CA Spectrum® Multicast Manager

User Guide

r9.2

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA Spectrum Multicast Manager

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA Technologies product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introducing Multicast Manager

This section contains the following topics:

Overview

Multicast Manager lets you manage multicast traffic within your network environment. This includes the identification and monitoring of all multicast groups, sources, receivers, and other critical sources like rendezvous point (RP) routers.

Multicast Manager discovers and models Cisco and Juniper devices that support Multicast traffic. Once these devices are discovered, Multicast Manager provides several views which let you monitor the connectivity and performance of these Multicast elements. These views offer details relating to Multicast groups, sources, receivers, routers, and RPs and their relationships to each other.

The information provided in the Multicast Manager views makes troubleshooting Multicast-related outages much more efficient. You can isolate a problem quickly because you can determine the group a receiver belongs to, the RP of the group, the source for the group, the routers and interfaces that a group uses, and the configuration and bandwidth limits of these interfaces. Based on this information, you can prioritize your troubleshooting efforts should multiple problems occur.

If you purchase a multicast service or a data feed from an external service and you do not have access to the source to obtain its status, Multicast Manager provides you with the ability to create a proxy to the source or you can configure Multicast Manager to exclude the unmanageable source's status in group condition calculation.

More information:

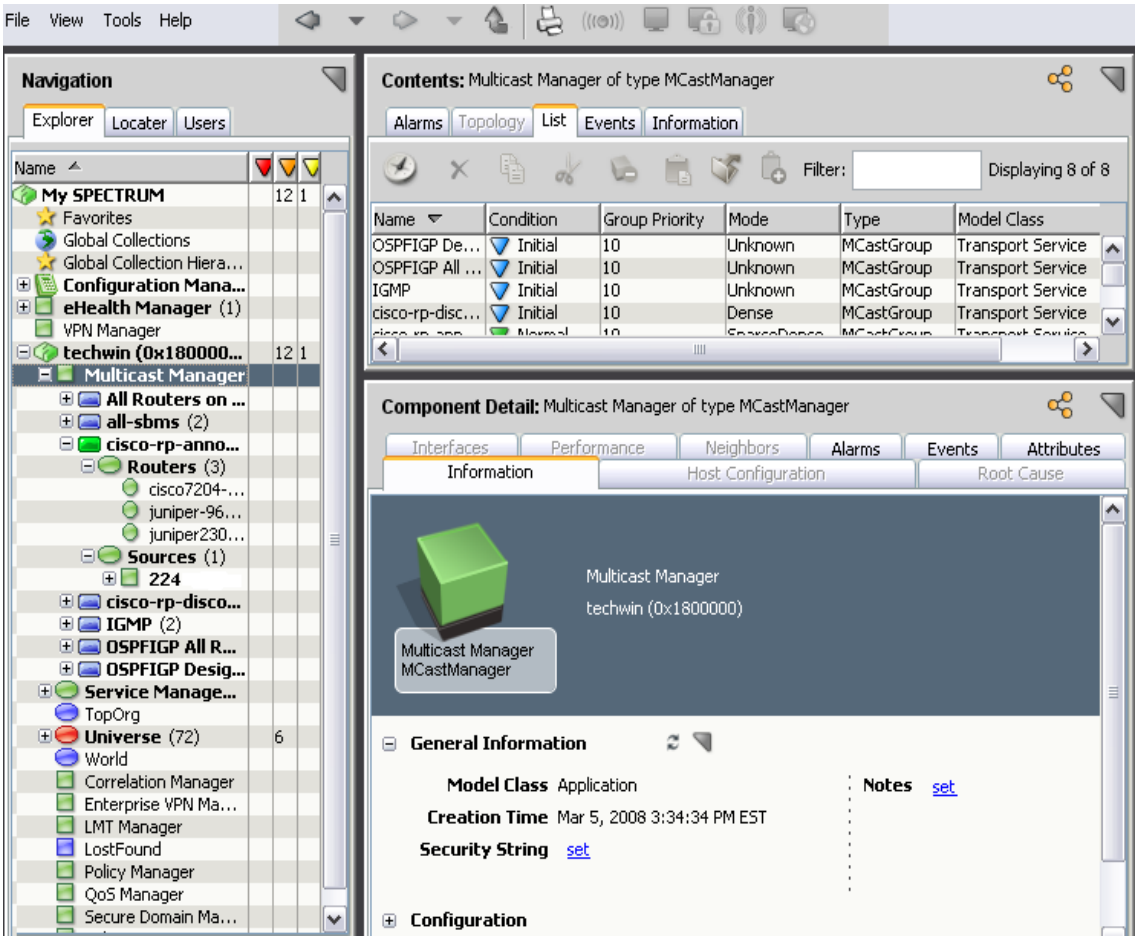
Configuration Information Subview (see page 25)
Define a Proxy for an Unmanageable Source (see page 36)

Multicast Manager View

You can access Multicast Manager from the Explorer tab of the Navigation panel in the OneClick Console. When you expand the Multicast Manager folder, all of the groups managed by Multicast Manager are listed. When you expand each group, the routers and sources contained in the Multicast Group are listed.

Once the physical components of your multicast network are modeled in CA Spectrum, you can use Multicast Manager to discover your multicast devices. You can then navigate to or search for these multicast elements in OneClick. The Contents panel and Component Detail panel provide configurations, alarms, events, and other information for a selected Multicast element.

The following shows the Multicast Manager view:



Note: For more information about modeling your network, see the *Modeling and Managing Your IT Infrastructure Administrator Guide.*

Chapter 2: Multicast Manager Configuration

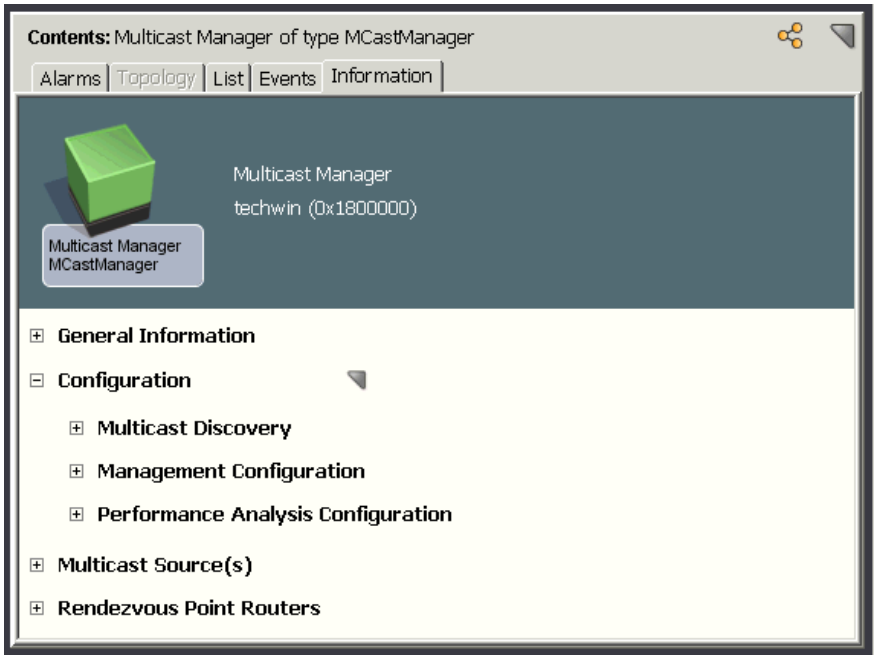
This section contains the following topics:

Access Multicast Manager Configuration Parameters

The Multicast configuration parameters are available to all users with administrative privileges.

To access Manager configuration parameters

1. Expand the desired landscape from the OneClick Explorer tab and select the Multicast Manager.
2. Click the Information tab in the Contents panel.
3. Expand the Configuration node to display the following options:



Multicast Discovery Subview

You can set the following parameters in the Multicast Discovery subview:

Discovery Status

Runs a Multicast discovery and displays status.

Device Reconfiguration Discovery

Runs a Device Application Reconfiguration action.

Group Address Filter Type

Specifies the addresses that you want to exclude or include. You can select one of the following options to set the filter type:

Inclusive

Filters and saves the Multicast addresses specified by the Group Address Filter.

Exclusive

Filters and saves the Multicast addresses except those specified by the Group Address Filter.

Group Address Filter

Specifies the Multicast addresses to be saved when the Multicast Discovery is run.

Note: The addresses are not filtered and saved if you do not add them in the Group Address Filter. So, even if the Group Address Filter Type is inclusive and the Group Address Filter is empty, all addresses are discovered.

Background Create Group Models

Creates models for the new Multicast groups, sources, or routers discovered from a background discovery.

Note: The Enable Background Discovery parameter must be set to Yes.

Model Sources as Pingables

It may not be possible for you to model the device representing the Source of the Multicast traffic because of the IT infrastructure in your particular network environment. You can set one of the following options:

- Yes (default)

  Creates a model using the pingable model type for each Multicast Source that does not have a corresponding device model. Multicast manager automatically assigns a model name to this pingable model using the convention <IPAddress>_mcast. The models created by running Multicast Discovery are placed in the Multicast Pingables Generic Container in the landscape topology view.

- No
- Only if reachable by ICMP ping

  Creates a model only if it gets a response from an ICMP packet.

By default, Multicast Manager determines the default gateway for the Source model. A correct default gateway is necessary for calculating performance and view in the topology.

Enable MSDP Discovery

Enables MSDP Discovery when set to yes.

Create Groups without Source

Creates a group when the source is not manageable. This occurs when the source is initiated outside the network. If there is no manageable source to the group, the group stays in the initial condition and no fault management information is computed. When Create Groups without Source attribute is set to No, Multicast Manager does not create groups for sources that are not manageable.

Default: Yes

Discovery Polling Interval (sec)

Determines how often (in seconds) Multicast Manager polls the attribute in the CiscoIPMRoute MIB during a background discovery. This determines if new multicast groups, sources, or routers exist.

Enable Background Discovery

Creates events when new multicast groups, sources, or routers become active on the network. Events for new groups and sources are asserted on the Multicast Manager model. Events for new multicast routes are asserted on the applicable device model.

Before you enable background discovery, run a manual discovery to find and model the RP routers that will be associated with discovered groups.

To determine if a new entity has become active, Multicast Manager polls an attribute in the Cisco IPMRoute MIB which counts the number of entries in the Multicast routing table.

More information:

Run On-Demand Multicast Discovery (see page 16)
Multicast Source Discovery Protocol (see page 17)
Configuration Subview (see page 32)

Management Configuration Subview

You can set the following parameters in the Management Configuration subview:

Default Group Priority

Sets the priority value given to a group when it is created. This value defines the relative importance of the group and can be used by the network operator to prioritize troubleshooting resources when there are problems with multiple groups.

Enable Port Polling

If this parameter is set to Yes, when Multicast Discovery is run, it enables port polling on all interfaces associated with group models. This enables port status to contribute to the overall group condition.

Default: Yes

Topology Display Units

Selects the units displayed in the Topology graph. You can select *one* of the following:

- % Throughput
- Pkts/s or Bits/s

  Note: The Topology Display Unit is Pkts/s or Bits/s based on the Performance Collection Type option set under Performance Analysis Configuration.

Global Enable Multicast Path Change Detection

Enables or disables Multicast Manager's ability to detect topology changes in the Multicast distribution tree. It does this by identifying changes in the device interface receiving Multicast traffic. By default, it is set to No. You can also enable or disable this feature on a group model basis.

Total Groups (modeled/known)

Shows the number of groups that are modeled and known by Multicast Manager. The number of groups modeled is the number of multicast groups that have been discovered and are presently modeled by Multicast Manager. The number of groups known reflects the number of groups discovered by Multicast Manager via the discovery process, but that are not currently modeled; that is, they have been deleted.

Group Count Threshold

Displays the group count threshold. This parameter generates a critical alarm on the Multicast Manager model if it is exceeded.

Total Sources (modeled/known)

Shows the number of sources that are modeled and known by Multicast Manager. The number of sources modeled is the number of multicast sources that have been discovered and are presently modeled by Multicast Manager. The number of sources known reflects the number of sources discovered by Multicast Manager via the discovery process, but that are not currently modeled; that is, they have been deleted.

Source Count Threshold

Displays the source count threshold. This parameter generates a critical alarm on the Multicast Manager model if it is exceeded.

More information:

Multicast Groups (see page 24)
Performance Analysis Configuration Subview (see page 25)

Performance Analysis Configuration Subview

You can set the following parameters in the Performance Analysis Configuration section:

Device Performance Alarms

Enables or disables the generation of Multicast performance based alarms on the device; these alarms are asserted in addition to those on the Multicast Group model. If enabled, alarms are produced on the device models in the Group causing the threshold violation.

Default: Disable

Performance Analysis

Enables or disables the entire Multicast Performance Monitoring system. You can also enable or disable performance monitoring on a group model basis.

Default: Enable

Note: Performance Analysis must be enabled for performance information to be displayed in the Multicast Topology view.

Collection Interval (sec)

Determines the interval at which the devices are sampled to obtain performance and IfIndex information. Lowering the interval may have a negative impact on the overall SpectroSERVER performance.

Default: 300 seconds (5 minutes)

Performance Collection Type

Sets the performance collection type. You can select Packets/s or Bits/s.

Default: Bits/s

More information:

Performance Analysis Configuration Subview (see page 25)
View Multicast Topology Information (see page 37)

Chapter 3: Multicast Manager Discovery and Modeling

This section contains the following topics:

Multicast Network Modeling

CA Spectrum discovers and models the physical network infrastructure using Discovery, manual modeling, or the Modeling Gateway. Before using the Multicast Discovery functionality in Multicast Manager, you must first model the physical components of your network in CA Spectrum using one of these methods.

Note: For more information about using Discovery, manual modeling, or the Modeling Gateway to model your network, see the *Modeling and Managing Your IT Infrastructure Administrator Guide* and the *Modeling Gateway Toolkit Guide.*

Multicast Discovery

Once the physical network components have been discovered, network elements which implement the Multicast MIBs supported by Multicast Manager can be discovered and modeled. This discovery is based on the MIBs specified within Device Support. These MIBs provide the information required to identify all the primary multicast components.

Multicast Manager models multicast groups, sources, and receivers. To do this, Multicast Manager uses group, source, and receiver model types.

Group models represent a domain-wide multicast data stream. The source and receiver models represent the producer and consumer of information in a multicast network. The RP represents the meeting point for sources and receivers in a multicast network.

Run On-Demand Multicast Discovery

You must log in with administrator privileges to run Multicast Discovery.

To run Multicast Discovery

1. Expand the desired landscape from the OneClick Explorer tab and select the Multicast Manager.

   Information and Configurations display in the Contents panel.

2. Select the Information tab in the Contents panel, expand the Configuration folder and then expand the Multicast Discovery node.

   Multicast Discovery controls and configurations display.

3. Set the appropriate Discovery parameters.

4. Click Run next to the Discovery Status field to begin Multicast Discovery.

   The Discovery Status field shows the status of the discovery process.

Run Multicast Discovery on Selected Models

You can configure the Multicast Network Services Discovery from the OneClick views that display models.

To run Multicast Discovery on selected models

1. Select the models.

2. Click Tools, Utilities, Network Services Discoveries, Multicast Discovery.

   The Discovery process is initiated. You can check the status in the Configuration subview.

Configuring Multicast Discovery During Modeling

CA Spectrum lets you configure Network Services Discoveries, including Multicast Discovery, during modeling. As a part of modeling configuration, you can specify which network service discoveries to run with the modeling process.

Note: For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Multicast Source Discovery Protocol

CA Spectrum supports the Multicast Source Discovery Protocol (MSDP). When you create a device model using OneClick Discovery, AutoDiscovery, or manual modeling, CA Spectrum automatically discovers MSDP information on network devices that support the MSDP protocol. This information is used during the Multicast Discovery process to identify Multicast network elements only visible from your network domain via MSDP.

If you already created device models representing the physical components of your Multicast network with a CA Spectrum release prior to 7.1 SP2, you must use the Device Reconfiguration Discovery button to discover MSDP protocol support on your network. After the Device Reconfiguration Discovery finishes, rerun Multicast Discovery.

Delete Device Models

You can delete a device model by right-clicking the device and selecting Delete. If a device model is deleted, any associated multicast group, source, or receiver model is also deleted.

Chapter 4: Managing the Multicast Network

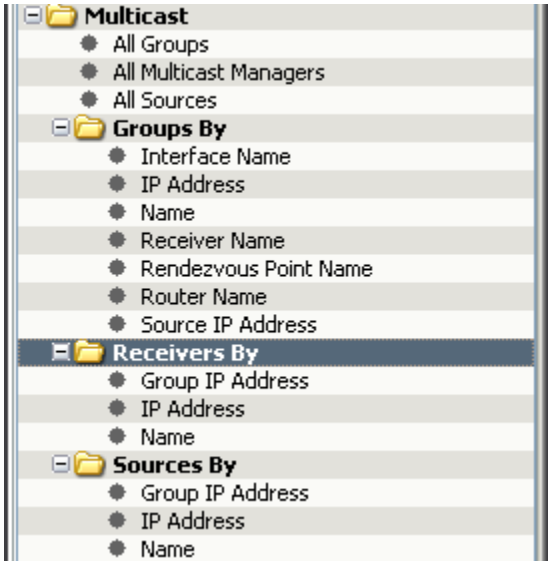
This section contains the following topics:

Search for Modeled Multicast Elements

Multicast searches, located in the Locater tab on the Navigation panel, lets you search your distributed network for Multicast Managers, multicast groups, multicast receivers, and multicast sources using criteria that you specify. You can use the search results to access a number of views which present management and performance information.

Search results appear in the Contents panel. Detailed information about the modeled device selected in the Contents panel is shown in the Component Detail panel.

The following shows the available multicast searches:



To search for modeled multicast elements

1. Select the Locater tab in the OneClick Navigation panel.

   All available OneClick searches display.

2. Expand the Multicast folder.

   All available Multicast searches display.

3. Double-click a search, enter the appropriate criteria, and click OK.

   Note: Search criteria is case sensitive.

   The search results appear in the Contents panel.

4. (Optional) Use the Filter field in the Contents panel to filter your results.

Note: For more information about running searches, see the *Operator Guide*.

Group Search Results

The results of group searches are displayed in the Contents panel. Use the Filter field in the Contents panel to filter your results. The following information displays for each group search:

Name

Indicates the name of the group. This may be the actual name or the IP address of the group.

Condition

Indicates the overall health of the group. It is calculated based on the condition of the RP routers, source, interconnecting routers, and router interfaces within the group. There are five possible conditions: Initial (blue), Normal (green), Degraded (orange), Maintenance (brown), and Down (red).

If the condition of the group is either Degraded or Down, an alarm will be generated on the Group model.

The condition displayed is based on the values in the following table.

For Multicast Manager to determine the condition of a group, the group's sources and RP must be modeled in CA Spectrum and must be contained in the same CA Spectrum landscape.

Group Priority

Indicates the relative importance of the group. It can be used to prioritize troubleshooting resources when there are problems with multiple groups. The smaller the number the higher the level of priority.

Mode

Indicates the multicast mode of the group. The value can be either sparse or dense.

Type

Indicates the model type of the model that represents the device.

Model Class

Indicates the model class of the model that represents the device.

Note: For more information about model classes, see the *Concepts Guide*.

The condition that is displayed for the overall health of a group is based on the values in the following table:

Group Condition	Performance Monitor Alarm Condition	RP Modeled	RP Contact Status is Established	Source Modeled	Source Contact Status is Established	Interface Contact Status is Established	Router Contact Status is Established
Good	Good	Y	Y	Y	Y	Y	Y
Minor	Minor	Y	Y	Y	Y	Y	Y
Major	Major	Y	Y	Y	Y	Y	Y
Critical	Critical	Y	Y	Y	Y	Y	Y
Good	Initial	Y	Y	Y	Y	Y	Y
Minor	Good	Y	Y	Y	Y	N	N
Minor	Minor	Y	Y	Y	Y	N	N
Major	Major	Y	Y	Y	Y	N	N
Critical	Critical	Y	Y	Y	Y	N	N
Minor	Initial	Y	Y	Y	Y	N	N
Critical	Good	Y	N	Y	N	Y	Y
Critical	Minor	Y	N	Y	N	Y	Y
Critical	Major	Y	N	Y	N	Y	Y
Critical	Critical	Y	N	Y	N	Y	Y
Critical	Initial	Y	N	Y	N	Y	Y
Good	Good	N	N/A	N	N/A	N/A	N/A
Minor	Minor	N	N/A	N	N/A	N/A	N/A
Major	Major	N	N/A	N	N/A	N/A	N/A
Critical	Critical	N	N/A	N	N/A	N/A	N/A
Initial	Initial	N	N/A	N	N/A	N/A	N/A

Note: A Multicast group will be put into maintenance mode if any of the following occur:

- If there are any RPs within the Multicast group and they are all in maintenance.
- If there are Multicast sources within the Multicast group and they are all in maintenance.
- If there are any devices within the Multicast group and they are all in maintenance.
- If there are any interfaces within the Multicast group and they are all in maintenance.

More information:

General Information Subview (see page 24)

Receiver Search Results

The results of receiver searches are displayed in the Contents panel. Use the Filter field in the Contents panel to filter your results. The following information displays for each receiver search:

Name

Indicates the name of the receiver. This may be the actual name or the IP address of the receiver.

Condition

Indicates the status of the model that represents the device. Possible conditions are initial (blue), normal (green), minor alarm (yellow), major alarm (orange), critical alarm (red), gray (unknown), and maintenance (brown).

Type

Indicates the model type of the model that represents the device.

IP Address

Indicates the IP address of the receiver.

Model Class

Identifies the model class of the receiver.

Note: For more information about model classes, see the *Concepts Guide*.

Source Search Results

The results of Source searches are displayed in the Contents panel. Use the Filter field in the Contents panel to filter your results. The following information displays for each source search:

Name

Identifies the name of the source. This may be the actual name or the IP address of the source.

Condition

Indicates the status of the model that represents the device. Possible conditions are initial (blue), normal (green), minor alarm (yellow), major alarm (orange), critical alarm (red), gray (unknown), and maintenance (brown).

Type

Indicates the model type of the model that represents the device.

Source Address

Identifies the IP address of the source.

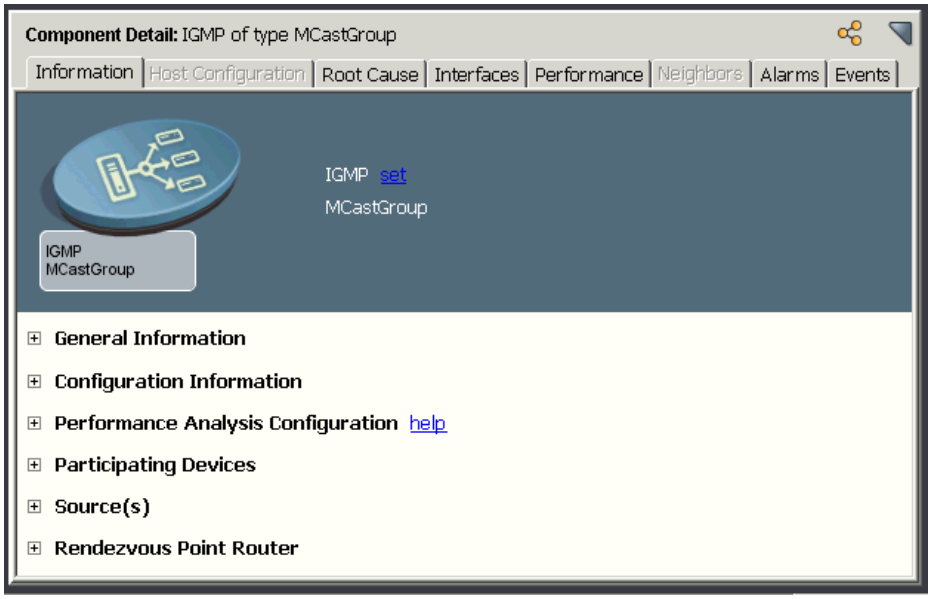
Model Class

Identifies the model class of the source.

Note: For more information about model classes, see the *Concepts Guide*.

Multicast Groups

The Component Detail panel contains tabs that let you view multicast information about a selected group. The Information tab provides a number of subviews for the group.



General Information Subview

You can set the following parameters for a group model in the General Information subview:

Group Address

Indicates the IP address of the group.

Group Priority

Indicates the relative importance of the Group. It can be used by the network operator to prioritize troubleshooting resources when there are problems with multiple Groups. The lower the value of Group Priority for a given Multicast Group, the higher its priority. If you are logged in as an administrator, you can edit this field by clicking set.

Model Class

Indicates the model class of the model that represents the device.

Note: For more information about model classes, see the *Concepts Guide*.

Creation Time

Indicates the creation date and time of the Group model.

Security String

Indicates the SNMP community string or password for the device. If you have the appropriate permissions, you can modify the security string. Click set, enter the security string into the available field, and press Enter.

Landscape

Indicates the CA Spectrum landscape on which the device is modeled.

Notes

Indicates notes or comments about the group. To add a note, click Set and then enter the appropriate information. When you have finished entering the note, click Save. If you do not want to save the note that you entered, click Cancel.

Configuration Information Subview

You can set the following attribute in the Configuration Information subview:

Ignore initial/unmodeled sources in group condition

Lets you choose (on a per-group basis) whether or not to include the status of the source model in the group condition calculation. If you purchase a Multicast service or a data feed from an external service, you may not have access to the source to obtain its status. You can use this option to exclude the source's status in the group condition calculation. If you do own and have access to the source of the multicast stream, you should include the source status in the group status configuration.

Performance Analysis Configuration Subview

Performance analysis shows you important information about the flow of multicast traffic on your network. In a properly functioning multicast network, each point of the network (where multicast is enabled for that group) should experience the same traffic flow in packets per second or bytes per second.

Any deviation from the traffic level as measured at the source could indicate one or more of the following scenarios:

- A change in group membership.
- A change in routing where multicast traffic is taking a different path due to load balancing, a redundant failover, or a change from shared to source mode.
- A change in the network's multicast configuration where multicast has been disabled on an interface or device.

- A change in interface status.
- Device or link instabilities.

You can configure how Multicast Manager analyzes the performance of the group model selected. A graphical representation of source traffic is also available. You can set the following parameters in the Performance Analysis Configuration subview:

Global Group Performance Analysis

Indicates whether the entire Multicast Performance Monitoring system is enabled or disabled. It can be set in the Multicast Manager model's Performance Analysis Configuration. The value of this parameter must be set to enable for the Group Performance Analysis to function.

Group Performance Analysis

Enables performance monitoring for each Group. This value must be enabled for performance information to be displayed in the Multicast Topology view.

Percent Degradation Threshold

Defines the percent variation allowed in the monitoring of Group performance. For example, if the source is measured at 100 pps, all other points in the network receiving this Group should be within this percent threshold (+/-). Otherwise, a threshold violation is noted for the Group on that device. The default value is three percent.

Enable Multicast Path Change Detection

When this parameter is set to Yes, the Multicast Group looks for changes in the interface receiving multicast traffic. If a change is detected, an event is generated on the offending device. This event gives information about the device that generated the event, the interface receiving the traffic, and the group to which the device belongs. By default, this parameter is set to No.

The following scenarios can cause a change in path to be detected:

- A router performs a routine load balancing operation and redirects the multicast traffic to be routed around the network by a different path. This does not necessarily indicate a failure.
- A router along the path of the multicast traffic goes down. In this case a topology change will occur and the device receiving the multicast traffic will detect that the interface sending the information has changed.

Enable Path Change Alarms

If this parameter is set to Yes, Multicast Manager generates a yellow (minor) alarm when a change in path is detected. For this parameter to operate correctly, Enable Multicast Path Change Detection must be set to Yes.

Group Performance Alarms

Enables Multicast Manager to create an alarm in response to the violation of performance thresholds defined in the Minor, Major, and Critical Alarm Threshold parameters.

Minor Alarm Threshold

Sets the Minor Threshold Percent. This value determines the severity of threshold violations on a Group. For example, a Group may have 100 interfaces sampled in the network. If more than the Minor Alarm Threshold percentage and less than the Major Alarm Threshold percentage of those samples are in violation of the Performance Degradation Threshold, a Minor event (and an alarm if Group Performance Alarms is set to enable) is generated.

Major Alarm Threshold

Sets the Major Threshold Percent. This value determines the severity of threshold violations on a Group. For example, a Group may have 100 interfaces sampled in the network. If more than the Major Alarm Threshold percentage and less than the Critical Alarm Threshold percentage of those samples are in violation of the Performance Degradation Threshold, a Major event (and an alarm if Group Performance Alarms is set to enable) is generated.

Critical Alarm Threshold

Sets the Critical Threshold Percent. This value determines the severity of threshold violations on a Group. For example, a Group may have 100 interfaces sampled in the network. If more than the Critical Alarm Threshold percentage of those samples are in violation of the Performance Degradation Threshold, a Critical event (and an alarm if Group Performance Alarms is set to Enable) is generated.

Minimum Rate (Bits/sec)

Sets the minimum rate for critical alarm threshold.

Default: 0 Bits/ sec

Maximum Rate (Bits/sec)

Sets the maximum rate for critical alarm threshold.

Default: 4294967295 Bits/ sec

Note: The Minimum Rate and Maximun Rate for alarm threshold apply only when Performance Collection Type is set to Bit/Sec. Thus these alarms should not occur unless the user inputs something for these values.

More information:

Performance Analysis Configuration Subview (see page 13)
Source Performance Information (see page 34)
View Multicast Topology Information (see page 37)

Participating Devices Subview

The Participating Devices subview provides information for all of the devices that participate in the multicast group. You can set the following parameters in the Participating Devices subview:

Condition

Indicates the status of the model that represents the device. Possible conditions are initial (blue), normal (green), minor alarm (yellow), major alarm (orange), critical alarm (red), gray (unknown), and maintenance (brown).

Name

Indicates the name of the participating device model.

Network Address

Identifies the network address of the device.

Manufacturer

Indicates the manufacturer of the device that the model represents.

Model Class

Identifies the model class of the device model.

Note: For more information about model classes, see the *Concepts Guide*.

MAC Address

Indicates the MAC address of the device.

Type

Indicates the model type of the model that represents the device.

Landscape

Indicates the CA Spectrum landscape on which the device is modeled.

Sources Subview

The Sources subview lists all of the sources for a multicast group. You can set the following parameters in the Sources subview:

Condition

Identifies the status of the source model. Possible conditions are initial (blue), normal (green), minor alarm (yellow), major alarm (orange), critical alarm (red), unknown (gray), and maintenance (brown).

Name

Identifies the name of the source model. This may be the actual name or the IP address of the source.

Type

Identifies the model type of the source model.

Model Class

Identifies the model class of the source model.

Note: For more information about model classes, see the *Concepts Guide*.

Landscape

Indicates the CA Spectrum landscape on which the device is modeled.

Rendezvous Point Router

The Rendezvous Point Router subview lists the RP router for the Multicast Group. You can set the following parameters in the Rendezvous Point Router subview:

Condition

Indicates the status of the model that represents the device. Possible conditions are initial (blue), normal (green), minor alarm (yellow), major alarm (orange), critical alarm (red), gray (unknown), and maintenance (brown).

Name

Indicates the model name of the model that represents the device.

Network Address

Identifies the network address of the device.

Manufacturer

Indicates the manufacturer of the device that the model represents.

Model Class

Indicates the model class of the model that represents the device.

MAC Address

Indicates the MAC address of the device.

Type

Indicates the model type of the model that represents the device.

Landscape

Indicates the CA Spectrum landscape on which the device is modeled.

Group Interfaces Information

You can access information about the interfaces associated with a selected multicast group by selecting a group model and then selecting the Interfaces tab on the Component Detail panel. The following information displays for the interface model:

Name

Indicates the model name of the model that represents the device.

Condition

Indicates the status of the model that represents the device. Possible conditions are initial (blue), normal (green), minor alarm (yellow), major alarm (orange), critical alarm (red), gray (unknown), and maintenance (brown).

Status

Indicates the contact status of the link between this interface and the interface to which it is connected.

PIM Status

Indicates the configured mode of this PIM interface.

Mode

Indicates the PIM mode of the interface. This value can be sparse, dense or sparseDense.

IGMP Version

Indicates the version of IGMP that is running on this interface.

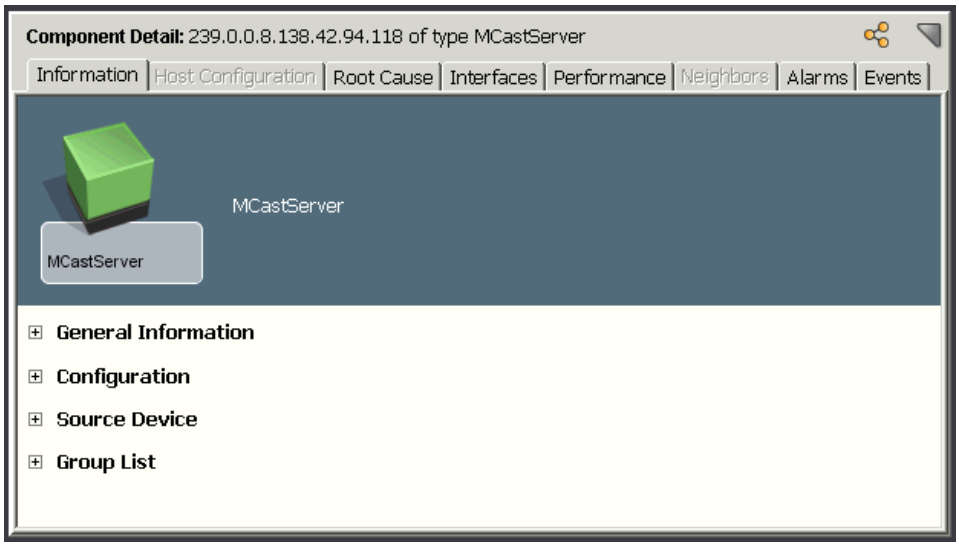
Note: If an interface does not participate in a particular protocol, the columns pertaining to that protocol for that interface will not contain any data.

Group Event Information

You can access the Event view for a group by selecting a group model and then selecting the Events tab on the Component Detail panel. The Events tab displays event information for events that occur on the group model.

Multicast Source Management

The Component Detail panel contains tabs that let you view additional information about a source selected from the search results list in the Contents panel. The Information tab provides a number of subviews for the source, as shown in the following example:



Note: If a multicast source is unmanageable, you can define a source proxy.

More information:

Define a Proxy for an Unmanageable Source (see page 36)

General Information Subview

You can set the following parameters for the multicast source model in the General Information subview:

Condition

Indicates the status of the model that represents the device. Possible conditions are initial (blue), normal (green), minor alarm (yellow), major alarm (orange), critical alarm (red), gray (unknown), and maintenance (brown).

Source Address

Indicates the IP address of the source.

Model Class

Indicates the model class of the model that represents the device.

Note: For more information about model classes, see the *Concepts Guide*.

Creation Time

Identifies the creation date and time of the source model.

Security String

Indicates the SNPMP community string or password for the device. If you have the appropriate permissions, you can modify the security string. Click set, enter the security string into the available field, and press Enter.

Landscape

Indicates the CA Spectrum landscape on which the device is modeled.

Configuration Subview

The Configuration subview lets you define a proxy to reach the selected source and reconfigure the Default Gateway. You can set the following parameters for a proxy in the Configuration subview:

Default Gateway

Indicates the IP Address of the device CA Spectrum should poll to obtain base-line performance statistics for a multicast group. This value will generally be the IP address of the default gateway for the Multicast Source. By default, Multicast Manager determines the default gateway. The default gateway must be correct to utilize the Multicast Performance and Topology views. Click Set to modify the IP address.

When the default gateway is set to the Virtual IP address of a Hot Standby Routing Protocol (HSRP) group, for Multicast Performance Analysis to work properly, it is necessary to configure the HSRP member routers to send HSRP related SNMP Traps to CA Spectrum. This lets CA Spectrum continue to obtain multicast performance statistics when the Active HSRP router changes.

Proxy IP

Indicates the IP Address of the proxy for an unmanageable multicast source. This lets you compute condition and gather performance data for an unmanageable source using the information from the closest ingress router to the unmanageable source.

More information:

Define a Proxy for an Unmanageable Source (see page 36)

Source Device Information

The following information is shown about the source device for a multicast source model.

Condition

Indicates the status of the model that represents the device. Possible conditions are initial (blue), normal (green), minor alarm (yellow), major alarm (orange), critical alarm (red), gray (unknown), and maintenance (brown).

Name

Indicates the model name of the model that represents the source.

Network Address

Identifies the network address of the device.

Manufacturer

Indicates the manufacturer of the device that the model represents.

Model Class

Indicates the model class of the model that represents the source.

Note: For more information about model classes, see the *Concepts Guide*.

MAC Address

Indicates the MAC address of the source device.

Type

Indicates the model type of the model that represents the source device.

Landscape

Indicates the CA Spectrum landscape on which the device is modeled.

Group List Subview

The Group List subview displays information about group models to which the source model sends information. You can set the following parameters for a group model in the Group List subview:

Condition

Indicates the status of the model that represents the device. Possible conditions are initial (blue), normal (green), minor alarm (yellow), major alarm (orange), critical alarm (red), gray (unknown), and maintenance (brown).

Name

Indicates the model name of the model that represents the device.

Group Priority

Indicates the relative importance of the group. It can be used to prioritize troubleshooting resources when there are problems with multiple groups. The smaller the number the higher the level of priority.

Mode

Indicates the multicast mode of the group. The value can be either sparse or dense.

Type

Indicates the model type of the model that represents the device.

Model Class

Indicates the model class of the model that represents the device.

Note: For more information about model classes, see the *Concepts Guide*.

More information:

General Information Subview (see page 24)

Source Event Information

You can access the Event view for a source by selecting a source model and then selecting the Events tab on the Component Detail view. The Events tab displays event information for events that occur on the source model.

Source Performance Information

Real-time multicast performance statistics can be obtained for a multicast source by selecting the Performance tab in the Contents panel. The Performance view provides a real-time graphical view of source traffic. The information provided in the Performance view is useful for monitoring multicast performance and faults within the multicast environment in a graphical format.

You can select *one* of the following:

- Multicast Source Octet Traffic
- Multicast Source Packet Traffic
- Multicast Source Bit Traffic

For the graph to function properly, the following must be true:

- If you are able to create a physical device model of the source, you should model it as an SNMP host. You can choose one of the following host model types:
  - Host_Compaq
  - Host_Dell
  - Host_Sun
  - Host_systemEdge
  - Host_Device
  - GnSNMPDev
- If you are not able to create a physical device model of the source, you should model the source as a pingable. The Multicast Discovery process creates pingable models automatically for all multicast sources that do not have a corresponding physical device model.
- CA Spectrum must be able to communicate with the source.
- The default gateway for the source must be modeled in CA Spectrum using the appropriate router model type.
- If you model the source as a pingable, the default gateway must be correct in the source model's Configuration view.
- CA Spectrum must be able to communicate with the default gateway for the source.
- The default gateway must support one of the IPM Route MIBs (draft or RFC).
- The routers in a Hot Standby Routing Protocol (HSRP) group must be set to send HSRP traps to the SpectroSERVER for Multicast Manager performance monitoring to work properly, and for performance graphs to show traffic statistics when the active router in the HSRP group has changed because of a failover.

More information:

Multicast Manager Configuration (see page 9)
Multicast Discovery (see page 15)
Configuration Subview (see page 32)

Define a Proxy for an Unmanageable Source

Multicast Manager lets you define a proxy to monitor an unmanageable source. Examples of an unmanageable source (or multicast stream) are groups which originate outside of your network. These could be feeds which traverse the Internet to get to this location or dedicated services like financial data streams which are purchased to feed trading applications.

The proxy should ideally be the ingress router where the multicast stream enters the network. Since you cannot monitor the source, you can configure the ingress router where the multicast stream enters the network to represent the unmanageable source for performance comparisons.

To define a proxy for an unmanageable source

1. Conduct a Multicast Search for the unmanageable source model.

   The Contents panel displays the results of the search.

2. Select the unmanageable source model from the results list.

   Information and configurations display in the Information tab of the Component Detail panel.

3. Expand the Configuration subview.

   The Default Gateway and Proxy IP configuration parameters display.

4. Click set next to Proxy IP and enter the IP Address of the ingress router where the Multicast Stream from the unmanageable source enters your network and press Enter.

   The IP Address of the unmanageable source's proxy displays.

Alarm List

The Contents panel displays the Alarms list for the modeled element that you select in the Navigation panel.

To know more about an alarming element, you can click the Alarm Detail button on the Alarm tab of the Component Detail panel.

If the Alarm list in the Contents panel is empty, the Component Detail panel displays the Information tab for a selected element.

Multicast Receiver Information

Information about multicast receivers modeled as pingables is available in the Multicast Information subview of the pingable model. Expand the Associated Multicast Servers subview to display the receiver's associated multicast servers and their condition. Expand the Associated Multicast Groups subview to display the receiver's associated multicast groups and their condition.

View Multicast Topology Information

The Multicast Topology view provides a graphical representation of the data flow from a multicast source through the associated devices, and allows you to more easily troubleshoot and gauge the overall impact of traffic flow changes and outages within your environment. You can access a topology view for each source within a multicast group that Multicast Manager has discovered and modeled. The performance information for each segment of the traffic distribution tree displays the percentage of source traffic reaching that segment. The percentage is calculated by comparing the baseline traffic from the source.

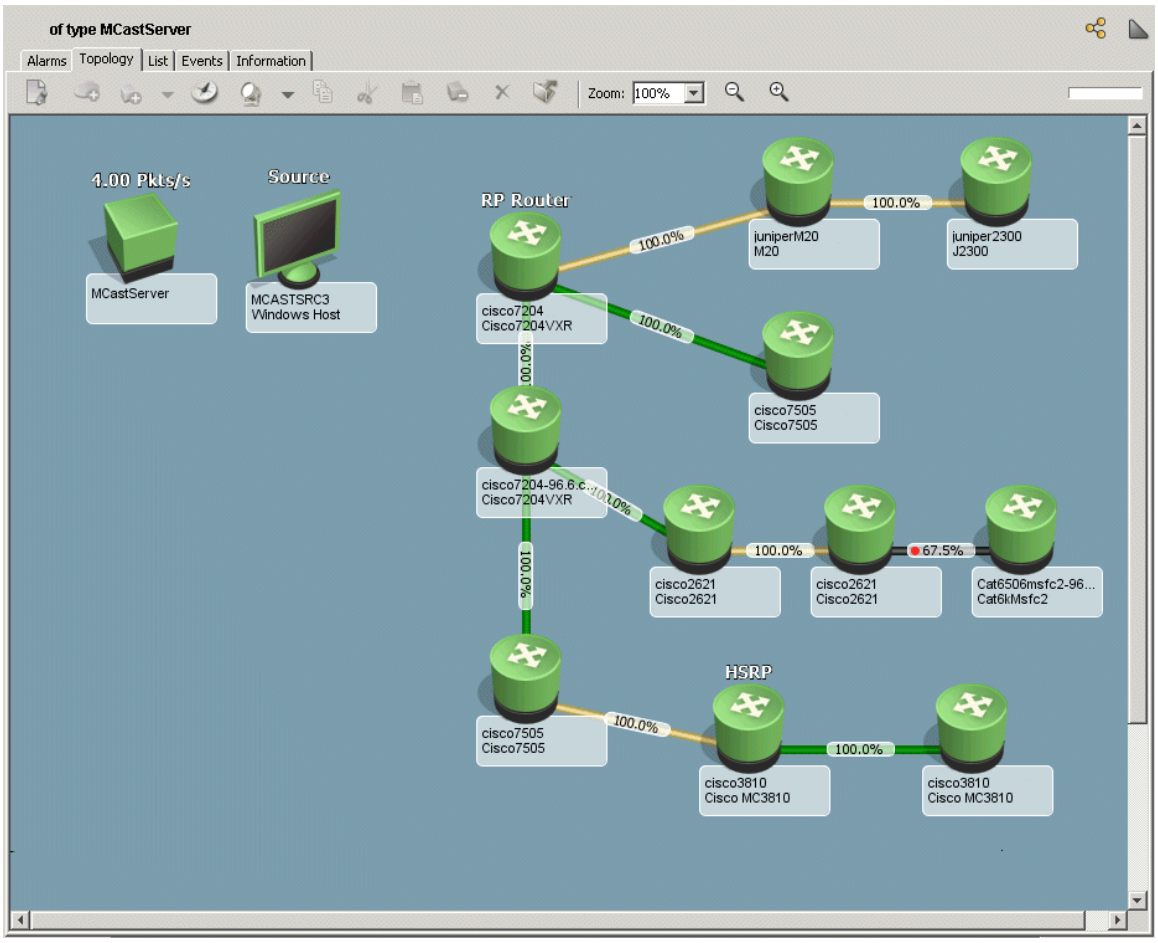
Performance Analysis must be enabled on the Multicast Manager model and for any multicast group you want performance information to be displayed for in the Multicast Topology view.

The path structure and performance data displayed is based on the latest poll. It may not necessarily reflect the current state.

To view multicast topology information

1. Expand the appropriate Multicast Manager Group node from the Navigation panel.
2. Expand the Source folder, select the desired source, and select the Topology tab in the Contents panel.

Multicast Manager displays a Topology view.



Note: Use the Topology Display Units attribute to choose the desired units to display in the topology.

More information:

Management Configuration Subview (see page 12)
Performance Analysis Configuration Subview (see page 13)
Performance Analysis Configuration Subview (see page 25)

Chapter 5: Trap Support

The Multicast Manager supports the handling of traps specified by the CISCO-PIM-MIB. The following table describes the supported traps and their information.

Supported Traps	OID	Event Generated	Alarm Generated	Default Alarm Severity
ciscoPIMRPMappingChange	1.3.6.1.4.1.9.9.184.2.0.3	0x2104a5	None	NA
ciscoPIMInvalidRegister	1.3.6.1.4.1.9.9.184.2.0.4	0x2104a6	None	NA
ciscoPIMInvalidJoinPrune	1.3.6.1.4.1.9.9.184.2.0.5	0x2104a7	None	NA

In addition to supporting traps specified by the CISCO-PIM-MIB, Multicast Manager supports the trap specified by the CISCO-HSRP-MIB. Multicast Manager can perform multicast performance monitoring on the active router in a HSRP group when the active router has changed due to a failover.

The following table describes the HSRP trap.

HSRP Traps	OID	Event Generated	Alarm Generated	Default Alarm Severity
cHsrpStateChange	1.3.6.1.4.1.9.9.106.2.6.1	0x0021091e	0x0021091e	Minor
		0x0021091f	0x0021091e	NA

Chapter 6: Device Support

This section contains the following topics:

Cisco and Juniper M Series Devices

Multicast Manager supports the discovery, modeling, and viewing of devices that support multicast traffic using the MIBs specified in the following table:

Supported MIBs	Cisco 12.0	Cisco 12.2 or later
ipMRoute - Cisco	Y	Y
ipMRoute - Experimental	Y	Y
ipMRoute - Standard	N	N
PIM – Cisco	Y	Y
PIM - Experimental	Y	Y
PIM - Standard	Y	Y
IGMP - Experimental	Y	N
IGMP - Standard	N	Y
Functions		
Group Discovery	Y	Y
Source Discovery	Y	Y
Receiver Discovery	Y	Y
RP Discovery	Y	Y
Group Performance	Y	Y
Traps		
Neighbor Loss	N	N
PIM Interface Up	N	N
PIM Interface Down	N	N
RP Mapping Change	Y	Y
Invalid Register	Y	Y

Supported MIBs	Cisco 12.0	Cisco 12.2 or later
Invalid Join Prune	Y	Y
Dynamic Discovery Traps		
Groups/Sources	N	N

Multicast Manager depends on functionality provided by CA Spectrum in the Cisco Router management module. Therefore, you must install the Cisco Router management module before or during the Multicast Manager installation.

Note: For more information about Cisco management modules, see the *Cisco Device Management Guide*.

Multicast Manager also supports Juniper M series devices using JunOS releases 6.1 and greater. The Juniper M series management module (SM-JPR1000) must be installed in order for Multicast Manager to discover and support multicast-enabled, Juniper devices.

Note: For more information about Juniper M series devices, see the *Device Management Reference Guide*.

Appendix A: Troubleshooting

The Group Condition Is Displayed Incorrectly

Symptom:

The group condition is being displayed incorrectly even though the source is down.

Solution:

If the source has not been modeled by CA Spectrum, when the physical device goes down there is no way to associate that status with a group on which it depends. Normally, a source down should produce a group down condition but, without the source modeled, the group shows a degraded condition.

Verify that the source is active and modeled by CA Spectrum, or that you have modeled third-party sources as pingable models.

More information:

Run On-Demand Multicast Discovery (see page 16)

The Group Condition Is Not Calculated Correctly

Symptom:

The group condition is not being calculated correctly when the model representing the RP is deleted after Multicast Discovery is run.

Solution:

Delete all of the groups and rerun Multicast Discovery.

Symptom:

The group condition is not being calculated correctly when the device representing the RP is not modeled.

Solution:

Model the RP, then rerun Multicast Discovery.

Changes Are Not Reflected in Performance Graphs

Symptom:

I added and removed some multicast sources and so I had to re-run Multicast Discovery. However, my changes are not immediately reflected in the performance graph.

Solution:

Restart the OneClick client.

New Group Models Staying in Initial Condition

Symptom:

New group models stay in Initial condition after a background discovery is run.

Solution:

No RPs will be discovered if a background discovery is run without previously running a manual discovery. Run a manual Multicast Discovery first.

Downward Spikes Display in a Group Performance Graph

Symptom:

When I display a group performance graph during an HSRP switchover, and the HSRP routers are configured to send HSRP traps to the SpectroSERVER, I see a downward spike to 0 for one polling cycle.

Solution:

After the switchover, the graph begins displaying the performance of the new active gateway.

No Data Is Displaying in Performance Graphs

Symptom:

No data is displayed for Group Performance Graph involving routers that are configured for HSRP.

Solution:

The likely cause is that the standby HSRP router has become the active router, and CA Spectrum was not notified of the change using the HSRP trap. Verify that the HSRP routers are configured to send the HSRP trap to the SpectroSERVER.

Performance Graphs Displaying Last Known Data Points After Contact is Lost

Symptom:

The Performance Graph view for a multicast group model displays the last known data point when contact with the default gateway is lost.

Solution:

This only happens for devices that do not support the IPMRoute MIB. For devices that support the IPMRoute MIB, the Performance Graph view displays a "0" data value until contact with the device is re-established.

Performance Statistics are Displaying as N/A

Symptom:

Performance statistics are displayed as N/A in the Multicast Topology view.

Solution:

The topology cannot gather data from the default gateway. If the performance information remains unavailable for an extended period, verify that the default gateway setting is set to a contactable multicast enabled router within this source's traffic topology tree.

More information:

Configuration Subview (see page 32)

Appendix B: Use Case Scenarios

Analyze Impact of a Device Alarm on Customer Multicast Traffic

Symptom:

Two unrelated trouble tickets against two core routers are generated at nearly the same time. Consider the following:

- The trouble tickets are routed based on the device class. They are sent to the level 2 operations Group. This Group focuses solely on maintaining the core routing infrastructure.
- The company's network management application has identified the routers in question and their offending components.
- The level 2 support group currently has a backlog of 25 open tickets for a variety of issues.
- The operators are currently using their knowledge of the core network to make decisions regarding issue prioritization.

Assume the following:

1. The customer has previously installed and configured Multicast Manager.
2. The customer has completed a discovery of their physical network.
3. The customer has completed a Multicast Discovery.
4. All multicast services have been modeled with CA Spectrum.
5. There are a couple of outages and the operator must analyze how these outages affect the multicast topology.
6. There is currently only one network administrator available to handle trouble tickets.

Solution:

1. The first router in the network goes down and is detected by CA Spectrum. Very shortly after this, the second router goes down.
2. CA Spectrum generates an alarm for each of the routers that has gone down.
3. The network management system (NMS) operator receives the alarms in the OneClick console and verifies the CA Spectrum alarms by pinging the routers and not receiving a response.

4. The NMS operator receives an alarm generated on one of the multicast groups modeled by Multicast Manager.
5. The NMS operator selects the multicast group in the OneClick console Alarms tab.
6. The NMS operator opens the Participating Devices subview of the Group's Information tab and sees that one of its routers has a Down (Red) condition. This router is one of the routers that an alarm was generated on in step 2 above. The network operator now understands that this router is critical to the operation of this multicast group, and of a higher priority than the other router issue.
7. The network operator creates a trouble ticket for the router which is impacting the multicast group. This ticket will show that the problem is a high impact outage and will include information on the impacted groups and applications. The network operator assigns the ticket to the network administrator.
8. The network administrator receives the trouble ticket and begins troubleshooting this high impact problem.
9. The network operator creates a trouble ticket for the second router outage that does not affect the multicast topology and assigns it to the network administrator.
10. The network administrator receives the second trouble ticket and will begin work on it after the multicast problem is resolved. CA Spectrum has allowed the troubleshooting process to be prioritized to the most critical fault.

More information:

Run On-Demand Multicast Discovery (see page 16)
Participating Devices Subview (see page 28)

An Individual User Is Not Receiving Multicast Traffic

Symptom:

When the stock market opens every day, a multicast feed is established to send real time market data to all the brokers on the company's network. The multicast group uses PIM Sparse mode to communicate to the traders who are widely dispersed throughout the company's operations. Today one broker is not receiving the market data feed but is receiving other multicast traffic.

Assume the following:

1. The customer has previously installed and configured Multicast Manager.
2. The customer has completed a discovery of their physical network.

3. The customer has completed a Multicast Discovery.
4. All multicast services have been modeled with CA Spectrum.
5. The broker has reported that he is no longer receiving the market data feed.

Solution:

1. The operator sees a CA Spectrum alarm in the OneClick console indicating that the router port has failed.
2. A trouble ticket is created and the operator begins troubleshooting the router port issue.
3. As part of his troubleshooting procedure the operator uses the Multicast Manager "Groups by Interface" search.
4. This view shows all the affected groups and their priority. Groups 1-3 are affected by this router.
5. In addition, a broker reports that he is no longer receiving the multicast data feed for Group 2.
6. The operator can tell the broker that he is part of the affected group (due to the router failure). A second trouble ticket does not need to be created.
7. The operator fixes the router interface.
8. The router interface is working and market data is now being received by the broker reporting an outage.
9. The operator confirms multicast traffic is being received by the broker and closes the trouble ticket.

More information:

Run On-Demand Multicast Discovery (see page 16)
Search for Modeled Multicast Elements (see page 19)

Multiple Users Are Not Receiving Multicast Traffic

Symptom:

At the same time each day, a single multicast stream is started. Today the source is started, but none of the users are seeing the multicast traffic, and consequently the business application they use is not functioning.

Assume the following:

1. The customer has previously installed and configured Multicast Manager.
2. The customer has completed a discovery of their physical network.

3. The customer has completed a Multicast Discovery.
4. All multicast services have been modeled with CA Spectrum.

Solution:

1. Several users contact the network operator to report that they are not receiving their daily service information.
2. The operator brings up Multicast Manager in the OneClick console and does a search on "All Groups".
3. The results of the search are shown in the Contents panel and all groups have a red condition.
4. The operator examines the source for each group in the Information tab of the Component Detail panel.
5. The operator finds no errors; all sources are operating properly.
6. The operator checks the RP Router for each group.
7. The operator finds that the condition of one of the RP routers is red, indicating that it is down.
8. The operator searches through open trouble tickets and finds a trouble ticket for a router, which is the RP for the group in question.
9. The operator reboots the RP router and the alarm is cleared.
10. Multicast traffic is restored to the network. The operator confirms that the users have service and the trouble ticket is cleared.

More information:

Run On-Demand Multicast Discovery (see page 16)
Search for Modeled Multicast Elements (see page 19)
Group Search Results (see page 20)
Sources Subview (see page 28)
Rendezvous Point Router (see page 29)

A Threshold Violation Has Occurred

Symptom:

At 10:00 A.M., users stop receiving Multicast traffic, consequently, the business application needed by these users is not functioning.

Assume the following:

1. The customer has previously installed and configured Multicast Manager.
2. The customer has completed a discovery of their physical network.

3. The customer has completed a Multicast Discovery.
4. All multicast services have been modeled with CA Spectrum.
5. The performance monitor configuration has been set up to generate alarms when a performance threshold is violated.
6. The Multicast Manager Device Performance Alarms parameter must be set to Enable.

Solution:

1. Several users contact the network operator to report that their daily service information is broken.
2. The operator brings up Multicast Manager in the OneClick console and does a search on "All Groups".
3. One of the Groups shows an Orange condition, indicating a major alarm on one of the elements of the Group.
4. The operator checks each of the devices in the Group and finds an alarm on one of the routers. This alarm is also shown in the OneClick alarm console.
5. A trouble ticket is created. The operator begins troubleshooting the router issue and discovers that one of the interfaces on the router is dropping packets. This generated the alarm on the group model, because the traffic tracked by the performance monitor had fallen below the assigned threshold.
6. The operator resolves the port issue and closes the trouble ticket.
7. Multicast traffic is restored to the network.
8. The operator confirms that service has been restored with users.

More information:

Performance Analysis Configuration Subview (see page 13)
Run On-Demand Multicast Discovery (see page 16)
Search for Modeled Multicast Elements (see page 19)
Performance Analysis Configuration Subview (see page 25)

Index

N

P

R

S

T

U

V