System Performance Monitoring

- Predefined System Objects, on page 1
- Voice and Video Monitoring, on page 3
- Intercompany Media Services, on page 28
- IM and Presence Monitoring, on page 30
- Cisco Unity Connection Monitoring, on page 35

Predefined System Objects

Unified RTMT displays information about predefined system objects in the monitoring pane.

Tip The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the Alert Manager and Collector (AMC) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application (not the back-end server) time provides the basis for the time stamp in each chart.

For information about service parameters, see the administration online help.

Tip To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart in which you are interested. Release the left mouse button when you have the selected area. RTMT updates the monitored view. To zoom out and reset the monitor to the initial default view, press the **R** key.

The following table provides information about the predefined objects that RTMT monitors.

Table 1: System Categories

Category	Description
System Summary	Displays information about Virtual Memory usage, CPU usage, Common Partition Usage, and the alert history log. To display information about predefined system objects, choose **System** > **System Summary**.

Category	Description
Server	• CPU and Memory: Displays information about CPU usage and Virtual memory usage for the server. To display information about CPU and Virtual memory usage, choose **System** > **Server** > **CPU and Memory**.To monitor CPU and memory usage for specific server, choose the server from the host drop-down list box. • Process: Displays information about the processes that are running on the server. To display information about processes running on the system, choose **System** > **Server** > **Process**. To monitor process usage for specific server, choose the server from the Host drop-down list box. • Disk Usage: Displays information about disk usage on the server. To display information about disk usage on the system, choose **System** > **Server** > **Disk Usage**. To monitor disk usage for specific server, choose the server from the host drop-down list box. • Critical Services: Displays the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services existed in a particular state for the server or for a particular server in a cluster (if applicable). To display information about critical services, choose **System** > **Server** > **Critical Services**, then click the applicable tab: • To display system critical services, click the **System** tab. • To display Unified Communications Manager critical services, click the **Voice/Video** tab. **Note** You can view the Voice/Video tab only if you select a Unified Communications Manager server from the host drop-down list box. • To display IM and Presence Service critical services, click the **IM and Presence** tab. **Note** You can view the IM and Presence tab only if you select an IM and Presence Service server from the host drop-down list box. • To display Cisco Unity Connection critical services, click the **Cisco Unity Connection** tab. • To monitor critical services for specific server on the tab, choose the server from the host drop-down list box and click the critical services tab in which you are interested. If the critical service status indicates that the administrator stopped the service, the administrator performed a task that intentionally stopped the service; for example, the service stopped because the administrator backed up or restored Unified Communications Manager; performed an upgrade; or stopped the service in Cisco Unified Serviceability or the CLI. **Note** If the critical service status displays as unknown state, the system cannot determine the state of the service.

Voice and Video Monitoring

Predefined Cisco Unified Communications Manager Objects

Unified RTMT displays information about predefined Unified Communications Manager objects in the monitoring pane when you select Voice/Video in the quick launch channel. The tool monitors the predefined objects on all servers in an cluster, if applicable.

Tip The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the Unified RTMT client application and not the backend server time, provides the basis for the time stamp in each chart.

For more information about service parameters, see the *System Configuration Guide for Cisco Unified Communications Manager* or *Cisco Unity Connection System Administration Guide*.

Tip To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart in which you are interested. Release the left mouse button when you have the selected area. Unified RTMT updates the monitored view. To zoom out and reset the monitor to the initial default view, press the **R** key.

The following table provides information about the predefined object that Unified RTMT monitors.

Table 2: Cisco Unified Communications Manager Categories

Category	Description
Voice and Video Summary	Displays registered phones, calls in progress, and active MGCP ports and channels. To display information about predefined Unified Communications Manager objects, choo **Voice/Video** > **Voice and Video Summary**.

Category	Description
Call Process	• Call Activity: Displays the call activity on Unified Communications Manager, including completed, calls attempted, calls in progress, and logical partition total failures. This incl all servers in the cluster, if applicable. To display information about call activities, choose **Voice/Video** > **Call Process** > **Call Activity**. • Gateway Activity: Displays gateway activity on Unified Communications Manager, inclu active ports, ports in service, and calls completed. This includes all servers in the cluster applicable. To display information about gateway activities, choose **Voice/Video** > **Call Process** > **Gateway Activity**. Select the type of gateway interface from the **Gateway Type** drop-d list. • Trunk Activity: Displays the trunk activity on Unified Communications Manager, includ calls in progress and calls completed. This includes all servers in the cluster, if applicabl To display information about trunk activities, choose **Voice/Video** > **Call Process** > **Tru Activity**. Select the trunk type in the **Trunk Type** drop-down list. • SDL Queue: Displays SDL queue information, including number of signals in queue an number of processed signals. To display information about the SDL Queue, choose **Voice/Video** > **Call Process** > **SD Queue**. Select the type from the **SDL Queue Type** drop-down list. • SIP Activity: Displays SIP activity on Unified Communications Manager, including sum requests, summary responses, summary of failure responses in, summary of failure respo out, retry requests out, and retry responses out. This includes all servers in the cluster, if applicable. To display information about SIP activities, choose **Voice/Video** > **Call Process** > **SIP Acti**
Session Trace	Displays all SIP message activity: specifically, the incoming and outgoing calls and sessions pass through the Unified Communications Manager. Provides associated call flow diagram for SIP transaction. To display information about Session Trace, choose **Voice/Video** > **Call Process** > **Session Tr**
Device	Device Summary displays information about the Unified Communications Manager server, inclu the number of registered phone devices, registered gateway devices, registered other station dev and registered media resource devices. This includes all servers in the cluster, if applicable. Device Search displays cluster name and device types in a tree hierarchy and allows you to q for information about phones and devices. Phone Summary displays information about the Unified Communications Manager server, inclu the number of registered phones, registered SIP phones, registered SCCP phones, partially regis phones, and the number of failed registration attempts. This includes all servers in the cluster applicable. To display information about the number of registered phones, gateways, and media resource devices on Unified Communications Manager, choose **Voice/Video** > **Device** > **Device Summ** **Tip** To monitor other devices, you must perform additional configuration steps.

Category	Description
Service	• Cisco TFTP: Displays Cisco TFTP status on the Unified Communications Manager including total TFTP requests and total TFTP requests aborted. This includes all serv the cluster, if applicable. To display information about the Cisco TFTP service, choose **Voice/Video** > **Service TFTP**. • Heartbeat: Displays heartbeat information for the Unified Communications Manager TFTP service. To display the heartbeat status of Unified Communications Manager servers, Cisco T servers, choose **Voice/Video** > **Service** > **Heartbeat**. • Database Summary: Provides connection information for the server, such as the char notification requests that are queued in the database, change notification requests tha queued in memory, the total number of active client connections, the number of replic have been created, and the status of the replication. To display information about the database, choose **Voice/Video** > **Service** > **Databa Summary**.
CTI	Displays information about the devices and applications that interfaces with the CTI Man To display information about CTI Applications, choose **Voice/Video** > **CTI** > **CTI Mana** To monitor specific CTI types, you must perform additional configuration steps. See topic to monitoring CTI applications, devices, and lines.
Intercompany Media Services	• Routing: Displays the total number of Cisco Intercompany Media Engine routes mai by Unified Communications Manager. To display information about call activities, choose **Voice/Video** > **Intercompany M Services** > **Routing**. • Call Activities: Displays the Cisco Intercompany Media Engine call activity, includi number of calls that were accepted, busy, no answer, and failed. To display information about call activities, choose **Voice/Video** > **Intercompany M Services** > **Call Activities**.

Cisco Unified Communications Manager Summary View

In a single monitoring pane, Unified RTMT allows you to monitor information about a Unified Communications Manager server or about all servers in a cluster (if applicable). In the CallManager Summary window, you can view information about the following predefined objects:

- Registered Phones
- Calls in Progress
- Active Gateway, Ports, and Channels

Call-Processing Activity Monitoring

The Call Process monitoring category monitors the following items:

- Call Activity: You can monitor the number of attempted calls, completed calls, in-progress calls, and logical partition total failures for a particular server or for an entire cluster (if applicable).
- Gateway Activity: You can monitor gateway activity for each gateway type. Gateway activity monitoring includes the number of active ports, the number of ports in service, and the number of calls that were completed for each gateway type for a particular server or for an entire cluster (if applicable).
- Trunk Activity: The system monitors trunk activity by trunk type for a particular server or for an entire cluster (if applicable). Trunk activity monitoring includes the number of calls in progress and the number of calls that were completed for a particular trunk type.
- SDL Queue: SDL queue monitoring monitors the number of signals in the SDL queue and the number of signals that were processed for a particular signal distribution layer (SDL) queue type. The SDL queue types comprise high, normal, low, and lowest queue. You can monitor the SDL queue for a particular server or for an entire cluster (if applicable).
- SIP Activity: The system displays a summary of SIP requests, SIP responses, total number of failed incoming responses (4xx, 5xx, and 6xx), total number of failed outgoing responses (4xx, 5xx, and 6xx), number of retry requests, and number of retry responses.
- Session Trace: You can search or trace the calls based on the following criteria: Calling Number/URI, Called Number/URI, Start Time, and Duration. RTMT downloads the Call Log file(s) that include the Start Time and Duration, search for the matching calls, list the matching call records, and provide the Call Flow Diagram.

The following table provides information about the call processing objects that RTMT monitors, the alert, thresholds, and defaults. For information about call activity daily reports, see the *Cisco Unified Serviceability Administration Guide*.

Table 3: Call Processing Category

Monitored Objects (displayed)	Alert/Threshold/Default
CallsAttempted, CallsCompleted, CallsInProgress, and Logical Partition Failures Total for each server and cluster (if applicable).	—
CallsAttempted, CallsCompleted, and CallsInProgress of each type of MGCP FXS/FXO/PRI/T1CAS/H.323 gateway, as well as SIP and H.323 Trunks for each server and cluster (if applicable).	—
Channel/Port Status of each MGCP FXS/FXO/PRI/T1CAS gateway.	—
SDL Queue activity on each server.	—

Monitored Objects (displayed)	Alert/Threshold/Default
MGCP FXS Gateway: Number of In-Service and Active ports for each server and cluster (if applicable).	Route-List exhausted
MGCP FXO Gateway: Number of In-Service and Active ports for each server and cluster (if applicable).	Route-List exhausted
MGCP PRI Gateway: Number of In-Service and Active channels for each server and cluster (if applicable).	• D-Channel out of service • Route List exhausted
MGCP T1CAS Gateway: Number of In-Service and Active ports for each server and cluster (if applicable).	Route List exhausted

Call-Processing Logs

The system accumulates call-processing data in the memory whenever Unified RTMT calls the LogCall API. Every 5 minutes, Unified RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every 5 minutes for the following counters on the basis of the following calculation:

- cmCallsAttempted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsInProgress: Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_CallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXO_CallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_PRI_CallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_T1_CAS_CallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsAttempted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsInProgress: Average of all the values that were collected in last 5 minutes
- gwH323_CallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkH323_CallsAttempted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)

- trunkH323_CallsInProgress: Average of all the values collected in last 5 minutes
- trunkH323_CallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsAttempted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsInProgress: Average of all the values that were collected in last 5 minutes
- trunkSIP_CallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXS_PortsInService: Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_PortsInService: Average of all the values that were collected in lasts 5 minutes
- gwMGCP_PRI_SpansInService: Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_SpansInService: Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_ActivePorts: Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_ActivePorts: Average of all the values that were collected in last 5 minutes
- gwMGCP_PRI_ActiveChannels: Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_ActiveChannels: Average of all the values that were collected in last 5 minutes

The AMC service logs the call data in windows Performance tool-compatible CSV format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for the server. These sets of columns repeat for every server in a cluster, if applicable.

The following filename format of the Call Log applies: CallLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log file comprises the header.

Perform Session Trace

Unified Communications Manager captures and logs all SIP message activities, which comprise the incoming and outgoing calls or sessions that pass through it. Unified Communications Manager stores the messages on a per-transaction basis in a new Call Log file, which can be downloaded through RTMT for postprocessing activity.

RTMT users can search or trace the calls based on the following criteria:

- Calling Number/URI
- Called Number/URI
- Start Time
- Duration

RTMT downloads the Call Log file that includes the Start Time and Duration. The tool searches for the matching calls, lists the matching call records, and provides the SIP message Call Flow Diagram.

You can also save the call logs on your local system. Based on the saved call logs, RTMT can search for the matching calls, list the matching records, and provide SIP Message Call Flow Diagrams.

Before you begin

Perform the following task:

- Use the enterprise parameter Enable Call Trace Log to enable or disable Call Tracing. For more information about configuring enterprise parameters, see the *System Configuration Guide for Cisco Unified Communications Manager* .
- The default value for maximum number of Call Trace log files specifies 2000 and the default value for maximum Call Trace log file size specifies 2MB.

Monitor Real-Time Data

Follow this procedure to monitor real-time data using RTMT.

Note You can search calls based on the following criteria: Calling Number/URI, Called Number/URI, Start Time, and Duration. The search applies to the entire Unified Communications Manager cluster, not just the local node. If any node fails to collect the trace files, the system displays an error message in the bottom panel and pops up the message prompt to the user.

Note In Calling Number/URI, Called Number/URI, you can use wildcard character "*" to match any number of characters. For example, a search for 123* fetches numbers like 123, 1234, or 123456.

If you want to search for numbers with a “*” in them, use “*”. For example, to search for a Called Number like 12*45, enter 12*45 in the search box.

Procedure

Step 1 To display information about Session Trace, from the RTMT menus, choose **Voice/Video** > **Call Process** > **Session Trace Log View** > **Real Time Data**.

The Real Time Data screen appears.

Step 2 Enter the search criteria and Click **Run**.

Click **Yes** to ignore the error and generate the table, based on the input.

If matching calls are found, the Matching Call pane displays Start Time, Calling DN, Original Called DN, Final Called DN, Calling Device Name, Called Device Name, and Termination Cause Code.

Note The Called Party Trace feature adds the Calling Device Name and Called Device Name fields.

- Calling and Called device names will not be available for failed calls such as calls made to unreachable destinations.
- The Termination Cause Code helps to identify the failed calls, and provides the reason for the failure of the calls. The Termination Cause Code is displayed in parenthesis followed by description.
- If the call is in progress or if the call trace logging is turned off after the call, the Termination Cause Code column remains blank.

After the call records are displayed in the Matching Calls pane, you can trace calls.

Note If cause code description is missing or if you want more information about the Termination Cause Codes, refer the CDR cause codes in *Cisco Unified Call Details Records Administration Guide*.

Monitor Session Trace Data From Local Disk

Follow this procedure to monitor session trace data from the logs that are saved on your local disk:

Procedure

Step 1 From the RTMT menus, choose **Voice/Video** > **Call Process** > **Session Trace Log View** > **Open from Local Disk**.

The Open from Local Disk screen appears.

Step 2 In the **File Location** field, specify the directory where the call log files are saved on your local disk. You can click **Browse** to specify the directory path.

Step 3 Check the **Enable Time Based Search** check box to view call records for a specific duration. If you check this check box, you can specify the duration in **Duration** field. If you do not check this check box, you will not be able to specify the duration. In such cases, all the calls from the specified Start Time that are present in the saved log files will be displayed.

Step 4 Enter the search criteria and click **Run.**

Note In Calling Number/URI, Called Number/URI, you can use the wildcard character '*' to match any number of characters. For example, a search for 123* fetches numbers like 123, 1234, 123456.

If you want to search for numbers with a '*' in them, use '*'. For example, to search for a Called Number like 12*45, enter 12*45 in the search box.

If matching calls are found, the Matching Call pane displays Start Time, Calling DN, Original Called DN, Final Called DN, Calling Device Name, Called Device Name, and Termination Cause Code.

Note The Called Party Trace feature adds the Calling Device Name and Called Device Name fields.

a) Calling and Called device names will not be available for failed calls such as calls made to unreachable destinations.
b) The Termination Cause Code helps to identify the failed calls, and provides the reason for the failure of the calls. The Termination Cause Code is displayed in parentheses followed by description.
c) If the call is in progress or if the call trace logging is turned off after the call, the Termination Cause Code column remains blank.

Note If cause code description is missing or if you want more information about the Termination Cause Codes, see the CDR cause codes in *Cisco Unified Call Details Records Administration Guide*.

Trace Calls

Follow this procedure to trace call records displayed as per the specified search criteria.

Note Use this procedure along with "Monitor real-time data" and "Monitor session trace data from local disk."

Procedure

Step 1 Select a call (a row) to trace.

By default, the **Include SIP Message** check box is selected to view the associated SIP protocol messages or call transactions.

Step 2 To generate the SIP Message Call Flow Diagram, click **Trace Call**. If you want to stop the generation of the session information, click **Cancel** on the progress window.

The **Analyze Call Diagram** window displays the corresponding SIP messages in the Call Flow Diagram.

Step 3 Click the tabs that you want to view. The following tabs are available:

a) Call Flow Diagram: Displays the corresponding SIP messages in the Call Flow Diagram.
b) Log File: Displays the entire log file.
c) SIP Message: Appears only when the **Include SIP Message** check box is checked. Displays the actual SIP message that is logged into the SDI log file.

Step 4 Move your mouse over the SIP messages in the Call Flow Diagram. The following table lists the details that are displayed:

Field	Description
Sender	Displays the IP address of the originating call.
GUID	Displays the SIP call ID.
Message Label	Displays the message type for the corresponding SIP message onto which you move your mouse; for example, 200 OK, or 180 Ringing.
Receiver	Displays the IP address of the destination call.
MAC_ADDRESS	Displays the name of the device.
Message Tag	Displays the sequence number to match the actual messages in the SDI Trace file.
MSG_TYPE	Displays the type of message.
Correlation ID	Displays the Correlation ID.
Timestamp	Displays the server time at which the call operation (call setup/split/join/release) happens.

Detailed SIP Message: Appears only when the Include SIP Message check box is checked. Displays the actual SIP message that is logged into the SDL log file.

Message in Log File: Displays the log file which contains the message.

To view the SIP messages that get logged into the SDL log file, perform the following actions:

- Check the **Enable SIP Call Processing Trace** check box in the Trace Configuration window of Cisco Unified Serviceability (**Trace** > **Configuration**). See *Cisco Unified Serviceability Administration Guide* for more information.

- Set the trace level to any one of the following: State Transition, Significant, Arbitrary or Detailed.

Note If you are monitoring the session trace data from the logs stored on your local disk, the detailed SIP message will be available only if the SDL/SDI logs are present in the parent directory of the call logs.

Step 5 Click **Save**.

If you are monitoring real-time data, the Call Flow Diagram is saved as index.html in the specified folder along with the SDL files which contain the SIP messages. You can email the files to the Technical Assistance Center (TAC). For more information on monitoring real-time data, see "Monitor real-time data." The SIP messages in the saved Call Flow Diagram appear as hyperlinks. When you click a SIP message, the detailed SIP message along with the following details is displayed in a new window.

Field	Description
Sender	Displays the IP address of the originating call.
GUID	Displays the SIP call ID.
Message Label	Displays the message type for the corresponding SIP message onto which you move your mouse; for example, 200 OK, or 180 Ringing.
Receiver	Displays the IP address of the destination call.
MAC_ADDRESS	Displays the name of the device.
Message Tag	Displays the sequence number to match the actual messages in the SDI Trace file.
MSG_TYPE	Displays the type of message.
Correlation ID	Displays the Correlation ID.
Timestamp	Displays the server time at which the call operation (call setup/split/join/release) happens.

If you open logs for Unified Communications Manager 8.5(1) or 8.6(1) using Open from Local Disk option and save the ladder diagram , the SIP messages, the SDI log files that contain the SIP messages and SDL Log files for a duration of from 5 minutes before the start of the call to 5 minutes after the start of the call will be saved. If you save logs from Unified Communications Manager 9.0(1) or later, the SDL log files that contain the call details are saved along with index.html and the SIP messages. For more information about monitoring the session trace data from the logs saved to your local disk, see "Monitor session trace data from local disk."

Note If the files are zipped, extract the zipped files to a local folder and open them to view the images.

You can perform the following actions:

a) To view the online help, click **Help**.
b) To exit the Analyze Call Diagram screen, click **Close**.

c) To navigate to the previous page, click **Previous Messages**.
d) To navigate to the next page, click **Next Messages**.

Note **Previous Messages** or **Next Messages** is enabled only when the message size exceeds a threshold.

The Session Manager logs the call data in new log files. These new log files are located in the following folder: `/var/log/active/cm/trace/ccm/calllogs/`.

The Call Log name has the following filename pattern: `calllogs_dddddddd.txt.gz`.

Detailed SIP messages are logged into SDI traces.

The Call Logs include the following message types:

- Call Control: Writes call information at call setup, split, join, and release.

```
Timestamp|MessageType (CC)|Operation (SETUP/SPLI/JOIN/RELEASE)|CI for one leg (aCI)|CI
 for other leg (bCI)|calling DN|Orig Called DN|Final Called DN
```

- Device Layer: Writes metadata information that relates to message from or to the device.

```
Timestamp|MessageType (SIPL/SIPT)|My leg CI|Protocol(tcp/ucp)|Direction (IN/OUT)|local
 ip|local port|device name|device ip|device port|Correlation id|Message Tag|SIP Call
ID|SIP method
```

The following limitations apply when the Call Flow Diagram is generated:

- Search does not show incomplete calls.

  Example:

  When the user picks up the handset and hangs up without dialing the complete DN, it will not be listed in the search results.

- The Call Flow Diagram does not show some SIP messages in the following scenarios:
  - Conference calls involving more than three parties.
  - A call leg is used to invoke a feature alone.

  Example:

  Phone B and Phone C are in the same pickup group.

  a. User A calls Phone B.

  b. User C lifts up the Phone C handset.

  c. User C presses the PickUp softkey to pickup the call.

SIP messages exchanged in Step b are not displayed in the Call Flow Diagram

In these cases, a RELEASE message is logged in the call logs without a corresponding SETUP message.

Services Monitoring

The Service monitoring category monitors the activities of Cisco TFTP requests, database activities, and heartbeat of the server or of different servers in a cluster (if applicable).

The Cisco TFTP service builds and serves files that are consistent with the Trivial File Transfer Protocol, which is a simplified version of the File Transfer Protocol (FTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files. You can view the total Cisco TFTP requests, requests not found, and requests that were aborted.

Unified RTMT monitors the heartbeat of Unified Communications Manager and Cisco TFTP services for the server or for different servers in a cluster (if applicable). The heartbeat acts as an indicator of the life of whatever it is monitoring. When the heartbeat is lost, a blinking icon appears in the lower right corner of the RTMT window. To find when the heartbeat loss was detected, click the blinking icon. An email can notify you of the heartbeat loss, if you configure the system to do so.

The database summary provides connection information for the server or for each server in a cluster (if applicable), such as the change notification requests that are queued in the database, change notification requests that are queued in memory, the total number of active client connections, the number of devices that are queued for a device reset, replicates created, and replication status.

For information about daily reports for CTI and Cisco TFTP usage statistics, see the *Cisco Unified Serviceability Administration Guide*.

The following table provides information about the service objects that RTMT monitors, the alert, thresholds, and defaults.

Table 4: Services Category

Monitored Objects (Displayed)	Alert/Threshold/Default
Number of open devices, lines, CTI connections, and active Unified Communications Manager links for each CTI Manager.	N/A
TotalTftpRequests and TotalTftpRequestsAborted for each Cisco TFTP server.	N/A
Connection and replication status for each Directory server.	• Connection failed. • Replication failed.
Heartbeat rate for Cisco CallManager, Cisco TFTP services.	• Unified Communications Manager heartbeat rate specifies <0.x. Default specifies 0.5. • Cisco TFTP heartbeat rate specifies <0.x. Default specifies 0.5.

Service Logs

The service data accumulates in the memory whenever RTMT calls the LogService API. Every five minutes, RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every five minutes for the following counters, based on the following calculation:

- ctiOpenDevices: Average of all the values that were collected in last five minutes
- ctiLines: Average of all the values that were collected in last five minutes
- ctiConnections: Average of all the values that were collected in last five minutes
- ctiActiveCMLinks: Average of all the values that were collected in last five minutes
- tftpRequests: Cumulative (difference between last collected value and the first collected value in last five minutes)
- tftpAbortedRequests: Cumulative (difference between last collected value and the first collected value in last five minutes)

The AMC service logs the service data in csv format. The header of the log comprises the time zone information and a set of columns with the counters that were previously listed for a server. These sets of columns repeat for every server in a cluster, if applicable.

The following filename format of the Service Log applies: ServiceLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log comprises the header.

Device Logs

The device data accumulates in the memory whenever RTMT calls the LogDevice API. Every five minutes, RTMT logs the data into the file as a single record and cleans the memory.

The data is logged every five minutes for the following counters based on the following calculation:

- gatewayDevicesFXS: Average of all the values that were collected in last 5 minutes
- gatewayDevicesFXO: Average of all the values that were collected in last 5 minutes
- gatewayDevicesPRI: Average of all the values that were collected in last 5 minutes
- gatewayDevicesT1: Average of all the values that were collected in last 5 minutes
- gatewayDevicesH323: Average of all the values that were collected in last 5 minutes

The AMC service logs the device data in CSV format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for a server. These sets of columns repeat for every server in a cluster, if applicable.

The following filename format of the Device Log applies: `DeviceLog_MM_DD_YYYY_hh_mm.csv`.

The first line of each log file comprises the header.

Device Monitoring

Device Monitoring

The Device monitoring category provides a summary of devices, device search capability, and a summary of phones.

For information about daily reports on registered devices, see the *Cisco Unified Serviceability Administration Guide*.

The following table provides information about the device objects that Unified RTMT monitors, the alert, thresholds, and defaults, and what kind of reports that Unified RTMT generates for those devices.

Table 5: Devices Category

Monitored Objects (Displayed)	Alert/Threshold/Default
Number of registered phones for each server or for all servers in a cluster (if applicable).	Total number of registered phones drops by X% in consecutive polls. Default specifies 10%.
Number of registered gateways on each server or for all servers in a cluster (if applicable).	For Unified Communications Manager: • (Warning) Clusterwide total number of registered gateways decreased in consecutive polls. • (Informational) Clusterwide total number of registered gateways increased in consecutive polls.
Number of registered media devices on each server or for all servers in a cluster (if applicable).	For Unified Communications Manager: • (Warning) Clusterwide total number of registered media devices decreased in consecutive polls. • (Informational) Clusterwide total number of registered media devices increased in consecutive polls. • Media List exhausted.

The Device Search menu comprises the following items on which you can search: phones, gateway devices, H.323 devices, CTI devices, voice-messaging devices, media resources, hunt lists, and SIP trunks.

You can search on any device in the Unified Communications Manager system and choose the status of the devices, including registered, unregistered, rejected, any status, and devices that are only configured in the database. You can also search by any model, or a specific device model, and set up criteria that include several different attributes. Within the phone search, you can also search on the basis of phone protocol. You can also generate reports for your devices to troubleshoot them.

Note Currently, only 200 devices are displayed in the Device Search page for a single node in the cluster.

Unified RTMT queries Cisco RIS to find the matching device. Results display in a table with a row for each matched device, a column for each of the specified attributes, and a timestamp of the device that has been opened or closed and the application that controls the device media.

If you have Unified Communications Manager clusters and you search for a device by choosing the Any Status option, Unified RTMT does not display a snapshot of the matched device type, but rather it displays data for that device type from the Cisco RIS database for all specified Unified Communications Manager servers for a period of time. As a result, you may see multiple entries of a device with multiple statuses (for example, Registered or Unregistered) in Unified RTMT.

When you see multiple entries of a device, the current status of the device reflects the entry that has the latest timestamp. By configuring the Cisco RIS Unused Cisco CallManager Device Store Period service parameter for the Cisco RIS Data Collector service in System Configuration Guide for Cisco Unified Communications Manager, you can configure the period of time that the Cisco RIS database keeps information on unregistered or rejected device. See the *System Configuration Guide for Cisco Unified Communications Manager* for more information about configuring service parameters.

Tip To find the matching item, Unified RTMT requires that you activate the Cisco RIS Data Collector service in the Service Activation window.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a timestamp of the device that has been opened or closed and the application that controls the device media.

The phone summary provides information about the number of registered phones, phones that are running SIP, phones that are running SCCP, partially registered phones, the number of failed registration attempts, and the number of registered dual-mode devices (supports only the TCT and BOT device types).

Find Specific Devices to Monitor

Follow this procedure to monitor data for the following device types:

- Phones
- Gateway Devices
- H.323 Devices
- CTI Devices
- Voicemail Devices
- Media Resources
- Hunt List
- SIP Trunk

Procedure

Step 1 Perform one of the following tasks:

a) On the Quick Launch Channel, perform the following steps:

1. Click **Voice/Video**.
2. In the tree hierarchy, double-click **Device**.
3. Click the **Device Search** icon.

b) Choose **Voice/Video** > **Device** > **Device Search** > **Open Device Search** and select the device type; for example, Phone, Gateway, Hunt List, and so on. A device selection window displays where you enter the search criteria.

The **Device Search** window displays the cluster names (if applicable) and tree hierarchy that lists all device types that you can monitor.

Tip After you display the Device Search or CTI Search panes, you can right-click a device type and choose **CCMAdmin** to go to Cisco Unified Communications Manager Administration.

Step 2 To find all devices or to view a complete list of device models from which you can choose, right-click the cluster name and choose **Monitor**.

Step 3 To monitor a specific device type, right-click or double-click the device type from the tree hierarchy.

Note If you right-click the device type, you must choose **Monitor** for the device selection window to display.

Step 4 In the **Select device with status** window, click the radio button that applies.

Step 5 In the drop-down list box next to the radio button that you clicked, choose **Any CallManager** or a specific Unified Communications Manager server for which you want the device information to display.

Tip In the remaining steps, you can choose the **<Back**, **Next>**, **Finish**, or **Cancel** buttons.

Step 6 Click the **Next>** button.

Step 7 In the Select Device with Download Status pane, click the radio button that applies, and click **Next**.

Step 8 In the Search by device model pane, click the radio button that applies.

Tip If you chose **Device Model**, choose the device type for which you want the device information to display.

Step 9 Click **Next**.

Step 10 In the Search with name pane, click the radio button that applies and enter the appropriate information in the corresponding fields, if required.

Note If you enter the IPv6 address, the IP Subnet does not apply.

Step 11 Click **Next**.

Step 12 In the Monitor following attributes pane, check one or all of the search attributes.

Step 13 Click **Finish**.

Note Some devices may not provide information for all search criteria. For example, if you select to monitor a phone for active load, inactive load, download status, or download reason, the download status results display Unknown for phone models that cannot provide this information.

View Phone Information

You can view information about phones that display in the RTMT device monitoring pane. This section describes how to view phone information.

Procedure

Step 1 Find and display the phone in the RTMT device monitoring pane.

Step 2 Perform one of the following tasks:

a) Right-click the phone for which you want information to display and choose **Open**.

b) Click the phone and choose **Device** > **Open**.

The **Device Information** window appears.

Step 3 In the Select Device with Status pane, click the radio button that applies.

Step 4 In the drop-down list box next to the radio button that you clicked, choose **Any CallManager** or a specific Unified Communications Manager server for which you want the device information to display.

Step 5 In the Search By Device Model pane, choose the phone protocol that you want to display.

Step 6 Click the **Any Model or Device Model** radio button.

If you click the **Device Model** radio button, choose a phone model that you want to display.

Step 7 Click **Next**.

Step 8 In the Search With Name pane, click the radio button that applies and enter the appropriate information in the corresponding fields.

Step 9 In the Monitor following attributes pane, check one or all of the search attributes.

Step 10 Click **Finish**.

The **Device Information** window appears. For more information about the device, choose any field that appears in the left pane of the window.

Generate PRT Information for Endpoints

Devices or endpoints generate alarms for each critical event for diagnostics and troubleshooting. Use the Generate PRT option to remotely trigger the log collection on the phone and upload it to the log server configured in the “Customer support upload URL” parameter.

Procedure

Step 1 Find and display the phone in the RTMT device monitoring pane.

Step 2 Right-click the phone for which you want information to display and choose **Generate PRT**.

The generated report is uploaded at the **Customer support upload URL**.

Note Check the **Customer support upload URL** parameter in either the Enterprise, Profile, or Device level configuration settings page. Else, PRT generation fails.

View Device Properties

You can view the properties of devices that appear in the RTMT device monitoring pane. Follow this procedure to view device properties.

Procedure

Step 1 Find and display the device in the RTMT device monitoring pane.

Step 2 Perform one of the following tasks:

- Right-click the device for which you want property information and choose **Properties**.
- Click the device for which you want property information and choose **Device** > **Properties**.

Step 3 To display the device description information, click the **Description** tab.

Step 4 To display other device information, click the **Other Info** tab.

Set Up Polling Rate for Devices and Perfmon Counters

Unified Communications Manager polls counters, devices, and gateway ports to gather status information. In the RTMT monitoring pane, you configure the polling intervals for the performance monitoring counters and devices.

Note High-frequency polling rate may adversely affect Unified Communications Manager performance. The minimum polling rate for monitoring a performance counter in chart view is 5seconds; the minimum rate for monitoring a performance counter in table view is 1second. The default value for both is 10seconds.

Note The default value for devices is 10minutes.

Follow this procedure to update the polling rate:

Procedure

Step 1 Display the device or performance monitoring counter in the RTMT monitoring pane.

Step 2 Click the device and choose **Edit** > **Polling Rate**.

Step 3 In the Polling Interval pane, specify the time that you want to use.

Step 4 Click **OK**.

CTI Application, Device, and Line Monitoring

The CTI category monitors CTI Manager activities and provides CTI search capability. With CTI Manager, you can monitor the number of open devices, lines, and CTI connections.

You can specify criteria for the CTI applications, devices, and lines that include CTI status, device name, application pattern, and attributes.

Tip To find the matching item, RTMT requires that you activate the Cisco RIS Data Collector service in the **Service Activation** window in Cisco Unified Serviceability.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a time stamp of the device that has been opened or closed and the application that controls the device media.

View CTI Manager Information

Follow this procedure to display a chart of open devices, lines, and CTI connections for each server or for each server in a cluster (if applicable).

Procedure

Step 1 Click **Voice/Video** in the quick launch channel.

Step 2 Double-click **CTI**.

Step 3 Click the **CTI Manager** icon.

Find CTI Applications to Monitor

Perform the following procedure to find specific CTI applications to monitor:

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel, perform the following steps:
  - **a.** Click **Voice/Video**.
  - **b.** In the tree hierarchy, double-click **CTI**.
  - **c.** Click the CTI Search icon.
- Choose **Voice/Video** > **CTI** > **CTI Search** > **CTI Applications**. The selection window appears where you can enter the search criteria.

Step 2 From the **CTI Manager** drop-down list box, choose the CTI Manager that you want to monitor.

Step 3 From the **Applications Status** drop-down list box, choose the application status.

Step 4 Click **Next**.

Step 5 In the Application Pattern pane, click the radio button that applies.

Step 6 Enter the information in the field for the radio button that you clicked; for example, if you clicked the **IP Subnet** radio button, enter the IP address and the subnet mask in the field.

Note If you enter the IPv6 address, the IP Subnet does not apply.

Step 7 Click **Next**.

Step 8 In the **Monitor following attributes** window, check one or all of the check boxes for the attributes that you want to monitor.

Step 9 Click **Finish**.

The applications monitoring pane displays the information that you choose.

Find CTI Devices To Monitor

Follow this procedure to find specific CTI devices to monitor.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel, perform the following steps:
  a. Click **Voice/Video**.
  b. In the tree hierarchy, double-click **CTI**.
  c. Click the CTI Search icon.
- Choose **Voice/Video** > **CTI** > **CTI Search** > **CTI Devices**. The selection window appears where you can enter the search criteria.

Tip If you right-click the option, choose **Monitor**.

Step 2 From the **CTI Manager** drop-down list box, choose the CTI Manager that you want to monitor.

Step 3 From the **Devices Status** drop-down list box, choose the device status.

Step 4 In the Devices pane, click the radio button that applies.

Tip If you chose **Device Name**, enter the device name in the field.

Step 5 Click **Next**.

Step 6 In the **Application Pattern** window, click the radio button that applies.

Step 7 Enter the information in the field for the radio button that you clicked; for example, if you clicked **IP Subnet**, enter the IP address and subnet mask in the field.

Note If you enter the IPv6 address, the IP Subnet does not apply.

Step 8 Click **Next**.

Step 9 In the **Monitor following attributes** window, check one or all check boxes for the attributes that you want to monitor.

Step 10 Click **Finish**.

The devices monitoring pane displays the information that you chose.

Find CTI Lines To Monitor

Follow this procedure to find specific CTI lines to monitor.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel, perform the following steps:
  a. Click **Voice/Video**.
  b. In the tree hierarchy, double-click **CTI**.
  c. Click the CTI Search icon.
- Choose **Voice/Video** > **CTI** > **CTI Search** > **CTI Lines**. The selection window appears where you can enter the search criteria.

Tip If you right-click the option, choose **Monitor**.

Step 2 From the **CTI Manager & Status** drop-down list box, choose the CTI manager that you want to monitor.

Step 3 From the **Lines Status** drop-down list box, choose the status.

Step 4 In the Devices pane, click the radio button that applies.

Tip If you chose **Device Name**, enter the device name in the field.

Step 5 In the Lines pane, click the radio button that applies:

Note If you chose **Directory Number**, enter the directory number in the field.

Step 6 Click **Next**.

Step 7 In the Application Pattern pane, click the radio buttons apply:

Step 8 Enter the information in the field for the radio button that you clicked; for example, if you clicked **IP Subnet**, enter the IP address and subnet mask in the field.

Note If you enter the IPv6 address, the IP Subnet does not apply.

Step 9 Click **Next**.

Step 10 In the **Monitor following attributes** window, check one or all check boxes for the attributes that you want to monitor.

Step 11 Click **Finish**.

The lines monitoring pane displays the information that you choose.

View Application Information

You can view the application information for selected devices such as the Cisco Unified IP Phone, CTI port, and CTI route point. Follow this procedure to view application information.

Procedure

Step 1 Find and display the devices in the RTMT monitoring pane.

Step 2 Perform one of the following tasks:

- Right-click the device for which you want application information; for example, CTI; then, choose **App Info**.
- Click the device for which you want application information and choose **Device** > **App Info**.

The Application Information window displays the CTI manager server name, application ID, user ID, application IP address, application status, app time stamp, device time stamp, device name, and CTI device open status.

Step 3 To view updated information, click **Refresh**. To close the window, click **OK**.

Access Learned Pattern and SAF Forwarder Reports for Call Control Discovery

Learned Pattern reports and Service Advertisement Framework (SAF) forwarder reports support the Call Control Discovery feature. When you configure the call control discovery feature, Unified Communications Manager advertises itself and its hosted DN patterns to other remote call-control entities that use the SAF network. Likewise, these remote call-control entities advertise their hosted DN patterns, which Unified Communications Manager can learn and insert in digit analysis. For more information about the call control discovery feature, see “Call Control Discovery” in the *Feature Configuration Guide for Cisco Unified Communications Manager* .

Note The learned pattern may be repeated in the report because the learned pattern may be coming from a different source; for example, it may be coming from a different IP address.

Learned Pattern reports include such information as learned pattern name, time stamp, and reachability status for the pattern. See the following table.

Table 6: Data From Learned Pattern Report

Column	Description
Pattern	Displays the name of the learned pattern from the remote call-control entity.
TimeStamp	Displays the date and time that the local Unified Communications Manager marked the pattern as a learned pattern.
Status	Indicates whether the learned pattern was reachable or unreachable

Column	Description
Protocol	Displays the protocol for the SAF-enabled trunk that was used for the outgoing call to the learned pattern; if the remote call-control entity has QSIG tunneling configured for the SAF-enabled trunk, the data indicates that QSIG tunneling was used; for example, EMCA is listed along with H.323 in this column.
AgentID	Displays the name of the remote call-control entity that advertised the learned pattern
IP Address	Displays the IP address for the call control entity that advertised the learned pattern; Displays the port number that the call-control entity uses to listen for the call.
ToDID	Displays the PSTN failover configuration for the learned pattern.
CUCMNodeId	Displays the ID from the local Unified Communications Manager node.

SAF Forwarder reports display information such as authentication status and registration status of SAF forwarders. See the following table.

Table 7: Data From SAF Forwarder Report

Column	Description
Name	Displays the name of the SAF forwarder that you configured in the SAF Forwarder Configuration window in Cisco Unified Communications Manager Administration.
Description	Displays the description for the SAF forwarder that you configured in the SAF Forwarder Configuration window in Cisco Unified Communications Manager Administration. If None displays, you did not enter a description for the SAF forwarder.
IP Address	Displays the IP address for the SAF forwarder, as configured in the SAF Forwarder Configuration window in Cisco Unified Communications Manager Administration.
Port	Indicates the port number that Unified Communications Manager uses to connect to the SAF forwarder; by default, Unified Communications Manager uses 5050.
Type	Indicates whether the SAF forwarder is classified as the primary or backup SAF forwarder.

Column	Description
Connection Status	Indicates whether Unified Communications Manager can connect to the SAF forwarder.
Authentication Type	Indicates that Unified Communications Manager used digest authentication to connect to the SAF forwarder.
Registration Status	Indicates whether the Unified Communications Manager is registered to the SAF forwarder.
Time Last Registered	Displays the date and time when the Unified Communications Manager last registered with the SAF forwarder.
No of Registered Applications	Displays the total number of CCD advertising and requesting services that are registered to the SAF forwarder.
No of Connection Re-Attempts	Displays the number of times that the call-control entity, in this case, the Unified Communications Manager, has attempted to connect to the SAF forwarder.

RTMT allows you to search based on different criteria; for example, if you specify a search for the remote call-control entity, all the learned patterns display for the remote call-control entity.

To access the Learned Patterns or SAF Forwarder reports in RTMT, perform the following procedure.

Procedure

Step 1 To access the report, perform one of the following actions:

a) For Learned Patterns: From the RTMT menus, choose **Voice/Video** > **Report** > **Learned Pattern**. Or, Click the **Voice/Video** tab; then, click **Learned Pattern**.

b) For SAF Forwarders: From the RTMT menus, choose **Voice/Video** > **Report** > **SAF Forwarders**. Or, click the **Voice/Video** tab; then, click **SAF Forwarders**.

Step 2 Choose the node from the **Select a Node** drop-down list box.

For learned pattern reports, if the Cisco CallManager Service is running but the CCD requesting service is not running on that node, a message displays that the CCD Report Service is not working after you choose the node. If the CCD requesting service is not active on the node that you choose, the report displays as empty.

Step 3 Review the data in the report.

See the Data from Learned Pattern Report table and the Data from SAF Forwarder Report table for descriptions of the items that were reported.

Step 4 After the data appears, if you want to filter the results based on specific criteria, click the **Filter** button; specific the criteria that you want to search, click **Apply** and then **OK**.

Step 5 To display the most current results, click **Refresh**.

Step 6 If you want to search on a specific string in the data, click the **Find** button, enter the string, then, click **Find Next**.

Step 7 If you want to save the results, click **Save**, and choose either **XML** or **Text**, depending on how you want to save the results. Browse to the location where you want to save the data, name the file that you want to save; then, click **Save**.

Access Called Party Trace Report

Called Party Trace allows you to configure a directory number or list of directory numbers that you want to trace. You can request on-demand tracing of calls using the Session Trace Tool.

The Called Party Trace feature provides information on the calling party number in addition to the called party number within a node. You can use the information from each node to trace a call back to the originator.

Note You must be an authorized administrator to access the directory number logs. To grant authorization to a specific role using MLA, the "Called Party Tracing" resource must have read permission enabled for the role.

To access the Called Party Trace report in the Real-Time Monitoring Tool, follow these steps:

Procedure

Step 1 From the RTMT menu, choose **Voice/Video** > **Callprocess** > **Called Party Trace**. Or, Click the **Voice/Video** tab; then, click **Called Party Trace**.

Step 2 Select the start time of the report using the drop-down box.

Note The start time cannot be older than five years from the current date.

Step 3 The report shows the following information:

- Start time
- Calling directory number
- Original called directory number
- Called directory number
- Calling device name
- Called device name

Note When 5 megabytes of trace file entries have been written to the log files being accessed by RTMT, the oldest log information is overwritten by new trace entries as they are recorded. The RTMT lists a maximum of 500 entries for any given search.

Intercompany Media Services

IME Service Monitoring

The IME Service category monitors the following items:

- Network Activity: Displays the activity on the Unified Communications Manager that relates to Cisco Intercompany Media Engine. The Network Activity object displays these charts:
  - IME Distributed Cache Health: Displays the health of the IME distributed cache based on the IMEDistributedCacheHealth counter for the IME Server performance object.
  - IME Distributed Node Count: Displays an approximation of the number of nodes in the IME distributed cache, based on the value of the IMEDistributedCacheNodeCount counter for the IME Server performance object. Because each physical Cisco Intercompany Media Engine server contains multiple nodes, the number that displays in the chart does not indicate the number of physical Cisco Intercompany Media Engine servers that participate in the IME distributed cache.
  - Internet BW Received: Displays the amount of bandwidth in Kbits/s that the Cisco IME service uses for incoming Internet traffic and represents the InternetBandwidthRecv counter for the IME Server performance object.
  - Internet BW Send: Displays the amount in Kbits/s that the Cisco IME service uses for outgoing Internet traffic and represents the InternetBandwidthSend counter for the IME Server performance object.
  - IME Distributed Cache Stored Data Records: Displays the number of IME Distributed Cache records that the Cisco Intercompany Media Engine server stores and represents the IMEDistributedCacheStoredData counter for the IME Server performance object.

    To display information about network activity, choose **Cisco IME Service** > **Network Activity**.

- Server Activity: Allows you to monitor the activity on the Cisco Intercompany Media Engine server. The Server Activity object displays these charts:
  - Number of Registered Clients: Displays the current number of clients that connect to the Cisco IME service and represents the value of the ClientsRegistered counter for the IME Server performance object.
  - IME Distributed Cache Quota: Indicates the number of individual DIDs that can be written into the IME Distributed Cache, by Unified Communications Manager servers attached to this IME server. This number is determined by the overall configuration of the IME Distributed Cache, and the IME license installed on the IME server.
  - IME Distributed Cache Quota Used: Indicates the total number of unique DID numbers that have been configured, to be published through enrolled patterns for Intercompany Media Services, by Unified Communications Manager sservers currently attached to this IME server.
  - Terminating VCRs: Indicates the total number of IME voice call records that are stored on the Cisco IME server for the terminating side of a call. These records can be used for validation of learned routes.

- Validations Pending: Displays the number of pending validations on the Cisco IME service as well as the threshold for validations. This chart represents the ValidationsPending counter for the Cisco IME Server performance object.

  To display information about server activity, choose **Cisco IME Service** > **Server Activity**.

IME System Performance Monitoring

The IME System Performance monitoring category provides the SDL Queue object that monitors the number of signals in the SDL queue and the number of signals that were processed for a particular signal distribution layer (SDL) queue type. The SDL queue types comprise high, normal, low, and lowest queue. You can monitor the SDL queue for a particular server or for an entire cluster (if applicable).

To display information about the SDL Queue, choose **Cisco IME Service** > **SDL Queue**. Select the type from the **SDL Queue Type** drop-down list box.

Monitor Intercompany Media Services

Tip The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application, not the back end server time, provides the basis for the time stamp in each chart.

Tip To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart that interests you. Release the left mouse button when you have the selected area. RTMT updates the monitored view. To zoom out and reset the monitor to the initial default view, press the **R** key.

The Intercompany Media Services monitoring category monitors the following items:

- Routing: Displays the total number of Cisco Intercompany Media Engine routes that Unified Communications Manager maintains. This total includes the following routes:
  - Learned routes that represent the phone numbers that the Cisco Intercompany Media Engine client learned and that exist in the Unified Communications Manager routing tables
  - Unique domains of peer enterprises for which Cisco Intercompany Media Engine routes exist
  - Published routes that represent the number of direct inward dialing numbers (DIDs) that were published successfully to the IME distributed hash table across all Cisco Intercompany Media Engine services
  - Rejected routes that represent the number of learned routes that were rejected because the administrator blocked them.

    These charts represent the following performance counters for the Cisco IME Client performance object: RoutesLearned, DomainsUnique, RoutesPublished, and RoutesRejected.

    To display information about routing, choose **Voice/Video** > **Cisco IME Client** > **Routing**.

- Call Activities: Allows you to monitor the total number of Cisco Intercompany Media Engine calls. This total includes the following types of calls:
  - Calls that were attempted (including calls that were accepted, busy, no answer, and failed)
  - Calls that were received
  - Calls that were set up (that is, made by Unified Communications Manager and accepted by the remote party)
  - Calls that were accepted (that is, received by Unified Communications Manager and answered by the called party)
  - Calls that completed fallback to the PSTN
  - Calls that did not successfully fall back to the PSTN.

These charts represent the following performance counters for the Cisco IME Client performance object: CallsAttempted, CallAccepted, CallsReceived, CallsSetup, IMESetupsFailed, and FallbackCallsFailed.

To display information on call activities, choose **Voice/Video** > **Cisco IME Client** > **Call Activities**.

IM and Presence Monitoring

IM and Presence and Cisco Jabber summary monitoring

The Real-Time Monitoring Tool provides a set of important performance counters that assist you in monitoring the overall performance of the IM and Presence service and Cisco Jabber. The IM and Presence and Cisco Jabber summaries in RTMT allow you to monitor important common information in a single monitoring pane.

To display information on important performance counters that reflect the overall performance of IM and Presence and Cisco Jabber, select **IM and Presence** > **IM and Presence Summary** or **IM and Presence** > **Cisco Jabber Summary**.

Under IM and Presence Summary, review the following information:

- PE Active JSM Sessions
- XCP JSM IM Sessions
- Total IMs Handled
- Current XMPP Clients Connected
- Total Ad hoc Chat Rooms
- Total Persistant Chat Rooms

Under Cisco Jabber Summary, review the following information:

- Client Soap interface
- SIP Client Registered Users
- SIP Client Registered User Failures

- SIP Client IM Messages

Cisco XCP counters

Number of connected XMPP clients

Cisco XCP CM—CmConnectedSockets

View the current number of XMPP clients connected to the Cisco XCP Connection Manager on an individual IM and Presence server. This number should rise and fall based on the usage patterns of your deployment. Further investigation may be required if this number is higher than expected for your user base.

Number of connected CAXL clients

Cisco XCP Web CM—WebConnectedSockets

View the current number of CAXL web clients connected to the Cisco XCP Web Connection Manager on an individual IM and Presence server. This number should rise and fall based on the usage patterns of your deployment. Further investigation may be required if this number is higher than expected for your user base.

Number of active outbound SIP subscriptions

Cisco XCP SIP S2S—SIPS2SSubscriptionsOut

View the current number of active outgoing SIP Subscriptions being maintained by the Cisco XCP SIP Federation Connection Manager service on the IM and Presence server. Monitor this counter if IM and Presence server is configured for SIP Interdomain Federation or SIP Intradomain Federation.

Note The total combined count of SIPS2SSubscriptionsOut and SIPS2SSubscriptionsIn must not rise above 260,000 on any single IM and Presence server.

Number of active inbound SIP subscriptions

Cisco XCP SIP S2S—SIPS2SSubscriptionsIn

View the current number of active inbound SIP Subscriptions being maintained by the Cisco XCP SIP Federation Connection Manager service on the IM and Presence server. Monitor this counter if IM and Presence server is configured for SIP Interdomain Federation or SIP Intradomain Federation.

Note The total combined count of SIPS2SSubscriptionsOut and SIPS2SSubscriptionsIn must not rise above 260,000 on any single IM and Presence server.

Number of IM sessions

Cisco XCP JSM—JsmIMSessions

This counter gives the total number of IM sessions on the IM and Presence node across all users. The Presence Engine (PE), which provides presence composition services and rich, always-on, network presence, creates an IM session on behalf of all users at PE start-up time. This is necessary so that network presence events such as Unified Communications Manager Telephony Presence and Exchange Calendar notifications are reflected in a user's presence even if that user is not logged in to any IM clients.

Every licensed user on a IM and Presence node has one IM Session for Presence Engine rich presence composition in addition to one IM Session for any logged in clients.

Example

There are 100 licensed users on the IM and Presence node as follows:

- 50 users are not logged in
- 40 users are logged in on one IM client
- 10 users are logged in on two IM clients

This gives a total of 160 IM Sessions comprised of:

- 100 x 1 for rich Presence Engine sessions
- 40 x 1 for users logged in on a single client
- 10 x 2 for users logged in on two clients

Total IM Packets

Cisco XCP JSM—JsmTotalMessagePackets

This counter gives the total number of IM packets handled by the IM and Presence node across all users.

Note that if user Alice sends an IM to user Bob, and both users are assigned to the same IM and Presence node, then this IM packet will be counted twice. This is because the XCP Router and Jabber Session Manager treat the two users separately. For example, Alice's privacy rules will be applied to the IM packet before it is delivered to Bob, and then Bob's privacy rules will be applied to the IM packet before it is delivered to Bob's client. Whenever IM and Presence handles an IM packet it is counted once for the originator and once for the terminator.

If Alice and Bob are assigned to different IM and Presence nodes and Alice sends an IM packet to Bob, then the IM will be counted once on Alice's node and once on Bob's node.

IMs in last 60 seconds

Cisco XCP JSM—JsmMsgsInLastSlice

This counter gives the total number of IM packets handled by the IM and Presence node across all users in the past 60 seconds. This counter is reset to 0 every 60 seconds. The same rules for counting IM packets apply as for JsmTotalMessagePackets. Monitoring of this counter will help identify the busy IM hours in your organization.

Per user and per session counters

Cisco XCP JSM Session Counters

These per session counters only exist for the duration of an IM session or user login. One set of these counters exists for each Presence Engine network presence session, and one set of these counters exists for each client login session. In the example given above for the IMSessions counters, there are 160 different sets of Cisco XCP JSM Session Counters. When a user logs out, or when the Presence Engine is stopped, the associated Cisco XCP JSM Session Counters instance is deleted.

You can use the Cisco XCP JSM Session counters to get a snapshot of all users currently logged in. These counters can be accessed from the CLI using the following command:

admin: show perf list instances "Cisco XCP JSM Session Counters"

Every user assigned to an IM and Presence node that is logged into the system will have a set of JSM session counters for their current logged in client session and also their Presence Engine network session. On an IM and Presence node with 5000 users logged in this would result in a minimum of 10,000 sets of JSM Session counters. Updating these counters with new values as they change would place the system under stress. To combat this, JSM Session counter values are cached locally by the system and only updated to RTMT every 30 minutes.

IM packets sent per session

Cisco XCP JSM Session Counters—JsmSessionMessagesIn

This counts the total number of IM packets sent by the user from his IM client or session. Note that the terminology JsmSessionMessagesIn is used as from the perspective of the IM and Presence server, the IM packet sent by the client is an inbound IM packet to IM and Presence.

IM packets received per session

Cisco XCP JSM Session Counters—JsmSessionMessagesOut

This counts the total number of IM packets sent to the user on his IM client or session. Note that the terminology SessionMessagesOut is used as from the perspective of the IM and Presence server, the IM packet is sent to the client and is an outbound IM packet from IM and Presence.

Note JsmTotalMessagePackets, JsmMsgsInLastSlice, JsmSessionMessagesIn and JsmSessionMessagesOut each represent instant message packets being sent to IM and Presence and are not exact figures of Instant Messages on the system. The amount of IM packets sent to IM and Presence per IM can vary depending on the client in use.

Total text conferencing rooms

Cisco XCP TC—TcTotalRooms

This counter represents the total number of Text Conferencing rooms hosted on the node. This includes both ad hoc rooms and persistent chat rooms.

Total adhoc group chat rooms

Cisco XCP TC—TcAdHocRooms

This counter represents the total number of AdHoc chat rooms currently hosted on the node. Note that AdHoc chat rooms are automatically terminated when all users leave the room, so this counter should rise and fall in value regularly.

Total persistant chat rooms

Cisco XCP TC—TcPersistentRooms

This counter represents the total number of persistent chat rooms hosted on the node. Persistent chat rooms must be explicitly terminated by the room owner. You can monitor this counter to identify if the total number of persistent chat rooms is very large and also to help identify if some persistent chat rooms are not being used regularly anymore.

Per-chat room counters

Cisco XCP TC Room Counters

These pre-chat room counters exist only for the lifetime of a chat room. For ad hoc chat rooms, these counter instances are deleted when the Ad Hoc chat room is terminated. For persistent chat rooms, the counter instances are also deleted when the persistent chat room is terminated, however persistent chat rooms are long-lived, so they should rarely be terminated.

You can use these per-chat room counters to monitor the usage and participants in persistent (and ad hoc) chat rooms over their lifetime and can help identify persistent chat rooms that are no longer being used frequently.

You can use the Cisco XCP TC Room Counters to get a snapshot of all rooms that are currently hosted on the node. These counters can be accessed from the CLI using the following command:

admin:**show perf list instances** "Cisco XCP TC Room Counters"

IM packets received per room

Cisco XCP TC Room Counters—TCRoomMsgPacketsRecv

This counter represents the number of IM packets received per room.

Number of occupants per room

Cisco XCP TC Room Counters—TCRoomNumOccupants

This counter gives the current number of occupants of the chat room. Monitor this counter for Persistent Chat rooms to get an indication of the usage trend for the chat room.

It is possible to have a maximum of 16,500 Text Conferencing rooms on an IM and Presence node. Each of these rooms will have its own set of Per-Chat Room counters. Similar to JSM Session counters, updating these with new values as they change would place the system under stress. To combat this, Per-Chat Room counter values are cached locally by the system and only updated to RTMT every 30 minutes.

SIP proxy counters

Number of idle SIP proxy worker processes

SIP Proxy—NumIdleSipdWorkers

View the current number of idle, or free, SIP worker processes on the IM and Presence SIP Proxy. This counter gives a good indication of the load being applied to the SIP Proxy on each IM and Presence server. Monitor this counter if IM and Presence server is configured for SIP Interdomain Federation or SIP Intradomain Federation.

The number of idle processes can drop to zero on occasion and is not a cause for concern. However, if the number of idle processes are consistently below 5 processes, then it is an indication that the IM and Presence Server is being heavily loaded and requires further investigation

Cisco Unity Connection Monitoring

Port Monitor

The Port Monitor lets you monitor the activity of each Cisco Unity Connection voice messaging port in real time. This information can help you determine whether they system has too many or too few ports.

The Port Monitor provides information about each Cisco Unity Connection voice messaging port in real time. This information can help you determine the activity of each port and whether the system has too many or too few ports. The Port Monitor displays the information for each port as described in the following table.

Table 8: Fields and Descriptions in the Port Monitor

Field	Description
Port Name	The display name of the port in Cisco Unity Connection Administration.
Caller	For incoming calls, the phone number of the caller.
Called	For incoming calls, the phone number that was dialed.
Reason	If applicable, the reason why the call was redirected.
Redir	The extension that redirected the call. If the call was redirected by more than one extension, this field shows the extension prior to the last extension.
Last Redir	The last extension that redirected the call.
Application Status	The name of the conversation that Cisco Unity Connection is playing for the caller. When the port is not handling a call, the status displays Idle.
Display Status	The action that the conversation is currently performing. When the port is not handling a call, the status displays Idle.
Conversation Status	Specific details about the action that the conversation is performing. When the port is not handling a call, the status displays Idle.

Field	Description
Port Ext	The extension of the port.
Connected To	For Unified Communications Manager SCCP integrations, the IP address and port of the Unified Communications Manager server to which the ports are registered.

Note Depending on the information that the phone system integration provided and the status of the call, some fields may remain blank.

Start Cisco Unity Connection Port Monitor Polling

Perform the following steps to use the Port Monitor.

Note Setting a low polling rate may impact system performance.

Procedure

Step 1 In the Real Time Monitoring Tool, access Unity Connection and click **Port Monitor**. The **Port Monitor** window appears.

Step 2 In the **Node** drop-down box, choose a Cisco Unity Connection server.

Step 3 In the Polling Rate field, accept the default or enter the number of seconds between updates in the data on the **Port Monitor** tab; then, click **Set Polling Rate**.

Step 4 Click **Start Polling**. The **Port Monitor** window displays the status of all voice messaging ports on Cisco Unity Connection.