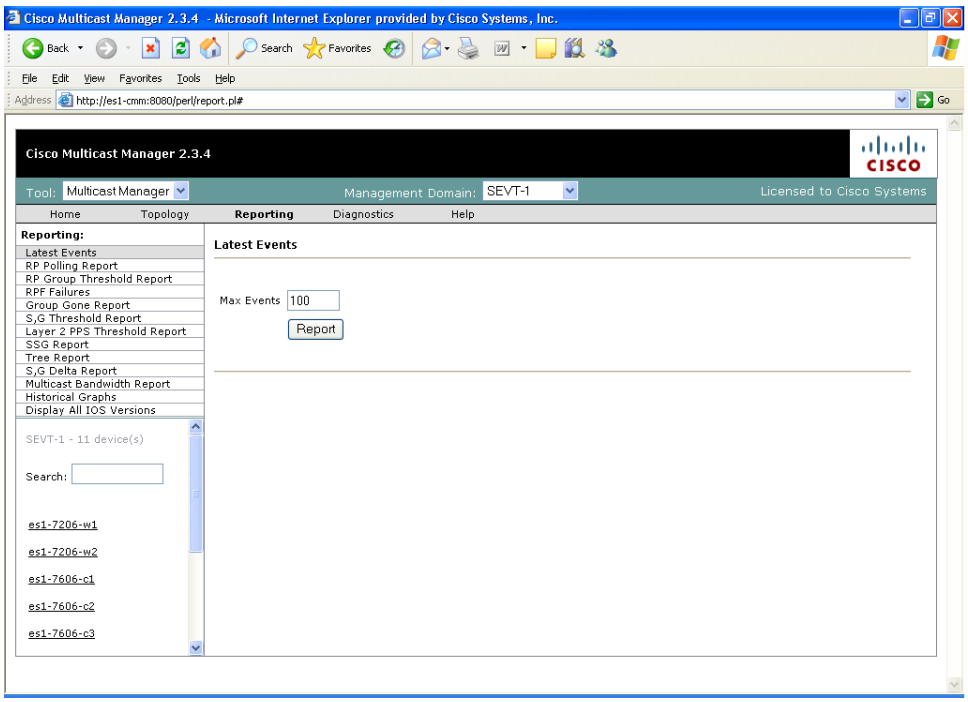
Reporting Options
SSG Report, page 3-10
Tree Report, page 3-11
S,G Delta Report, page 3-13
Multicast Bandwidth Report, page 3-14
Historical Graphs, page 3-15
Display All IOS Versions, page 3-16

Note The information shown for each type of report, with the exception of Historical Graphs, spans only the previous 24 hours. There may be more information available in the log file. However, it is recommended that the events.log file be rotated every 24 to 48 hours, depending on event activity.

Latest Events

Using the **Latest Events** page, you can set a configurable amount of the latest events generated by the CMM. Clicking **Report** lists the traps in time order.

Figure 3-5 Latest Events



RP Polling Report

Using the **RP Polling Report**, you can monitor:

- All leaves and joins for the selected RP (if the Enable RP Add/Delete Traps option is selected, see the "RP Polling" section on page 2-17).
- If the selected RP becomes unavailable.
- Any rogue source or group that joins the selected RP.

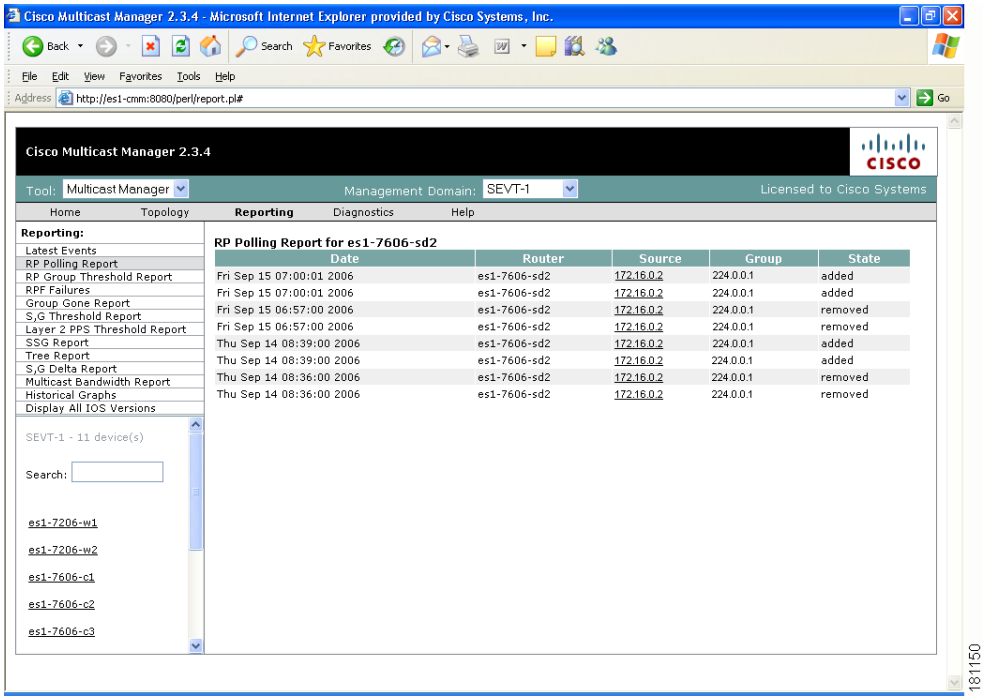
To generate an RP Polling report:

Step 1 Select an RP from the list.

Step 2 You can specify the maximum number of events to display.

Step 3 Click **Report**. The report contains any events that have occurred in the last 24 hours.

Figure 3-6 RP Polling Report



RP Group Threshold Report

Using the **RP Group Threshold Report**, you can monitor a list of RPs that have exceeded their active number of groups limit.

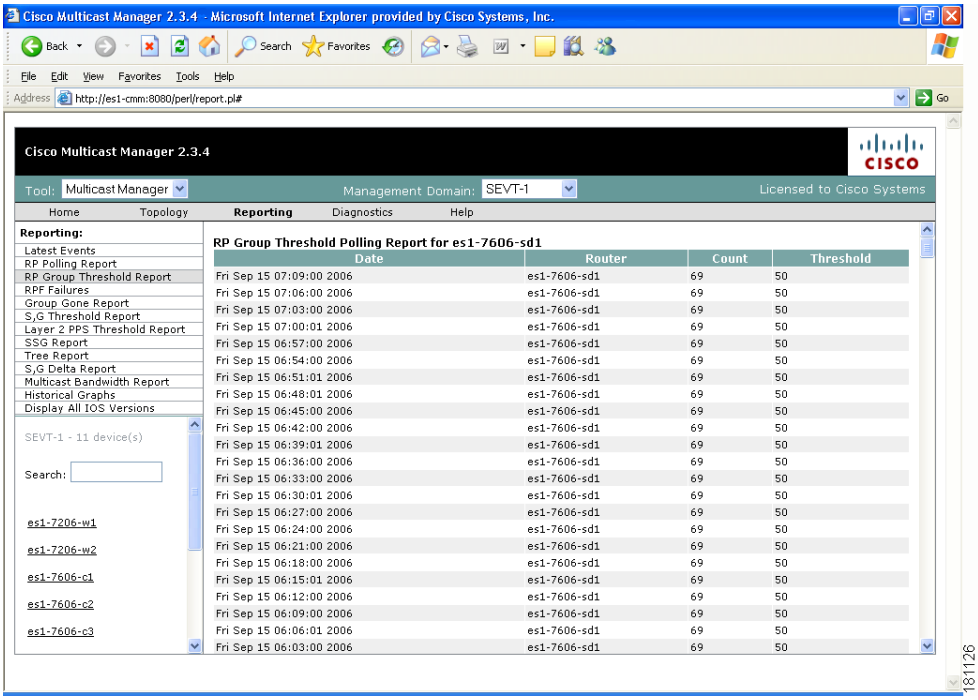
To generate an RP Group Threshold report:

Step 1 Select an RP from the list.

Step 2 You can specify the maximum number of events to display.

Step 3 Click **Report**. The report contains any events that have occurred in the last 24 hours.

Figure 3-7 RP Group Threshold Polling Report



RPF Failures

Using the **RPF Failures Report**, you can monitor all routers that are experiencing RPF failures above the configured threshold for the configured sources and groups.

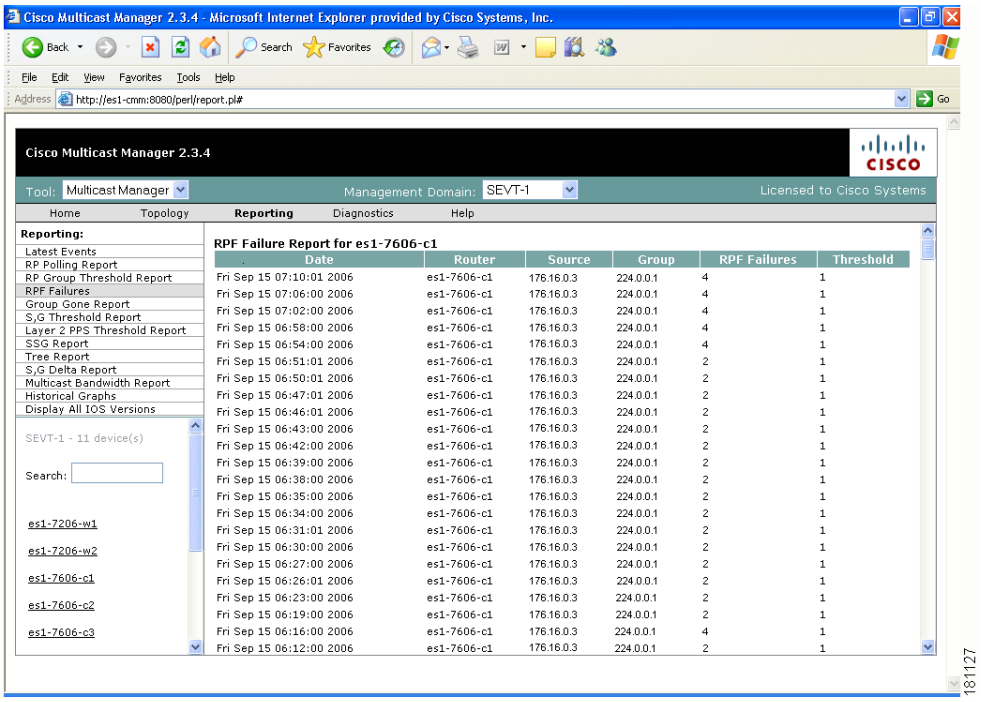
To generate an RPF Failures report:

Step 1 Select an RP from the list.

Step 2 You can specify the maximum number of events to display.

Step 3 Click **Report**. The report contains any events that have occurred in the last 24 hours.

Figure 3-8 RPF Failures Report



Group Gone Report

The **Group Gone Report** is currently unsupported. Functionality in this page has moved to the **S,G Polling Report**.

S,G Threshold Report

Using the **S,G Threshold Report**, you can monitor every source and group that has exceeded its configured threshold.

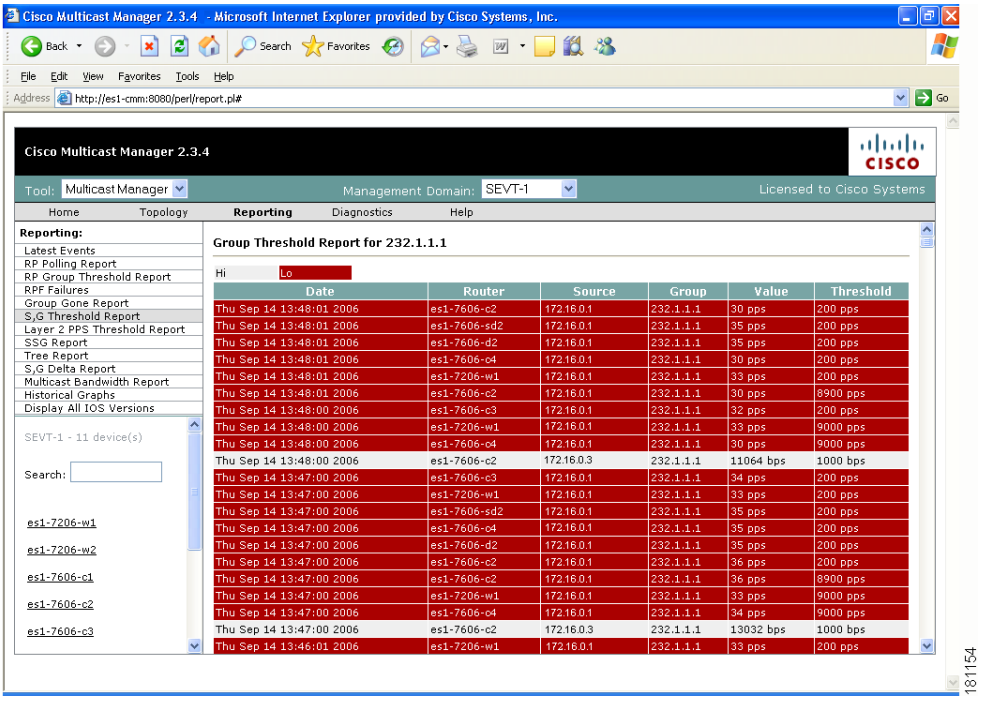
To generate an S,G Threshold report:

Step 1 Select a group from the list.

Step 2 You can specify the maximum number of events to display.

Step 3 Click **Report**. The report contains any events that have occurred in the last 24 hours, and shows pps and bps.

Figure 3-9 S,G Threshold Report



Layer 2 PPS Threshold Report

Using the **Layer 2 PPS Threshold Report**, you can monitor all Layer 2 ports that have exceeded their configured thresholds.

To generate a Layer 2 PPS Threshold Report:

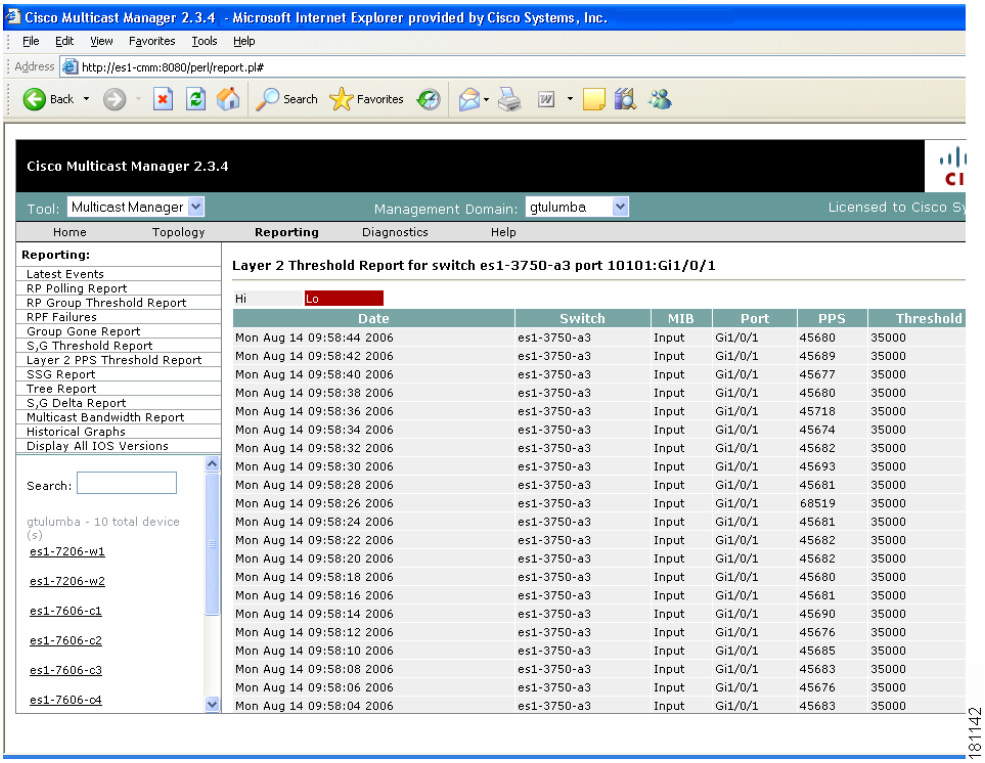
Step 1 Select a switch from the list.

Step 2 Select a port from the list.

Step 3 Click **Select**. The report contains any events that have occurred in the last 24 hours.

Note The report is for inbound and outbound traffic on the port.

Figure 3-10 Layer 2 PPS Threshold Report



SSG Report

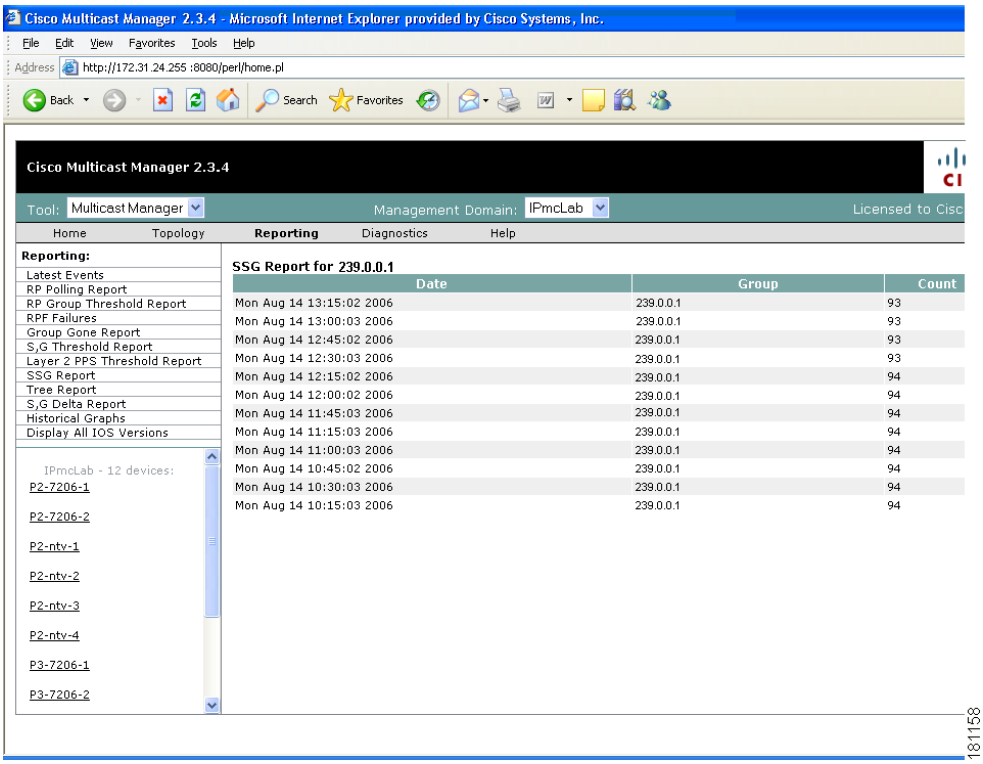
Using the **SSG Report**, you can display information about groups that have more than one sender.

To generate an SSG Report:

Step 1 Enter the multicast group address.

Step 2 Click **Report**. The report contains any events that have occurred in the last 24 hours. The count indicates the number of sources sending to the group.

Figure 3-11 SSG Report



Tree Report

Using the **Multicast Tree Report**, you can draw and save multicast trees (called baselines). You can then set up the CMM to draw trees that have been saved in the background, and report any changes. (Only changes to Layer 3 devices are reported.)

Note The drawing and saving of trees is covered in Show All Groups, page 4-1.

If a multicast tree you are monitoring changes, a trap is generated. You can then view the baseline and the changed tree. Changes are highlighted in the text and also in the drawing.

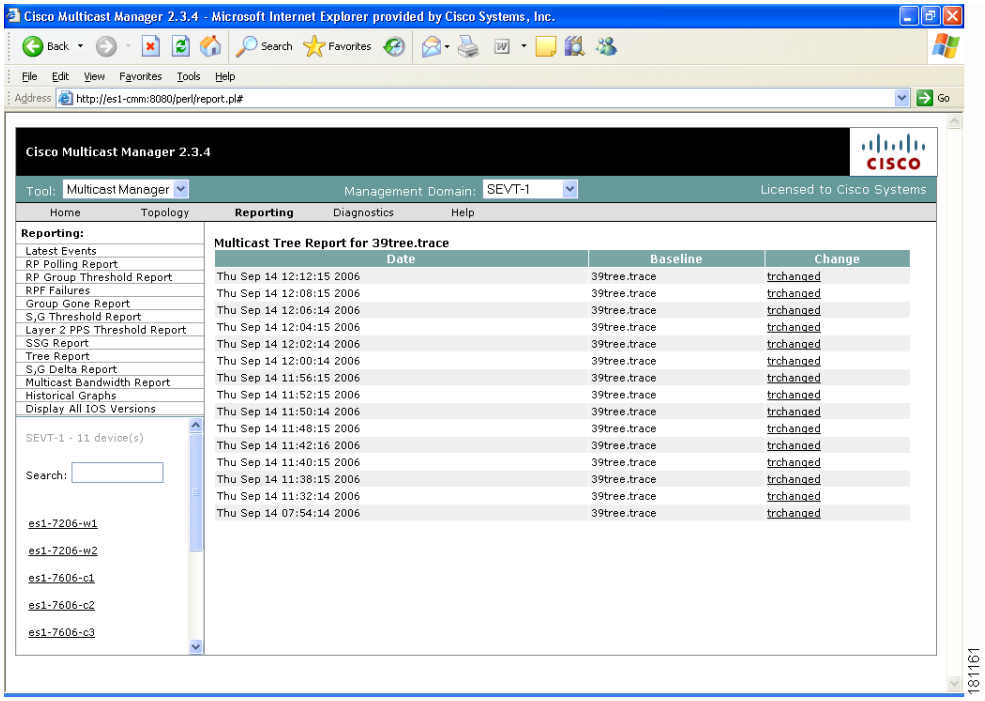
To generate a Multicast Tree Report:

Step 1 Select a baseline (multicast tree) from the list.

Step 2 You can specify the maximum number of events to display.

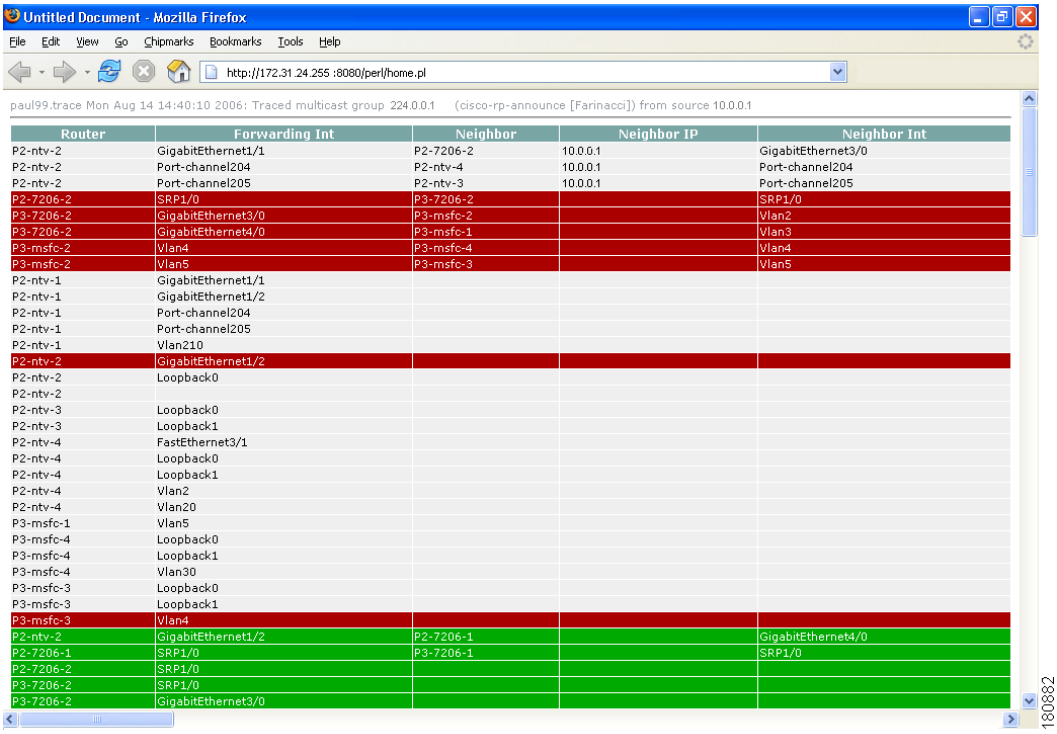
Step 3 Click **Select**. The report contains any events that have occurred in the last 24 hours.

Figure 3-12 Tree Report



Selecting “trchanged” in the third column in the report will graphically show the baseline, along with the changed tree. Changes to the tree are highlighted in the table at the top as shown in the figure. The baseline and the current tree are also shown graphically.

Figure 3-13 Tree Report Page—trchanged



S,G Delta Report

Using the **Multicast S,G Delta Report**, you can view information about PPS rate deviation on multicast trees.

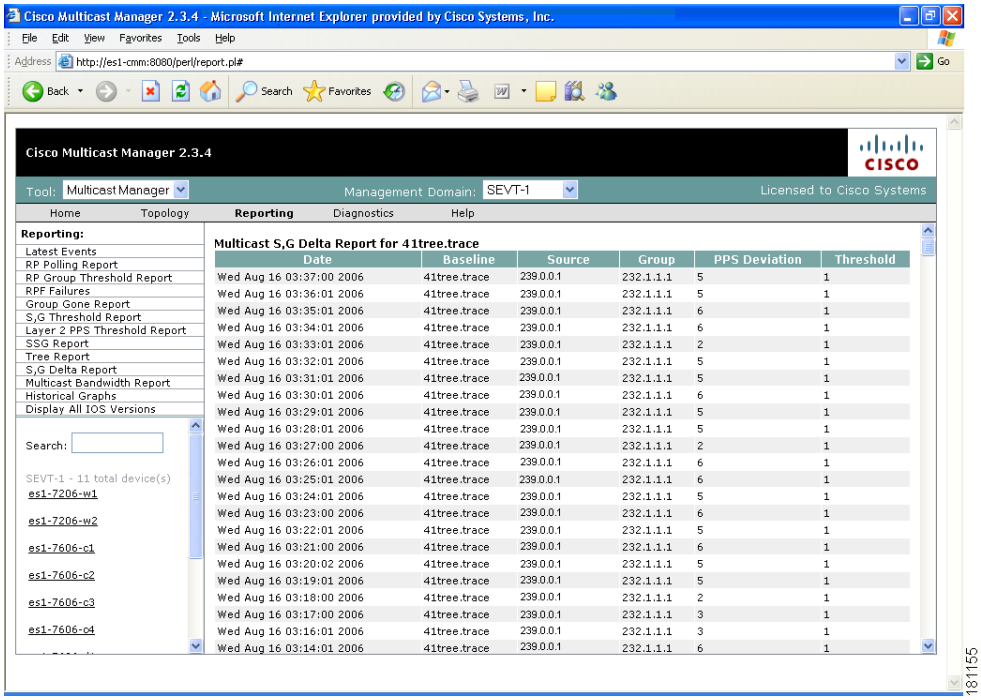
To generate a Multicast S,G Delta Report:

Step 1 Select a baseline (multicast tree) from the list.

Step 2 You can specify the maximum number of events to display.

Step 3 Click **Select**. The report contains any events that have occurred in the last 24 hours.

Figure 3-14 Multicast S,G Delta Report



Multicast Bandwidth Report

To generate a report for a router interface that has exceeded its multicast bandwidth thresholds:

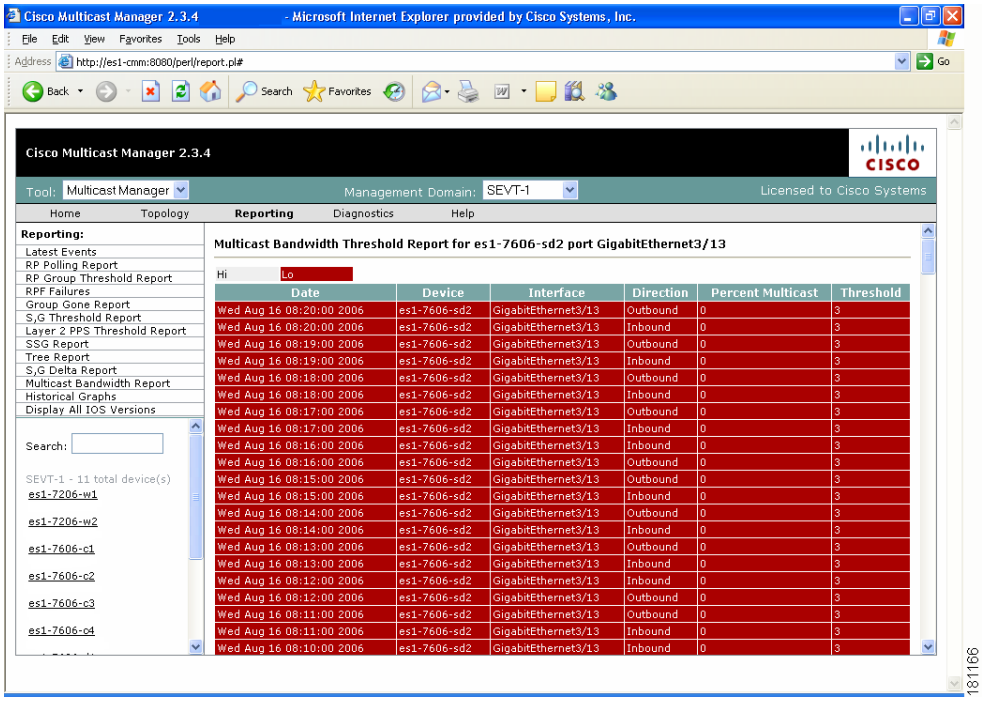
Step 1 Select the device.

Step 2 Select the port.

Step 3 Select the maximum number of events.

Step 4 Click **Report**.

Figure 3-15 Multicast Bandwidth Threshold Report



Historical Graphs

Using **Historical Graphs**, you can view historical data in a graph format. Historical data is collected when you start to monitor any of the following:

- Source and group activity in a router
- Multicast packets inbound or outbound of a Layer 2 port
- Source and group packet deviations on baseline multicast trees.

To view Historical Graphs:

Step 1 Select a **Graph Type** from the list:

- SG Delta PPS
- SG PPS
- SG BPS
- Switch Port PPS

Step 2 Select a **Time Range**:

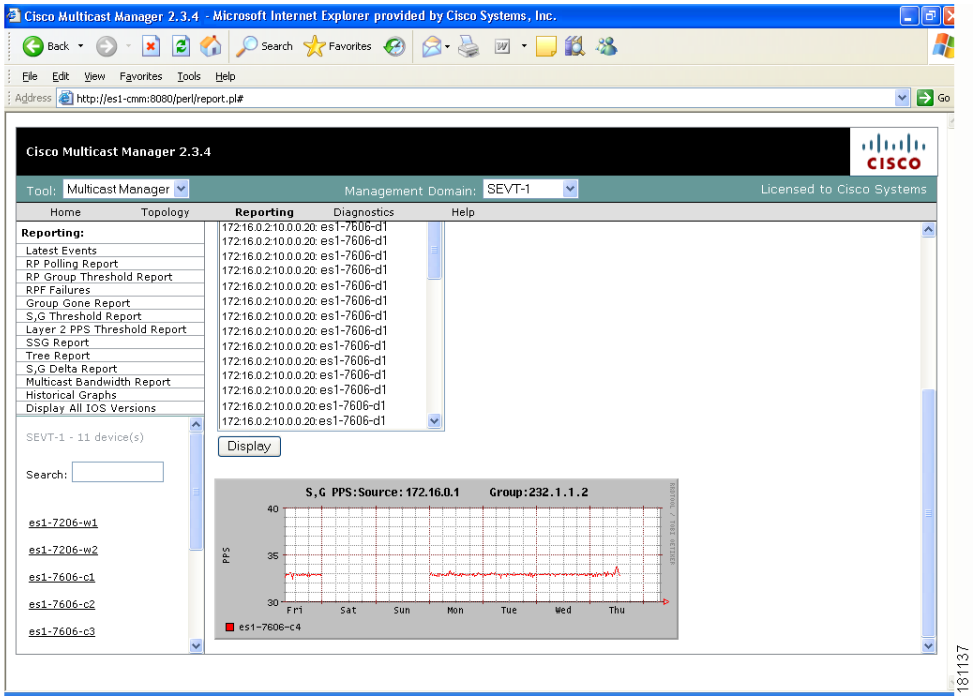
- User Specified
- Hour
- Day
- Week
- Month

Then select a **Start** and **End** range.

Step 3 A list of available reports appears. Highlight the appropriate report(s) and click **Display**. You can select up to 3 reports to display on the graph. Data stored for trending purposes is kept for up to 18 months.

Note Data must be collected to generate a report. If you have selected the correct Graph Type, and you do not see any entries, ensure that data is being collected (see Top Talkers, page 4-16).

Figure 3-16 Historical Graphs



Display All IOS Versions

Using the IOS Version Info page, you can view the IOS version of all discovered routers in the current domain. You can sort the table by device, IP address, IOS version, or model by selecting the corresponding column heading.

Figure 3-17 IOS Version Info