Troubleshooting

Cisco Prime Infrastructure provides the following for sophisticated monitoring and troubleshooting of end-user network access.

The following sections describe some typical troubleshooting tasks:

Getting Help from Cisco

Prime Infrastructure provides helpful tools for network operators to connect to Cisco experts to diagnose and resolve problems. You can open support cases and track your cases from Prime Infrastructure. If you need help troubleshooting any problems, Prime Infrastructure allows you to:

- Connect with the Cisco Support Community to view and participate in discussion forums. See Launching the Cisco Support Community, page 21-1.
- Open a support case with Cisco Technical Support. See Opening a Support Case, page 21-2.

Launching the Cisco Support Community

You can use Prime Infrastructure to access and participate in discussion forums in the online Cisco Support Community. This forum can help you find information for diagnosing and resolving problems.

Note You must enter your Cisco.com username and password to access and participate in the forums.

To launch the Cisco Support Community:

Step 1 Choose **Operate > Alarms & Events**, click an alarm, then choose **Troubleshoot > Support Forum**.

Step 2 In the Cisco Support Community Forum page, enter additional search parameters to refine the discussions that are displayed.

Opening a Support Case

You can use Prime Infrastructure to open a support request and to track your support cases. Prime Infrastructure helps you gather critical contextual information to be attached to the support case, reducing the time it takes to create a support case.

Note To open a support case or access the Cisco Support Community, you must:

- Have a direct Internet connection on the Prime Infrastructure server
- Enter your Cisco.com username and password

To open a support case:

Step 1 Chose **Operate > Alarms & Events**, then hover your mouse over the IP address of the device on which the alarm occurred.

Step 2 From the device 360° view, click the **Support Request** icon.

Step 3 Enter your Cisco.com username and password.

Step 4 Click **Create**.

Prime Infrastructure gathers information about the device and populates the fields for which it can retrieve information. You can enter a Tracking Number that corresponds to your own organization's trouble ticket system.

Step 5 Click **Next** and enter a description of the problem.

By default, Prime Infrastructure enters information that it can retrieve from the device. Prime Infrastructure automatically generates the necessary supporting documents such as the technical information for the device, configuration changes, and all device events over the last 24 hours. You can also upload files from your local machine.

Step 6 Click **Create Service Request**.

Checking an End User's Network Session Status

When an end user calls the help desk, typically with a complaint that might not be very specific ("I can't log in" or "The network is really slow"), you will want to get an overall view of the user's current network session status, identify which individual session is associated with the problem, and examine the details for that session.

For example, how is the user attached to the network? Does this person have more than one endpoint (where an endpoint could be, for example, a laptop, desktop, iPad, iPhone, or Android)?

Before You Begin

This feature requires:

- Integration with an ISE server (to access endpoint information).
- Integration with LDAP (to display information about the end user).

To check an end user's network session status:

Step 1 In the system search field (see Search Methods, page A-15), enter the name of the user (or client) who is experiencing the issue. If there are multiple matches, select the correct username from the list of matches.

Step 2 Start the User 360° View (see Getting User Details from the User 360° View, page A-13).

The information that is available from this view typically includes current information about the end user and all of that user's current or recently ended network sessions.

Troubleshooting Authentication and Authorization

Using the User 360° View, you can identify possible problems with the end user's authentication and authorization for network access.

For example, there could be authentication problems (such as the user's password being rejected), or there could be authorization issues (such as the user being placed in a policy category such as "guest" or "quarantine" that might result in unexpected behavior).

Before You Begin

This feature requires integration with an ISE server.

To troubleshoot the network

Step 1 Open the User 360° View for that user and check the value in "Authorization Profile". This is a mnemonic string that is customer-defined, so it might not contain clear information (for example, "standard_employee" or "standard_BYOD" or "Guest").

Step 2 If this field is a link, click it to display information about the user's authorization profile. Based on this information:

- If the end user is associated with the appropriate policy category, this procedure is complete.
- If the end user is not associated with the appropriate policy category, you can hand off the problem (for example, to an ISE admin or help tech) or perform actions outside Prime Infrastructure to investigate why the user was placed in the current policy category (Authorization Profile).

Step 3 Check to see whether there are any indications of authentication errors (authentication failure could be due to various things, including an expired password). The visual indication of authentication errors allows you to see more data related to the authentication errors. At that point, you might need to hand off the problem (for example, to an ISE admin or help tech).

Troubleshooting Network Attachments

Use the following procedure to determine if there are problems with the end user attaching to the network, such as errors on the access port (wired) or radio association problems (wireless).

To troubleshoot network attachments:

Step 1 Open the User 360° View for that user and click the **Go to Client Details** icon (see Getting User Details from the User 360° View, page A-13).

Step 2 If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note the problem and hand it off to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose **Operate > Client and Users**).

Troubleshooting Network Attachment Devices

Use the following procedure to troubleshoot any active alarms or error conditions associated with the network attachment device and port for the end user that might be causing problems for the end user's network session:

Step 1 To view any existing active alarms or error conditions associated with the network attachment device and port for the end user (available for the controller, switch, access point, and site), open the User 360° View for that user and click the **Alarms** tab.

Step 2 To see if a problem has been detected, click the **Go to Client Details** icon (see Getting User Details from the User 360° View, page A-13).

Step 3 If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note that fact and hand off the task to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose **Operate > Client and Users**).

Troubleshooting Site Network Devices

Use the following procedure to determine if there are any existing active alarms or error conditions associated with any of the network devices that are part of the site for the end user that could be causing problems for the user's network session.

Step 1 To view any existing active alarms or error conditions associated with network devices that are part of the site for the end user, open the User 360° View for that user and click the **Alarms** tab.

Step 2 You can choose to view:

- Active alarms list for the site
- List of all site devices (with alarm indications)
- Topo map of site (with alarm indications)

Step 3 If a problem with a site has been detected, an alarm icon will appear next to the site location. Click the icon to view all of the alarms associated with that site.

Step 4 If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note that fact and hand off the task to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose **Operate > Client and Users**).

Troubleshooting Applications

Use the following procedure to determine if there are any problem indications associated with any of the specific applications being run across the network by the end user.

Before You Begin

This feature requires:

- Integration with an ISE server (to access endpoint information).
- That session information (netflow/NAM data, Assurance licenses) is available.

Step 1 To view the applications accessed by the end user and the response time for the applications for the user's devices, open the User 360° View for that user and click the **Applications** tab.

Step 2 This tab displays the following information:

- Endpoint
- Mac address
- Application
- Last one hour volume (in MB)

To get more information about an application, choose **Operate > Monitoring Dashboards > Detail Dashboards**.

Troubleshooting the User Application and Site Bandwidth Utilization

If an end user is experiencing high bandwidth utilization for a site on the interface dashboard, use the following procedure to identify the applications consumed by the user and the bandwidth consumed by every application for a given endpoint owned by the user.

Before You Begin

This feature requires:

- Integration with an ISE server (to access endpoint information).
- For wired sessions, that AAA accounting information is being sent to ISE.
- That session information (netflow/NAM data, Assurance licenses) is available.

Step 1 To view the applications accessed by the end user and the response time for the applications for the user's devices, open the User 360° View for that user and click the **Applications** tab.

Step 2 The Applications tab displays information about the applications accessed by the end user (see Troubleshooting Applications, page 21-5). To get more information about an application, including the bandwidth utilization of the application consumed by the end user (the bandwidth consumed for the conversation), choose **Operate > Monitoring Dashboards > Detail Dashboards**.

Troubleshooting User Problems

You can use the User 360° View to troubleshoot problems reported by users.

Step 1 In the Search field on any page, enter the end user's name.

Step 2 In the Search Results window, hover your mouse over the end user's name in the User Name column, then click the User 360° view icon that appears as shown in Figure A-12.

Step 3 With the User 360° view displayed, identify where the problem is occurring using the information described in Table 21-1.

Table 21-1 Using the User 360° View to Diagnose User Problems

To Gather This Data	Click Here in User 360° View	Additional Information
Information about the device to which the user is attached, such as the endpoint, location, connections, and session information	Click a device icon at the top of the User 360° View.	Click available links to display additional information. For example, you can click the Authorization Profile link to launch ISE. See Troubleshooting Authentication and Authorization, page 21-3
Alarms associated with the device to which the user is attached	Click a device icon at the top of the User 360° View, then click the **Alarms** tab.	Click the Troubleshoot Client icon to go to client troubleshooting. See "Client Troubleshooting" in the *Cisco Prime Infrastructure Classic View Configuration Guide for Wireless Devices, Release 2.0*.
Applications running on the device to which the user is attached	Click a device icon at the top of the User 360° View, then click the **Applications** tab.	Click an application to view the end-user data filtered for the user you specified. See Troubleshooting Applications, page 21-5.

Troubleshooting the User's Experience

If an end user reports a problem with accessing the application, use the User 360° View to troubleshoot the user's experience.

Before You Begin

This feature requires that session information (netflow/NAM data, Assurance licenses) is available.

Step 1 To view the applications accessed by the end user and the response time for the applications for the user's devices, open the User 360° View for that user and click the **Applications** tab.

Step 2 The Applications tab displays information about the applications accessed by the end user (see Troubleshooting Applications, page 21-5). To get more information about an application, choose **Operate > Monitoring Dashboards > Detail Dashboards**.

Troubleshooting Voice/Video Delivery to a Branch Office

To successfully diagnose and resolve problems with application service delivery, network operators must be able to link user experiences of network services with the underlying hardware devices, interfaces, and device configurations that deliver these services. This is especially challenging with RTP-based services like voice and video, where service quality, rather than gross problems like outages, impose special requirements.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

Prime Infrastructure with the licensed Assurance features makes this kind of troubleshooting easy. The following workflow is based on a typical scenario: The user complains to the network operations desk about poor voice quality or choppy video replay at the user's branch office. The operator first confirms that the user is indeed having a problem with jitter and packet loss that will affect the user's RTP application performance. The user further confirms that other users at the same branch are also having the same problem. The operator next confirms that there is congestion on the WAN interface on the edge router that connects the local branch to the central voice/video server in the main office. Further investigation reveals that an unknown HTTP application is using a high percentage of the WAN interface bandwidth and causing the dropouts. The operator can then change the unknown application's DSCP classification to prevent it from stealing bandwidth.

Step 1 Choose **Operate > Details Dashboards > End User Experience**.

Step 2 Next to **Filters**, specify:

- The IP address of the **Client** machine of the user complaining about poor service.
- The **Time Frame** during which the problem occurred.
- The ID of the problem **Application**.

Click **Go** to filter the Detail Dashboard information using these parameters.

Step 3 View **RTP Conversations Details** to see the Jitter and Packet Loss statistics for the client experiencing the problem.

Step 4 View the **User Site Summary** to confirm that other users at the same site are experiencing the same issue with the same application.

Step 5 In the **User Site Summary**, under Device Reachability, hover the mouse over the branch's edge router. Prime Assurance displays a 360 View icon for the device under the Device IP column. Click the icon to display the 360° View.

Step 6 In the 360° View, click the **Alarms** tab, to see alarms on the WAN interfaces, or on the Interfaces tab, to see congested WAN interfaces and the top applications running on them.

Troubleshooting Unjoined Access Points

When a lightweight access point initially starts up, it attempts to discover and join a wireless LAN controller. After joining the wireless controller, the access point updates its software image if needed and receives all of the configuration details for the device and network. Until the access point

successfully joins a wireless controller, it cannot be managed by Prime Infrastructure, and it does not contain the proper configuration settings to allow client access. Prime Infrastructure provides you with a tool that diagnoses why an access point cannot join a controller, and lists corrective actions.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

The Unjoined AP page displays a list of access points that have not joined any wireless controllers. All gathered information about the unjoined access point is included on the page. This information includes name, MAC address, IP address, controller name and IP address, switch and port that the access point is attached to, and any join failure reason, if known.

To troubleshoot unjoined access points:

Step 1 Choose **Operate > Wireless > Unjoined APs**.

Step 2 In the Unjoined APs page, select an access point to diagnose, then click **Troubleshoot**.

Step 3 After the troubleshooting analysis runs, check the results in the Unjoined APs page.

If the access point has tried to join multiple wireless controllers but has been unsuccessful, the controllers are listed in the left pane.

Step 4 Select a controller and check the middle pane for:

- A statement of the problem
- A list of error messages
- Controller log information

Step 5 Check the right pane for recommendations for solving any problems, and perform any recommended actions.

Step 6 (Optional) To further diagnose the problem, run RTTS through the Unjoined AP page by clicking the RTTS icon located to the right of the table. Examine the debug messages that appear in the table to determine a cause for the access point being unable to join the controllers.

RTTS Debug commands for Troubleshooting Unjoined Access Points

Table 21-2 contains the list of RTTS debug commands for Legacy controllers and NGWC controllers.

Table 21-2 RTTS Debug commands for Legacy controllers and NGWC controllers

Controller	Commands
Legacy	• debug capwap info enable • debug dot1x all enable • debug mobility directory enable
NGWC	• debug capwap ap error • debug dot1x events • debug capwap ios detail

Troubleshooting RTP and TCP Flows Using Mediatrace

The Mediatrace troubleshooting tool generates a table that lists the currently active RTP streams or TCP sessions. Using these Mediatrace tables and their associated options, you can:

- Identify and select RTP or TCP flows with problems (see Using the Mediatrace Tables, page 21-10).
- Troubleshoot problems with RTP or TCP flows (see Running Mediatrace from Selected RTP or TCP Flows, page 21-11).
- Troubleshoot problems with RTP or TCP flows between any two arbitrary endpoints (see Launching an Ad Hoc Mediatrace From Endpoints, page 21-12).
- Troubleshoot problems with RTP flows starting from the RTP Conversations dashlet (see Troubleshooting Worst RTP Endpoints Using Dashlets, page 21-14).
- Identify and compare flow performance indicators and data sources (see Comparing Flow Data From Multiple Sources, page 21-15).

To configure data collection for Mediatrace, see Managing Metrics in the *Cisco Prime Infrastructure 2.0 Administrator Guide*.

Using the Mediatrace Tables

The flow information shown in the RTP Streams and TCP Sessions tables is collected and aggregated from NAM and NetFlow data generated throughout the network.

Many rows in the RTP Streams table are arranged in a tree hierarchy. This will occur whenever an RTP application flow involves more than one data stream. In these cases, the flows between the two application endpoints are aggregated into a single row with a triangle icon.

By default, Prime Infrastructure automatically refreshes the RTP Streams table data every 60 seconds; you can also use one of the preset filters.

Prime Infrastructure refreshes TCP Sessions data once every 300 seconds (5 minutes); you can use the **Filter by Application** filtering option to include or exclude applications from the list.

You can also click either table's **Refresh** button at any time. You can turn off automatic refresh by unchecking the **Enable auto refresh** check box.

To use the Mediatrace tables:

Step 1 Choose **Operate > Operational Tools > Mediatrace**.

Step 2 From the **Application** drop-down list, choose **RTP** or **TCP**. The page shows the corresponding table: RTP Streams or TCP Sessions.

Step 3 Find the flow that you want to troubleshoot:

- To review all flows with a particular type of issue, click the appropriate column heading to sort on that column.

  For example, if you are monitoring RTP performance across the network and want to see the streams with the worst jitter or packet loss, click the Jitter or Packet Loss column headings to sort the streams on these performance indicators. You can then select any of the streams for troubleshooting.

- To find a particular flow with a problem, click the **Quick Filter** icon and enter a filter criterion under one or more row headings.

  For example, an end user having trouble accessing an application might report the IP address and the name of that application. You can do a quick filter on the TCP table for either the Client IP address or Application ID, then select that session for troubleshooting.

- To spot issues in RTP subflows, click the triangle icon next to any aggregated RTP flow.

  For example, an RTP voice/video flow between any two endpoints will appear in the RTP Streams table as a single flow with a triangle icon. Clicking the icon will show you the four subflows: an incoming and outgoing video subflow, and an incoming and outgoing voice subflow.

Step 4 To troubleshoot the flow, see Running Mediatrace from Selected RTP or TCP Flows, page 21-11.

Running Mediatrace from Selected RTP or TCP Flows

To troubleshoot RTP or TCP flows using Mediatrace:

Step 1 Choose **Operate > Operational Tools > Mediatrace**. In the **Application** drop-down list, choose **RTP** or **TCP**, then find the flow that you want by using the steps in Using the Mediatrace Tables, page 21-10.

Step 2 Select the flow and click **Trace Service Path**. Prime Infrastructure displays the RTP or TCP Stream Details page for the selected flow, with all of the routers in the flow's path in the Troubleshooting Status table, in the order of their distance from the flow's source endpoint. Routers that are Medianet-capable are indicated by a filmstrip icon.

Step 3 To run Mediatrace or Traceroute from a router in the flow's path, click the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

Note The **Start Mediatrace** link is present when the device is Mediatrace-capable; the **Start Traceroute** link is present when the device is not Mediatrace-capable.

Mediatrace can take a minute or more to run, depending on traffic, congestion, and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:

- The progress of the operation.

- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where non-Medianet-capable routers where encountered and how they were processed.
- Medianet-capable routers on which Medianet is not configured.

Step 4 When the operation is complete, the Troubleshooting tab displays a topology map of all of the devices between the flow's two endpoints. Device icons in the map consist of:

- Alarm Severity—The most severe alarm currently recorded for the device.
- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign on red background—The device is Medianet-capable but not configured as a Medianet responder. RTP/TCP performance statistics will not be available for the device. To remedy this situation, you must configure the device as a Medianet responder as explained in Troubleshooting RTP and TCP Flows Using Mediatrace, page 21-10.
- Minus sign—The device is unmanaged.

Step 5 To see key performance metrics, such as CPU and memory utilization, jitter, and packet loss, for all Medianet-capable devices in the RTP or TCP flow's path, click the **Medianet Path View** tab. To see the performance metrics in numerical and graphic form, click the subtabs in the Medianet Path View pane.

Note The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

Step 6 Use the appropriate links in the Troubleshooting Status table to:

- Launch a Mediatrace or Traceroute operation on a different router.
- Restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Launching an Ad Hoc Mediatrace From Endpoints

You can quickly launch a Mediatrace against all RTP or TCP flows between any two endpoints in the network. This can include either specific flows running between any two endpoints on the same or different sites, or between a pair of routers on two different sites.

This is handy if your network lacks NAM monitoring, or when you are in a hurry and you know at least the IP addresses of the two endpoints of the RTP or TCP flow. You must still navigate to and start the trace from the appropriate RTP or TCP Mediatrace table.

To launch an ad hoc Mediatrace from two endpoints:

Step 1 Choose **Operate > Operational Tools > Mediatrace**. From the **Application** drop-down list, choose **RTP** or **TCP**.

Step 2 Click **Specify Session for Mediatrace**.

Step 3 Enter the required information:

- For an RTP flow:

  - Select the Source Site.
  - Enter the Source Endpoint IP address.
  - Enter the Destination EndPoint IP address.
- For a TCP flow:
  - Select the Client Site.
  - Enter the Client Endpoint IP address.
  - Enter Server Endpoint IP address.

Step 4 Provide any additional endpoint information that you have:

- For an RTP flow, select or enter the Source Endpoint Port and Destination Endpoint Port.
- For a TCP flow, select or enter the Server Endpoint Port.

Step 5 Click **Trace Service Path** (for an RTP flow) or **OK** (for a TCP flow). Prime Infrastructure displays the RTP or TCP Stream Details page for the specified flow, with all of the routers in the flow's path in the Troubleshooting Status table, in the order of their distance from the flow's source or client endpoint. Routers with a "filmstrip" icon next to them are Medianet-capable.

Step 6 To run Mediatrace or Traceroute from a router in the flow's path, click the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

Mediatrace can take a minute or more to run, depending on traffic, congestion, and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:

- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where and how non-Medianet-capable routers where encountered and processed.
- Medianet-capable routers on which Medianet is not configured.

Step 7 When the operation is complete, the Troubleshooting tab displays a topology map of the all the devices between the flow's two endpoints. Device icons in the map will be badged as follows:

- Alarm Severity—The most severe alarm currently recorded for the device.
- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign on red background—The device is Medianet-capable but not configured as a Medianet responder. RTP/TCP performance statistics will not be available for the device. To remedy this situation, you must configure the device as a Medianet responder.
- Minus sign—The device is unmanaged.

Step 8 To see key performance metrics for all Medianet-capable devices in the flow's path, click the **Medianet Path View** tab. Click the subtabs in the Medianet Path View panel to see the performance metrics in numerical and graphic form.

Note The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

Step 9 Use the appropriate links in the Troubleshooting Status table to launch a Mediatrace or Traceroute operation on a different router, restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Troubleshooting Worst RTP Endpoints Using Dashlets

You can quickly launch a Mediatrace against the poorest performing RTP flows in your network using the Worst N RTP End Point Pairs. and RTP Conversation dashlets. This works only for RTP flows.

The RTP Conversations dashlet shows the complete history for a source endpoint, including flows that are no longer active. You will want to select only the most recent flows. If you launch Mediatrace on such an inactive flow, you will receive an error message advising you of this fact.

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards > End User Experience**.

Step 2 In the **Worst N RTP End Point Pairs** dashlet (if this dashlet is not already in the dashboard, see Adding Dashlets, page A-4), note the Source Address for your worst performing RTP flows.

Step 3 In the **RTP Conversations** dashlet in the same page, find the most recent conversation for the same Source Address.

Step 4 Select that conversation in the RTP Conversations dashlet, then choose **Troubleshoot > Trace Service** path. Prime Infrastructure displays the RTP Stream Details page for the selected flow, with all of the routers in the flow's path in the Troubleshooting Status table, in order of their distance from the flow's source endpoint. Routers that are Medianet-capable are indicated by a filmstrip icon.

Step 5 To run Mediatrace or Traceroute from a router in the flow's path, click the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

Note The **Start Mediatrace** link is present when the device is Mediatrace-capable; the **Start Traceroute** link is present when the device is not Mediatrace-capable.

Mediatrace can take a minute or more to run, depending on traffic, congestion, and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:

- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where and how non-Medianet-capable routers where encountered and processed.
- Medianet-capable routers on which Medianet is not configured.

Step 6 When the operation is complete, the Troubleshooting tab displays a topology map of the all of the devices between the flow's two endpoints. Device icons in the map will be badged as follows:

- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign—The device is unmanaged.

Step 7 To see key performance metrics for all Medianet-capable devices in the flow's path, click the **Medianet Path View** tab. To see the performance metrics in numerical and graphic form, click the subtabs in the Medianet Path View panel.

Note The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

Step 8 Use the appropriate links in the Troubleshooting Status table to:

- Launch a Mediatrace or Traceroute operation on a different router.
- Restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Comparing Flow Data From Multiple Sources

When interpreting Mediatrace performance data, you might find it helpful to:

- Identify the NAM, NetFlow, and other sources reporting this performance data.
- If you have multiple NAM or NetFlow data sources, compare how those sources are reporting key performance indicators for a particular flow.

To compare flow data from multiple sources:

Step 1 Choose **Operate > Operational Tools > Mediatrace**.

Step 2 From the **Application** drop-down list, choose **RTP** or **TCP**, then find the flow you want using the steps in Using the Mediatrace Tables, page 21-10.

Step 3 Expand a row (for an RTP or TCP flow) to view the details of the key performance indicators appropriate for the selected flow and the data source for each such set of indicators.

Step 4 When you are finished, click **OK**.