CA Unified Communications Monitor

Use Cases for Configuring Monitored Environments

Version 3.5

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Preparing an Avaya Communication Manager Environment

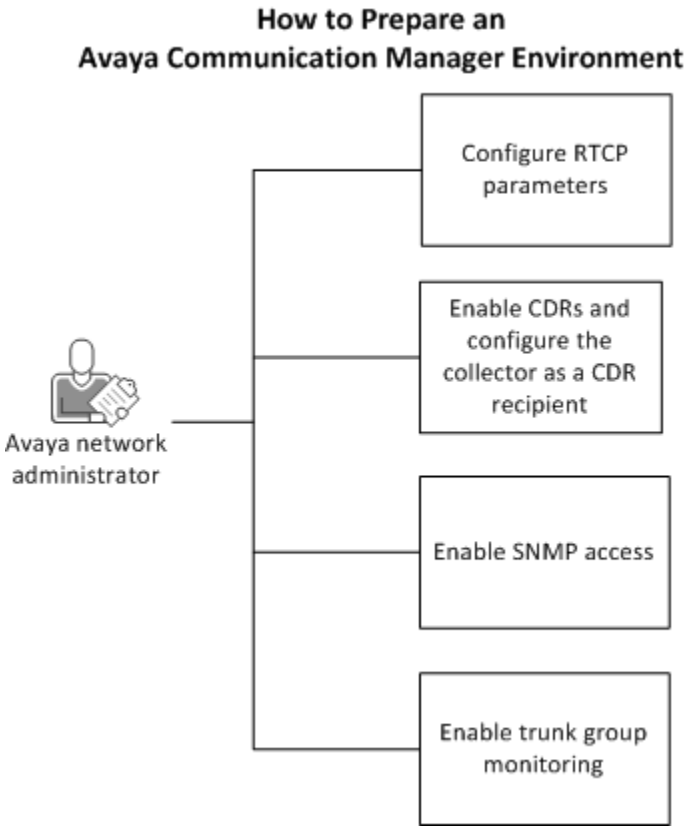
CA Unified Communications Monitor (UC Monitor) supports unified communications deployments that rely on the Avaya Communication Manager for call processing. UC Monitor requires certain aspects of the Avaya Communication Manager to be configured in specific ways.

This use case helps an Avaya network administrator prepare an Avaya Communication Manager environment for monitoring with UC Monitor.

This section contains the following topics:

How to Prepare an Avaya Communication Manager Environment

The following diagram identifies the tasks for preparing an Avaya Communication Manager environment for monitoring with UC Monitor.



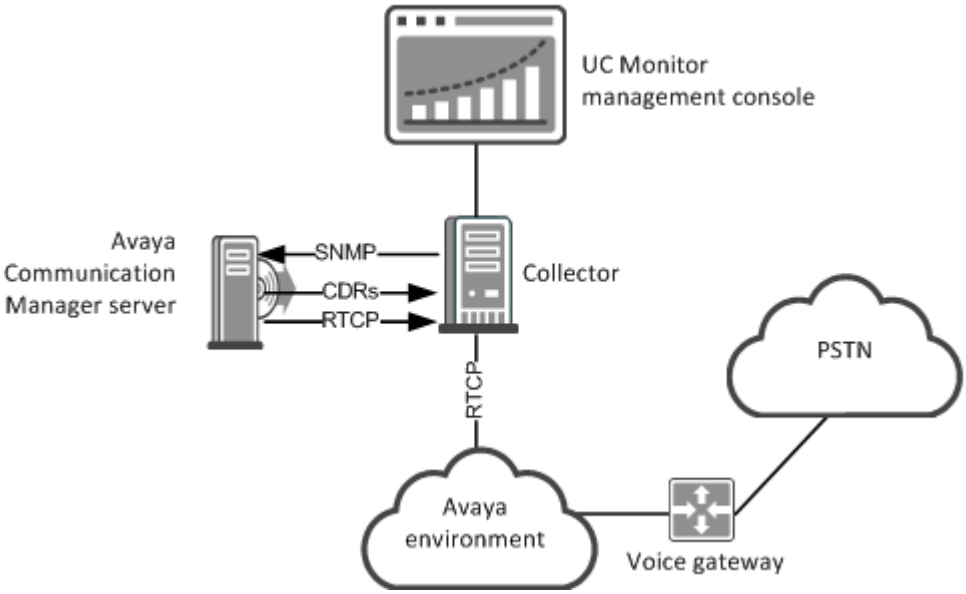
The following topics describe the tasks for preparing an Avaya Communication Manager environment. You can perform these tasks in any order. Your environment is ready after you complete the tasks.

- Configure RTCP parameters (see page 10).
- Enable CDRs and configure the collector as a CDR recipient (see page 12).
- (*Optional*) Enable SNMP access (see page 14).
- Enable trunk group monitoring (see page 15).

Architecture for Avaya Deployments

The collector must have network connectivity to the networks where Avaya endpoints and phones are making calls. The endpoints send data directly to a web service on the collector.

The following diagram illustrates UC Monitor in an Avaya-only environment:



For monitoring Avaya deployments, UC Monitor requires a management console and at least one collector. For small environments or initial rollouts with fewer than than 2500 phones, a standalone system is sufficient. A distributed system is recommended for larger deployments. The collector is then configured as the report recipient for the endpoints that are registered to the Communication Manager. The distributed architecture is flexible because collector licenses can be upgraded to support more IP phones or endpoints.

Bandwidth Considerations

Call volume is the key metric to consider when determining the scale of any UC Monitor deployment. In Avaya environments, call volume affects not only database size and growth and collector load, but also bandwidth usage, as many endpoints send quality data to the collector. However, our testing indicates that the amount of additional bandwidth used is negligible.

The following breakdown is based on our testing and provides a range that includes the approximate usage in your environment.

- In an Avaya system, the average RTCP packet size is 250 bytes, which includes Ethernet and UDP headers. By default, the Avaya phones and voice gateways send RTCP call-quality reports at 5-second intervals, which amounts to 12 packets sent per call minute, per endpoint.
- With two different devices sending reports, you can see 2 x 12 = 24 packets sent per call minute. With 24 packets per minute at 250 bytes each, network traffic from Avaya endpoints to the collector reaches approximately 6000 bytes per minute, or .0977 Kbps. Or equally, 100 bytes per second, per call minute, which is .0000954 MBps per call minute.
- When endpoints encounter congestion, they increase the 5-second interval to throttle the number of report packets sent. To prevent congestion on WAN links, increase the interval to 10 seconds and use the class-default queue for the RTCP traffic.

The following table illustrates bandwidth usage that is based on the number of simultaneous calls and the average duration of each call:

	Average Call Duration (in minutes)			
Busy-Hour Calls	**2**	**3**	**4**	**5**
1000	0.19 MBps	0.29 MBps	0.38 MBps	0.48 MBps
5000	0.95 MBps	1.43 MBps	1.91 MBps	2.38 MBps
10000	1.91 MBps	2.86 MBps	3.81 MBps	4.77 MBps
20000	3.81 MBps	5.72 MBps	7.63 MBps	9.54 MBps
50000	9.54 MBps	14.3 MBps	19.1 MBps	23.8 MBps
100000	19.1 MBps	28.6 MBps	38.1 MBps	47.7 MBps

The call detail records (CDRs) that the Avaya Communication Manager sends to the collector are 155 bytes per call. Only one CDR is sent for each call, containing information for both directions of call data flow. CDR-related traffic is further reduced when you install the UC Monitor collector near the Communication Manager.

Configure Avaya to Send RTCP Data

Instruct the Avaya endpoints to send RTCP call quality data to the UC Monitor collector, which takes the role of the RTCP Monitor. Use the Native Configuration Manager in the Avaya Communication Manager web interface to configure the RTCP Monitor, either globally or per IP network region.

The following commands and field entries are suitable for an environment in which multiple IP network regions are defined. For more information about using the Native Configuration Manager, consult the documentation for your version of Avaya Communication Manager.

Follow these steps:

1. Set the parameters of the RTCP Monitor server.
   a. Run the following command:

      ```
      change system-parameters ip-options
      ```

      Tip: To review the current settings before you change them, use the following command:

      ```
      display system-parameters ip-options.
      ```

   b. Complete the following fields:

      - **Default Server IP Address**: The IP address of the management NIC.
        Tip: You can use the UC Monitor management console to verify the address of the management NIC. Click Administration, Data Collection, Collectors. Select the collector in the list, and click Edit. The address is shown on the Collection Device Properties page.
      - **Default Server Port**: 5005
      - **Default RTCP Report Period**: 5

      Note: Configure only one Default Server per IP network region.

2. Enable RTCP reporting.
   a. Run the following command, where *N* is the number of the IP network region you want to monitor.

      ```
      change ip-network-region N
      ```

   b. Complete the following fields.

      - **RTCP Reporting Enabled**: y
      - **Use Default Server Parameters**: y

      This setting configures the phones in the IP network region to use the same parameters that you set for the Default Server. To use different collectors for selected IP network regions, set this field to *n* for each region where you want to configure a different collector.

Enable CDRs and Configure the Collector as a CDR Recipient

Because most Avaya metrics come from RTCP reports, UC Monitor does not require you to enable call detail records (CDRs). However, RTCP reports do not include the following information:

- The origin of the call.
- The dialed number when a call transverses a gateway.

When you enable CDRs, the UC Monitor collector correlates the CDRs with the RTCP data to determine call direction and the dialed number.

Note: If you do not enable CDRs, then UC Monitor cannot determine the origin of the call. In such cases, UC Monitor reports display an asterisk (*), indicating that call origination information is unknown.

Use the Avaya Communication Manager System Access Terminal (SAT) to enable CDRs and configure the collector as a CDR recipient. For more information, consult the documentation for your version of Avaya Communication Manager.

Tip: You can configure more than one CDR recipient. For example, you can configure UC Monitor and a call accounting application as CDR recipients.

Follow these steps:

1. Associate the IP address of the collector to a node name.
    a. Run the following command:

        ```
        ch node-names ip
        ```

    b. Enter the appropriate node name:
        - For S8300 servers, the default node name is procr.
        - For S8700 or S8500 servers, the node name is clan1 or clan2.

2. Define the CDR link between Avaya Communication Manager and the collector.
   a. Run the following command:

      ```
      ch ip-services
      ```

   - Complete the following fields:
     - **Service Type**: Enter CDR1 as the primary CDR link.
     - **Local Node**: Enter the name of the node that terminates the CDR link on the Avaya Communication Manager: either procr or clan1.
     - **Remote Node**: Set to the node name you defined with the ch node-names ip command.
     - **Remote Port**: Must match the port that the collector uses, which is 9000 by default.
     - **Reliable Protocol**: Set to n to disable the use of the Avaya Reliable Session Protocol for CDR transmission.

3. Set the parameters and the format of the CDR data.
   a. Run the following command:

      ```
      h system-parameters cdr
      ```

   b. Complete the following fields:
      - **Primary Output Format**: Unformatted.
      - **Primary Output Endpoint**: CDR1.
        Note: If the collector is the second of two CDR recipients, set the Secondary Output Format field to unformatted. Set the Secondary Output Endpoint field to CDR2.
      - **Use Legacy CDR Formats**: Set to y to support 3.x systems.
      - **Intra-switch CDR**: Set to y to enable call records for internal calls involving specific stations.
      - **Record Outgoing Calls Only**: Set to n to enable incoming and outgoing trunk calls to appear in the CDRs.
      - **Outg Trk Call Splitting**: Set to y to enable a separate call record for any portion of an outgoing call that is transferred or conferenced.
      - **Suppress CDR for Ineffective Call Attempts**: Set to n to prevent blocked calls from appearing in CDRs.
      - **Inc Trk Call Splitting**: Set to y to enable a separate call record for any portion of an incoming call that is transferred or conferenced.
        Note: The default values are acceptable for all other fields.

4. Define the extensions for CDR collection.
   a. Run the following command:

      ```
      ch intra-switch-cdr
      ```

   b. Complete the Assigned Members field. Enter specific extensions whose usage is tracked with a CDR. Add an entry for each extension you want to track.
      Note: Avaya provides a utility to help you perform large-scale configuration changes for multiple extensions. Contact your Avaya account representative and request a license for the Intra-Switch CDR by COS feature.
5. Verify that CDR reporting is enabled for the trunk groups whose CDRs you want to monitor.
   a. Run the following command, where *n* is the trunk group number:

      ```
      ch trunk-group n
      ```

   b. Complete the CDR Reports field. Set to y. This setting applies to all trunk group types.

Enable SNMP Access

Note: This procedure is optional. You do not need to perform this procedure if you already enabled read-only access to the SNMP Master Agent on Avaya Communication Manager.

The UC Monitor collector uses SNMP polling to access records about active devices and trunk group utilization from Avaya Communication Manager. Avaya Communication Manager provides some administrative settings that affect SNMP access to the server MIB. Only when SNMP access is enabled does UC Monitor collect the following types of information about a monitored device:

- Model or type
- Serial number
- Switch address
- Switch port

You use the Avaya Communication Manager web interface to enable SNMP access. For more information about using the web interface, consult the documentation for your version of Avaya Communication Manager.

Follow these steps:

1. Navigate to the Alarms section of the Server (Maintenance) page and enable 'SNMP Agents.'
2. Open UDP port 161 to allow SNMP access.
   - **For Avaya Aura Communication Manager**, enabling 'SNMP Agents' automatically opens UDP port 161, which is the default.
   - **For earlier versions of Avaya Communication Manager**, manually open UDP port 161. Navigate to the Firewall page of the Security section and performing the following tasks:
     - Select the Input to Server check box for the SNMP service.
     - Select the Output from Server check box for the SNMP service.

Enable Trunk Group Monitoring

Avaya Communication Manager does not automatically collect data from trunk groups. Use the Native Configuration Manager in the Avaya Communication Manager web interface to identify the trunk groups that you want to monitor.

Use the following command to open the Trunk Group Measurement Selection page, where you can identify the trunk groups that you want to monitor. The trunk group numbers do not have to be in numerical order. You can administer a maximum of 75 trunk groups for the hourly report on the G3r.

```
display meas-selection trunk-group
```

For more information about using the Native Configuration Manager, see the documentation for your version of Avaya Communication Manager.

Chapter 2: Preparing a Cisco Unified Communications Manager Environment

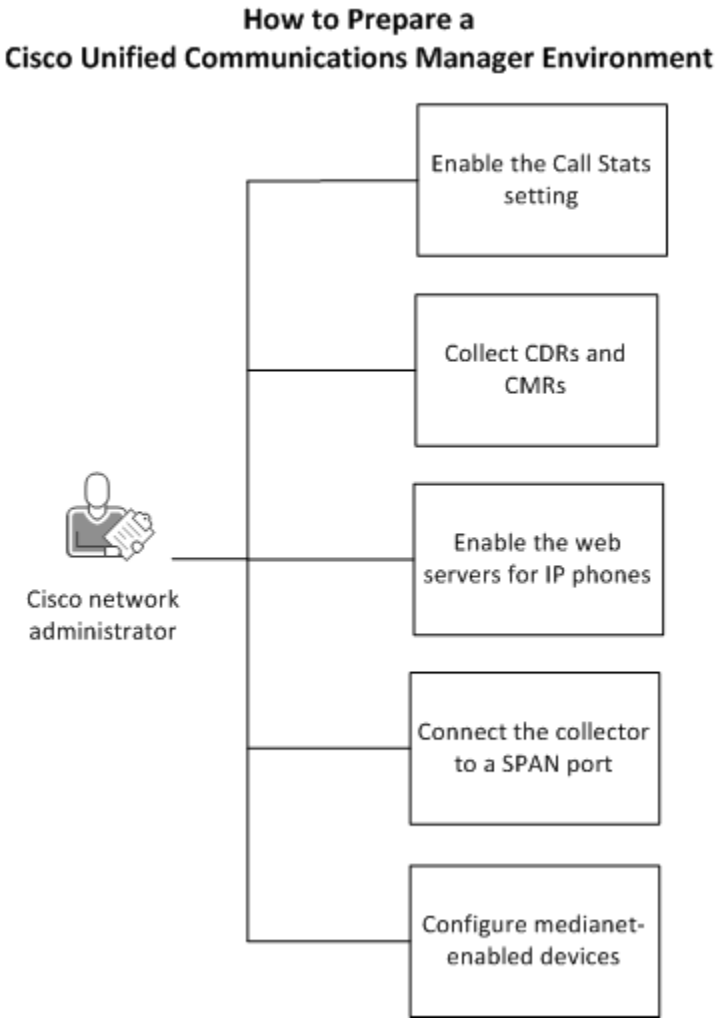
CA Unified Communications Monitor (UC Monitor) supports unified communications deployments that use Cisco Unified Communications Manager for call processing. UC Monitor requires certain aspects of Cisco Unified Communications Manager to be configured in specific ways.

This use case helps a Cisco network administrator prepare a Cisco Unified Communications Manager environment for monitoring with UC Monitor.

This section contains the following topics:

How to Prepare a Cisco Unified Communications Manager Environment

The following diagram illustrates the tasks for preparing a Cisco Unified Communications Manager environment for monitoring with UC Monitor.



The following topics describe the tasks for preparing a Cisco Unified Communications Manager environment. You can perform these tasks in any order. Your environment is ready after you complete the tasks.

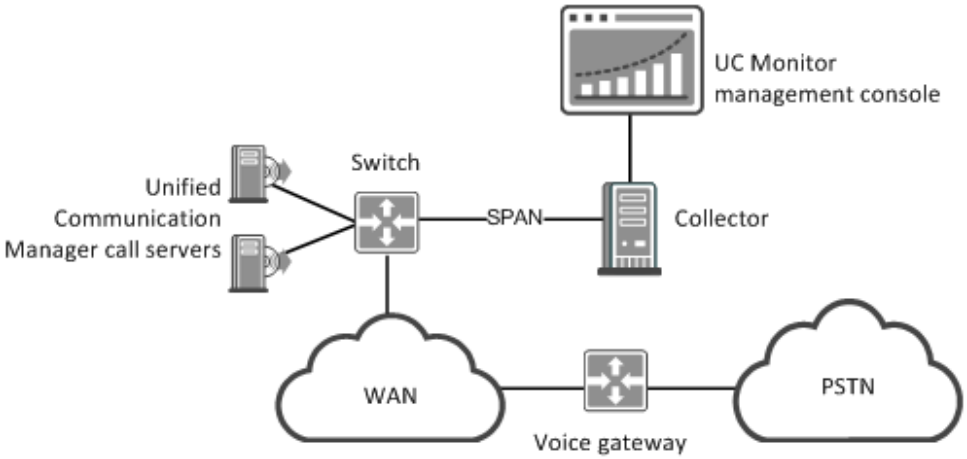
- Enable the Call Stats setting (see page 20).
- Collect CDRs and CMRs (see page 20).
- (*Optional*) Enable the web servers for IP phones (see page 21).
- Connect the collector to a SPAN port (see page 21).
- Configure medianet-enabled devices (see page 22).

Architecture and Scalability for Cisco Deployments

For Cisco deployments, UC Monitor requires a management console and at least one collector. For small environments or initial rollouts with only one Cisco Unified Communications Manager cluster, a standalone system is sufficient. For larger deployments, a distributed system is recommended.

In general, one UC Monitor collector is required for every switch that handles call setup flows from the Unified Communications Manager call server.

The following diagram illustrates UC Monitor in a Cisco-only environment:



Cisco recommends that you deploy Cisco Unified Communications Manager so as to ensure failover capability and processing redundancy:

- Do not allow the members of a call server cluster to share a VLAN or switch.
- Use different access switches. Connect them to the same distribution or core switch, or to different distribution or core switches.
- Place call servers in different buildings within the same LAN or WAN.

Enable the Call Stats Setting

Phones that use the Session Initiation Protocol (SIP) return quality metrics *only* when you enable the Call Stats setting in the Cisco Unified Communications Manager Administration web interface. You can change the standard SIP profile or you can create a new voice-quality-enabled profile.

After you enable the Call Stats setting of the SIP profile, apply the new or edited profile to your IP phones.

For information about editing or creating SIP profiles, consult the documentation for your version of Cisco Unified Communications Manager.

Collect CDRs and CMRs

UC Monitor requires the collection of call detail records (CDRs) and call management records (CMRs) for reporting end-of-call metrics. IP phones send CDRs and CMRs to the Cisco Unified Communications Manager. UC Monitor receives CDR and CMR data from the SPAN of traffic into and out of the Cisco Unified Communications Manager.

CDRs and CMRs contain the following information:

- When calls were made
- Where calls were directed
- Which phones made the calls
- Whether the calls were successfully completed

Use the Cisco Unified Communications Manager Administration web interface to enable CDR and CMR collection. For more information about using the web interface, consult the documentation for your version of Cisco Unified Communications Manager.

Enable CDR and CMR collection on the call servers in each monitored cluster. In some secure environments, CDR data cannot be stored on the call server. In such a case, store the CMRs and discard the CDRs.

Follow these steps:

1. Perform the following steps on each call server to enable CDR and CMR collection:
    a. Set the CDR Enabled flag to True.
    b. Set the Call Diagnostics Enabled flag to True.

       By default, both settings are disabled.

       You do not need to restart the call server for the change to take effect.

2. Perform the following steps on each call server to enable CMR collection, but disable CDR collection:
   a. Set the CDR Enabled flag to False.
   b. Set the Call Diagnostics Enabled flag to True.

Note: With CDRs and CMRs enabled, the Cisco Unified Communications Manager may enable archiving of these records. UC Monitor does not require the archiving of CDRs and CMRs.

Enable the Web Servers for IP Phones

An IP phone's internal web server lets other programs access the phone's web page, which provides configuration and status information that the UC Monitor collector uses. The Web Access Enabled parameter on the phone indicates whether the internal web server is enabled.

You can disable the Web Access Enabled parameter for security reasons. Core monitoring functionality for UC Monitor does not require you to enable this setting. However, enable the setting to use the UC Monitor Call Watch feature and to view data about discovered phones.

You can verify this setting from the Network Configuration menu at the phone itself. However, you can change it only at the Cisco Unified Communications Manager call server.

For more information about performing these tasks, consult the documentation for your version of Cisco Unified Communications Manager.

Connect the Collector to a SPAN Port

Connect the UC Monitor collector server to a SPAN (Switched Port Analyzer) port on the switches that carry VoIP traffic on your network. Port mirroring is a safe, effective way to mirror traffic to the collector.

For more information, see *CA Best Practices for Data Acquisition Guide* in the CA Unified Communications bookshelf on CA Support Online.

Configure Medianet-enabled Devices

A medianet is an IP architecture that enhances the performance of video, voice, and data, and automates many aspects of configuration. UC Monitor receives performance data about medianet-enabled (midstream) devices from Cisco IOS Flexible NetFlow. Medianet data appears in several Troubleshooting reports.

Use the following information when configuring your medianet-enabled devices. We recommend that you consult your network engineer or device vendor when configuring your medianet-enabled devices.

Component	Description
IPv4	Configure the devices for IPv4 routing.
UDP port 9995	Configure the devices to send data from Cisco IOS Flexible NetFlow directly to UDP port 9995 on the collector. Do not include the devices in a SPAN.
Collection interval	UC Monitor supports a collection interval of 60 seconds or less. We recommend an interval of 15 or 30 seconds. Such an interval helps ensure correct correlation of data and accurate start and end times. To configure the duration of the collection interval for a Performance Monitor policy, use the interval duration command in monitor parameters configuration mode.
Flow Exporter	In the Flow Exporter configuration, set the export destination (the collector) and the SNMP index-to-name mapping. ■ To configure the destination for a Performance Monitor Exporter, use the destination command in config-flow-exporter configuration mode. ■ To configure the interface-table option for a Performance Monitor Exporter, use the option command in config-flow-exporter configuration mode.

Component	Description
Flow Monitor	Create a Flow Monitor record that includes at least the following collect and match Performance Monitor commands: ■ match ipv4 protocol ■ match ipv4 source address ■ match ipv4 destination address ■ match transport source-port ■ match transport destination-port ■ match transport rtp ssrc ■ collect ipv4 dscp ■ collect ipv4 ttl ■ collect transport packets lost counter ■ collect transport packets out-of-order **(*)** ■ collect transport rtp jitter mean ■ collect transport rtp jitter maximum ■ collect transport rtp payload-type **(*)** ■ collect interface input ■ collect interface output ■ collect application media packets counter ■ collect application media packets rate **(*)** Requires Cisco IOS release 15.2 or later.

Note: For more information about using Performance Monitor commands, consult the *Cisco IOS Media Monitoring Command Reference* guide.

Monitoring Authenticated SIP Traffic

UC Monitor automatically reports on call quality metrics from authenticated SIP traffic by parsing packets that contain Transport Layer Security (TLS) authenticated messages.

Cisco Unified Communications Manager uses port 5061 for authenticated SIP traffic.

If you do not want to monitor SIP traffic, or you want to use a different port, contact CA Technical Support for information about configuring the .ini file.

Chapter 3: Preparing a Microsoft Lync Environment

CA Unified Communications Monitor (UC Monitor) supports unified communications deployments that use Microsoft Lync for call processing. This use case helps a Microsoft network administrator prepare a Microsoft Lync environment for monitoring with UC Monitor.

This section contains the following topics:

How to Prepare a Microsoft Lync Environment

UC Monitor supports unified communications deployments that use Microsoft Lync for call processing. The flexible product architecture lets you monitor Cisco and Avaya call servers *and* the Lync system, or a pure Lync system.

- No dedicated telephony hardware is required in a Lync environment, although the system does support optional integration with a PBX.
- The standard system can process VoIP and video calls. Audio and video calls are integrated with other Microsoft Office applications, such as Outlook, and with user contact information, such as IP address, SIP URI, and presence status.
- UC Monitor supports hardware-based IP phones, such as Polycom, in a Lync system. Users can make calls from supported phones, or from the lightweight Office Communicator application.

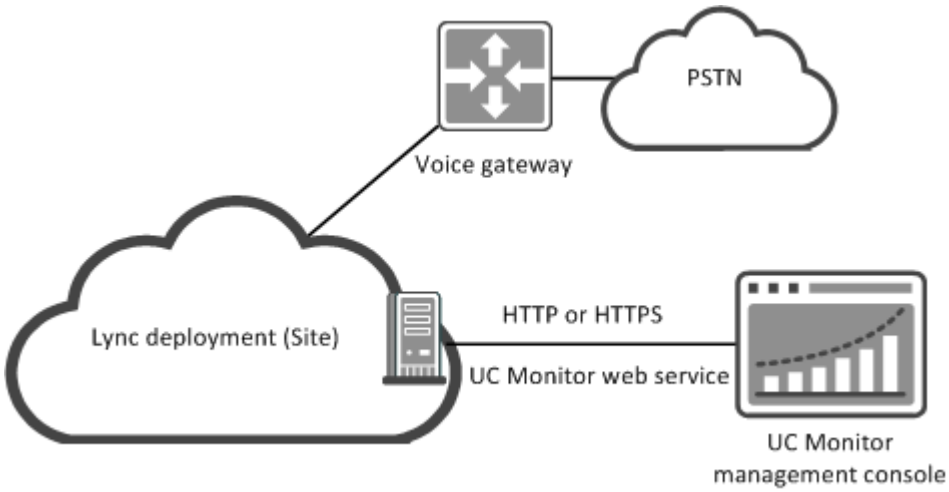
A Lync network administrator configures HTTPS or uses authentication certificates to enable secure communication between Lync servers and UC Monitor. UC Monitor does not require HTTPS or authentication certificates, but your environment may require them.

Note: See the Microsoft website for information about managing certification authority on Windows Server 2008 R2:
http://technet.microsoft.com/en-us/library/cc772011.aspx.

Architecture for Microsoft Deployments

A UC Monitor standalone system supports a Microsoft Lync deployment. A separate collector is not required. Instead of using the standard UC Monitor collector, UC Monitor leverages data from a server in the Lync site that is configured as the Lync collector.

The Lync site uses HTTP to send call quality reports to the UC Monitor web service at the management console. The following diagram illustrates this architecture:



Note: For information about configuring a Lync collector, see the use case titled *Managing Collectors in a Microsoft Lync Environment*.

Bandwidth Considerations

In our testing, we measured the size and volume of quality reports to derive some guidelines about bandwidth consumption for the Lync collector. When the Lync collectors send quality reports in batches to the web service on the management console, the bandwidth consumption is roughly as follows:

- Audio calls: 3500 bytes per report, or 7000 bytes per call
- Audio + video calls: 5300 bytes per report, or 10,600 bytes per call

The Microsoft capacity-planning guidelines identify 125 reports per second as the limit for a monitoring server. This represents call traffic from more than 125,000 users. With this benchmark, the bandwidth consumption is as follows:

- Audio calls: 125 reports per second multiplied by 3500 bytes per report = 437500 bytes per second = 3500 kbps = 3.5 Mbps.
- Audio + video calls: 125 reports per second multiplied by 5300 bytes per report = 662500 bytes per second = 5300 kbps = 5.3 Mbps

The baseline of 125 reports per second equates to a call volume of more than 220,000 calls per hour. A more likely enterprise benchmark that we observed in our testing is closer to 22,000 calls per hour:

- Audio calls: 12.5 reports per second multiplied by 3500 bytes per report = 43750 bytes per second = 350 kbps
- Audio + video calls: 12.5 reports per second multiplied by 5300 bytes per report = 66250 bytes per second = 530 kbps

Chapter 4: Preparing to Monitor Acme Packet Session Border Controllers

CA Unified Communications Monitor (UC Monitor) supports Acme Packet Session Border Controllers (SBCs). SBCs are often deployed between a unified communications system and a service provider network. UC Monitor reports can display data from the SBC Call Detail Records (CDRs). The SBCs push the CDRs to the UC Monitor management console, which is configured as the FTP receiver.

This use case helps a network administrator configure the SBCs so that call accounting data and QoS metrics are displayed in UC Monitor reports. UC Monitor automatically discovers properly configured SBCs when calls pass through them.

This section contains the following topics:

Configure the SBCs (see page 29)

Configure the SBCs

Use the SBC accounting configuration and realm configuration (in Superuser mode) to set the parameters for the following tasks. Consult your SBC *Accounting Guide* and *ACLI Configuration Guide* for instructions on setting the parameters. Perform the tasks for each SBC that you want to monitor.

The following tasks identify only the parameters that UC Monitor requires.

Perform the following tasks in the SBC account-config:

1. Enable local CDR storage.

   file-output

   Set this parameter to **enabled** to create CDRs in comma-separated format.

   file-path

   This parameter is required to enable the FTP push feature. Either location, /ramdrv or /ramdrv/logs, is acceptable as long as the location is configured for FTP push.

   max-file-size

   The default value is acceptable.

max-files

The default value is acceptable.

file-rotate-time

This parameter controls how often UC Monitor receives the CDRs. Set it to a value from a minimum of 2 minutes to a maximum of 5 minutes.

2. Set the CDR file format.

vsa-id-range

Leave this parameter blank.

cdr-output-inclusive

Set this parameter to **enabled** to fill empty CDR fields with "0" to provide a consistent presentation of columns when the CDR is output in .csv format.

3. Enable FTP push and identify the push receiver.

ftp-push

Set this parameter to **enabled**.

push-receiver:

- **server**. Set this parameter to the IP address of the UC Monitor management console server.

  Note: UC Monitor installation creates an FTP site on the management console that supports login by an anonymous user. If your environment requires secure FTP, you can configure any server as the secure FTP recipient, as long as that server then pushes the CDRs to the following location on the management console:
  <*install directory*>\VoipMonitor\FTPSite\ACME.

- **port**. This parameter identifies the port number on the management console server. Set it to **21**.
- **remote-path**. This parameter identifies where the CDR files are saved on the management console. Set it to **/ACME**.
- **filename-prefix**. Leave this parameter blank.
- **protocol**. Set this parameter to **FTP**.

- **username**. Use the anonymous login credentials, unless otherwise specified by your administrator
- **password**. Use the anonymous login credentials, unless otherwise specified by your administrator.

Perform the following task in the SBC realm-config:

1. Enable QoS metrics.

   qos-enable

   Set this parameter to **enabled** to generate QoS metrics for UC Monitor reports. Enable QoS for the originating realm.

Index

A

C

M

S