Manage Traffic Metrics

How to Manage Traffic Metrics

> **Note** The mediatrace feature has been deprecated from the latest IOS releases.

supports tracing Real-Time Transport Protocol (RTP) and TCP application traffic paths across endpoints and sites. Tracing data paths depends on Cisco Medianet and Web Services Management Agent (WSMA). Both are built-in features of Cisco IOS software and Catalyst switches that help isolate and troubleshoot problems with RTP and TCP data streams. supports all versions of Cisco Medianet and WSMA and makes it easy to enable them on any router.

Where Cisco Network Analysis Module (NAM) traffic monitoring data is not available, supports RTP service path tracing (Mediatrace) using Cisco Medianet Performance Monitor and Cisco IOS NetFlow. When properly configured, Mediatrace can be your most valuable tool when troubleshooting RTP and TCP application problems.

Related Topics

Prerequisites for Traffic Metrics With Mediatrace, on page 1
Configure Mediatrace on Routers and Switches, on page 3
Configure WSMA and HTTP(S) Features on Routers and Switches, on page 3

Prerequisites for Traffic Metrics With Mediatrace

Before you can use Mediatrace feature, you must complete the prerequisite setup tasks shown under Related Topics, below. These prerequisite tasks are required to enable Cisco routers (ISRs, ISR G2s, ASRs) and NAM devices to act as data (metrics collection) sources to monitor network traffic (RTP and TCP) performance metrics.

Related Topics

Configure to Use NAM Devices as Data Sources, on page 2
Configure to Use Routers and Switches as Data Sources, on page 2

Configure to Use NAM Devices as Data Sources

If your network uses Cisco NAMs to monitor network traffic, complete the following steps to trace service paths for both RTP and TCP traffic.

Step 1 Add NAMs to the system. You can do this either automatically using Discovery, or manually using bulk import or the Device Work Center (see the section *Add and Organize Devices* in Cisco Prime Infrastructure User Guide).

Step 2 Enable NAM Data collection. To do this:

a) Choose **Services** > **Application Visibility & Control** > **Data Sources.**

b) In the NAM Data Collector section, select each NAM and click **Enable** to enable data collection on the selected NAMs (see the section *Enable NAM Data Collection* in Cisco Prime Infrastructure User Guide).

Step 3 Create a site structure for your organization and assign your principal routers to the appropriate sites:

a) Choose **Maps** > **Site Maps**.

b) Add one or more campuses, buildings, and floors.

Step 4 Associate your sites with authorized data sources:

a) Choose **Services** > **Application Visibility & Control** > **Data Deduplication**.

b) Click **Enable Data Deduplication**, then click **Apply**. You can then assign authoritative sources for ART, Traffic Analysis and Voice/Video data (see Enable Data Deduplication).

Step 5 Associate your sites with endpoint subnets:

a) Choose **Services** > **Application Visibility & Control** > **Endpoint Association**.

b) Associate subnets with your sites. (see the section *Associate Endpoints with a Site* inCisco Prime Infrastructure User Guide).

If you fail to do this, the data collected for these endpoints will have their sites set to “Unassigned.”

Step 6 Configure your routers for Mediatrace and WSMA (see the section *Troubleshoot RTP and TCP Flows Using Mediatrace* in Cisco Prime Infrastructure User Guide).

For more details, see Control System Jobs".

Configure to Use Routers and Switches as Data Sources

If your network uses Cisco routers and switches to monitor network traffic, complete the following steps to enable path tracing for both RTP and TCP flows.

Step 1 Create a site structure for your organization and assign your principal routers to the appropriate sites:

a) Choose **Maps** > **Site Maps**.

b) Add one or more campuses, buildings, and floors (for details, see the section *Work With Site Maps* in Cisco Prime Infrastructure User Guide).

Step 2 Associate your sites with authorized data sources:

a) Choose **Services** > **Application Visibility & Control** > **Data Deduplication**.

b) Click **Enable Data Deduplication**, then click **Apply**. You can then assign authoritative sources for ART, Traffic Analysis and Voice/Video data (see Enable Data Deduplication).

Step 3 Associate your sites with endpoint subnets:

a) Choose **Services > Application Visibility & Control > Endpoint Association**.

b) Associate subnets with your sites. (see the section *Associate Endpoints with a Site* in Cisco Prime Infrastructure User Guide).

If you fail to do this, by default the data collected for these endpoints will have their sites set to “Unassigned.”

Step 4 Configure your compatible routers for Cisco Medianet Performance Monitor (see Configure Mediatrace on Routers and Switches).

Step 5 Configure your routers for Mediatrace and WSMA (see the section *Troubleshoot RTP and TCP Flows Using Mediatrace* in Cisco Prime Infrastrucute User Guide).

Related Topics

Enable Data Deduplication

Configure Mediatrace on Routers and Switches

supplies an out-of-the-box template that configures Mediatrace on routers and switches. You must apply this configuration to every router and switch that you want to include in your results whenever you are tracing service paths.

See Deploying Templates , to get a list of all the supported routers and switches for Mediatrace.

Before You Begin

You must complete the following tasks:

- Configuring to Use NAM Devices as Data Sources
- Configuring to Use Routers and Switches as Data Sources

To configure the Mediatrace-Responder-Configuration template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Mediatrace -Responder-Configuration**.

Step 2 Enter the required information for the template (see the Field reference for the template).

Step 3 Click **Save as New Template** and give the new template a name and description. Click **Save**.

Step 4 Click **Deploy** to deploy the new template .

For more details, see Enabling NetFlow Data Collection, Field Reference: Mediatrace-Responder-Configuration and Deploying Templates .

Configure WSMA and HTTP(S) Features on Routers and Switches

To trace service path details, the Web Services Management Agent (WSMA) over HTTP protocol must run Mediatrace commands on your routers and switches. Configure this feature on the same set of routers and switches as you did when following the instructions in “Configure Mediatrace on Routers and Switches” (see Related Topics).

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies** > **CLI Templates** > **System Templates - CLI** > **HTTP-HTTPS Server and WSMA Configuration-IOS**.

Step 2 Enter the required information for the template (see the Field reference for the template.

Be sure to enable the HTTP protocol. WSMA over HTTPS is *not supported* in the current version of Prime Infrastructure.

Step 3 Click **Save as New Template** and give the new template a name and description. Click **Save**.

Step 4 Click **Deploy** to deploy the new template.

When adding a device to Prime Infrastructure, you must provide the HTTP user and password for the device.

For more details, see Field Reference: HTTP-HTTPS Server and WSMA Configuration-IOS, Deploying Templates and Add Devices to Prime Infrastructure .

Related Topics

Configure Mediatrace on Routers and Switches, on page 3