CA Unified Communications Monitor

Monitoring Medianet 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: Introduction

A medianet is an IP architecture that enhances the performance of video, voice, and data, and automates many aspects of configuration. CA Unified Communications Monitor (UC Monitor) employs passive monitoring to gather data from unidirectional traffic flows from medianet-enabled (midstream) devices, such as switches and routers.

This document describes how UC Monitor monitors your medianet environment, and includes configuration requirements, report descriptions, and database settings.

Chapter 2: How UC Monitor Monitors Medianet Traffic

UC Monitor receives data about medianet-enabled (midstream) devices from Cisco IOS Flexible NetFlow. This data lets UC Monitor monitor the performance of Real-Time Transport Protocol (RTP) traffic on the midstream devices in your network.

Medianet data consists of device information and flow metrics (audio and video), including interface names and data from stream legs. A *stream leg* is a unidirectional stream of packets. Data from these midstream legs can help your troubleshooting efforts in situations such as the following examples:

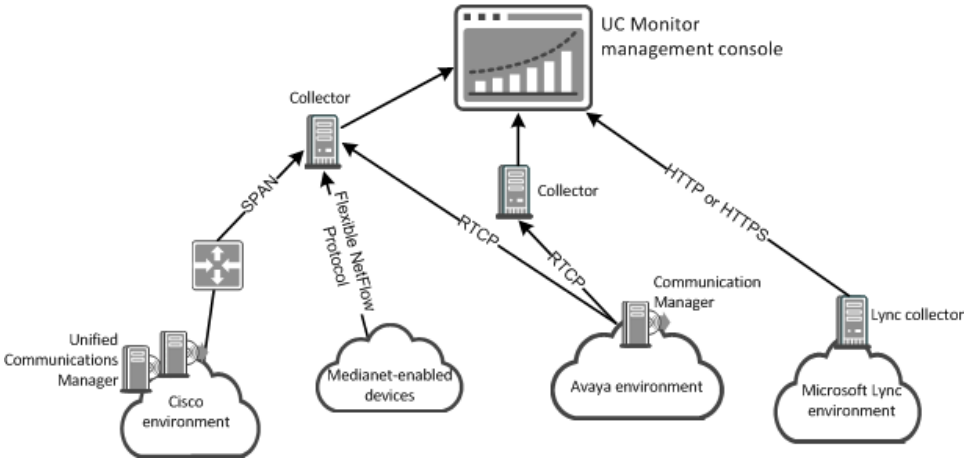
- Review video monitoring statistics for one video flow after a user submits a trouble ticket.
- Monitor all video flows from a particular source to verify the quality of video that enters the network.

The UC Monitor support for monitoring medianet data works as follows:

- Throughout a call, medianet-enabled devices (midstream routers and switches) send real-time data to the Harvester on the collector.
- UC Monitor discovers a midstream device for every IP address that sends data.
- The Harvester parses and aggregates the data every 5 seconds and sends the data to the management console.
- The management console stores the data in the database, for display in reports.
  - If the call is in progress, real-time midstream metrics are available from the Midstream Legs (see page 17) report, which identifies the RTP traffic flows (or unidirectional stream legs) on the medianet-enabled devices.
  - If the call has ended, the real-time midstream metrics are correlated with other call metrics (from phones and gateways, for example) and then associated with a specific call. The correlated metrics are available from the Midstream Metric Details (see page 15) chart in the Call Watch Details report.

Note: UC Monitor supports reporting on an indefinite number of midstream devices. In addition, midstream devices do not count toward the UC Monitor license.

The following diagram illustrates a UC Monitor deployment that includes medianet and Cisco Unified Communications Manager, Avaya Communication Manager, and Microsoft Lync:



Chapter 3: How to Configure Medianet-enabled Devices

Use the following information when configuring your medianet-enabled devices to be monitored with UC Monitor. 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 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.

Chapter 4: Reports for Troubleshooting

The Troubleshooting reports help network engineers explore performance metrics, plan for network changes, and identify performance issues at a particular VoIP endpoint. Data from SPAN and from endpoints while calls are in progress help you track statistics such as:

- When calls are made
- Where calls come from
- How calls are routed
- How calls perform

This section contains the following topics:

Midstream Details Tables

The Midstream Details tables provide in-depth data about the performance of RTP traffic flows (or stream legs) on the medianet-enabled devices on your network.

Device

The name of the medianet-enabled (midstream) device that is associated with the stream leg. Can be the DNS name or the IP address.

DSCP

The Differentiated Services Code Point setting of the incoming RTP packets.

Egress Interface

The interface where traffic exits a device.

Forwarding Status

When applicable, this field explains why a medianet-enabled device did not forward packets as expected. For example, when the device drops packets, this field provides a Status of “Dropped” and a Reason such as “Bad TTL.”

The device manufacturer provides the Status and Reason descriptions. Two other descriptions provided in this field, Value and Extended, are not defined, and can vary depending on the Status and Reason.

When a forwarding status is available, this field contains a blue “i” icon. Position your mouse pointer over the “i” to review the information.

Ingress Interface

The interface where traffic enters a device.

Jitter, Max Jitter

Packet delay that distorts the quality of a voice conversation. Either the average or the maximum value for the stream leg.

Packet Loss

The percentage of data packets that were lost in transit. These packets were sent but never received at the destination.

Packet Rate

The number of data packets that are received per second. UC Monitor uses this value to determine whether an RTP stream is audio or video for medianet-enabled devices that do not report a codec.

Packets Dropped

The number of data packets that reached the destination, but then were discarded.

Packets Lost

The number of data packets that were lost in transit. These packets were sent but never received at the destination.

Packets Received

The number of data packets in a stream.

TTL

(Time to Live) A counter embedded in data to prevent a data packet from circulating through the network indefinitely. The counter decrements each time that the packet passes through a router or a switch.

Video Jitter, Video Max Jitter

The variation in delay among video packets in the same stream. Either the average or the maximum value.

Video Packet Loss

The percentage of video packets that were lost in transit. These packets were sent but never received at the destination.

Video Packet Rate

The number of video packets that were received per second.

Video Packets Dropped

The number of video packets that reached the destination, but then were discarded.

Video Packets Lost

The number of video packets that were lost in transit. These packets were sent but never received at the destination.

Video Packets Received

The number of video packets in a stream.

Midstream Metric Details

When the Call Details page contains Midstream Details tables, you can drill down to the Midstream Metric Details page for per-metric information.

The Origination and Destination Information sections provide details about the endpoints at the beginning and end of the stream.

The Midstream Details tables (see page 13) are the same as the tables on the Call Details page.

The charts on the Midstream Metric Details page are graphical representations of the metrics from the Midstream Details tables: one chart per metric per direction of the stream leg. Each chart graphs the metric over the length of the stream leg for the ingress and egress interfaces of medianet-enabled devices.

Important: When Call Watch and midstream data exist for a call, the Midstream Metric Details (see page 15) charts are part of the Call Watch Details report.

Midstream Devices

The Midstream Devices page provides an overview of the performance of RTP traffic flows (or stream legs) on the medianet-enabled devices on your network. A *stream leg* is a unidirectional stream of packets.

ID

A link to the Calls Overview, where you can drill down to more information.

IP Address

The IP address of the medianet-enabled device that is associated with the stream leg.

Last Activity

The date and time of the most recent activity for the medianet-enabled device.

Max Jitter

Packet delay that distorts the quality of a voice conversation.

Max Packet Loss

The percentage of data packets that were lost in transit. These packets were sent but never received at the destination.

Name

The name of the medianet-enabled device that is associated with the stream leg. Can be the DNS name or the IP address. If UC Monitor is a registered data source for CA Performance Center, the name is a link to the CA Performance Center context page.

Packets Dropped

The number of data packets that reached the destination, but then were discarded.

Stream Count

The number of active and completed stream legs that are used to calculate the metrics on the Midstream Devices page. The number is a link to the Midstream Legs (see page 17) page.

Video Max Jitter

The variation in delay among video packets in the same stream.

Video Max Packet Loss

The percentage of video packets that were lost in transit. These packets were sent but never received at the destination.

Video Packets Dropped

The number of video packets that reached the destination, but then were discarded.

Midstream Legs

The Midstream Legs page identifies the RTP traffic flows (or stream legs) on the medianet-enabled devices on your network. A *stream leg* is a unidirectional stream of packets. An active stream leg is not yet associated with the end-of-call record for a device.

You can filter the information in the Midstream Leg List with the Media Type and Status lists.

The Midstream Leg List provides the following information:

Average MOS

The Mean Opinion Score (MOS) is an industry standard method for gauging call quality. MOS is an estimation of how impairments to a voice signal affect listener perception of call quality.

MOS calculated from medianet data considers only the codec and any packet loss metrics. Other impairment metrics traditionally associated with a MOS, such as latency and jitter buffer loss, are unknown in medianet streams. Therefore, the MOS for medianet streams may be higher (better) than MOS reported from the endpoints, where all impairment metrics are known.

Codec

The codec in use for the stream leg, or one of the following descriptions:

- "n/a" indicates that a codec exists, but UC Monitor does not recognize it. Or that the router did not send codec information.
- "Dynamic Payload" indicates a video stream leg.
- A dash (-) or "unavailable" indicates that no codec existed for the stream leg.

This field is disabled by default. Click the Settings link to include the field in the Midstream Leg List.

Destination IP Address

The IP address of the device that received the stream leg.

Destination Location

The Location of the device that received the stream leg.

Destination Port

The port number through which the device that received the stream leg. This field is disabled by default. Click the Settings link to include the field in the Midstream Leg List.

DSCP

The Differentiated Services Code Point setting of the incoming RTP packets. Two or more values in this field indicate that the DSCP changed over the course of the stream.

Duration

The length of the stream leg.

ID

A link to the Midstream Leg Information (see page 19) page, and to charts representing MOS, packet loss, average jitter, and maximum jitter.

Last Activity

The last time data was processed for the stream leg. The end time appears on the Midstream Leg Information (see page 19) page.

Media Type

The type of media in the stream leg: Audio or Video.

Packet Loss

The percentage of data packets that were lost in transit. These packets were sent but never received at the destination.

Source IP Address

The IP address of the device that sent the stream leg.

Source Location

The Location of the device that sent the stream leg.

Source Port

The port through which the device sent the stream leg. This field is disabled by default. Click the Settings link to include the field in the Midstream Leg List.

SSRC

The contents of the SSRC field in the RTP header. Also a unique identifier of the source of the stream leg. This field is disabled by default. Click the Settings link to include the field in the Midstream Leg List.

Midstream Leg Information

The tables on the Midstream Leg Information page provide some or all of the following information. The charts below the tables present MOS, packet loss, average jitter, and maximum jitter for the stream leg.

Average MOS, Minimum MOS

The Mean Opinion Score (MOS) is an industry standard method for gauging call quality. MOS is an estimation of how impairments to a voice signal affect listener perception of call quality. Either the average or minimum value for the midstream leg.

MOS calculated from medianet data considers only the codec and any packet loss metrics. Other impairment metrics traditionally associated with a MOS, such as latency and jitter buffer loss, are unknown in medianet streams. Therefore, the MOS for medianet streams may be higher (better) than MOS reported from the endpoints, where all impairment metrics are known.

Call ID

The ID number of the call to which the midstream leg becomes associated. The ID is a link to the call details on the Calls Overview page.

The call ID is "Unavailable" when the midstream leg is not associated with a call. For example, the caller dials a number, which generates stream legs. The callee does not answer, so the call is incomplete. Midstream legs are not associated with incomplete calls.

Codec

The codec in use for the stream leg, or one of the following descriptions:

- "n/a" indicates that a codec exists, but UC Monitor does not recognize it. Or that the router did not send codec information.
- "Dynamic Payload" indicates a video stream leg.
- A dash (-) or "unavailable" indicates that no codec existed for the stream leg.

Duration

The length of the stream leg.

Egress Interface

The interface where traffic exits a device.

End

The date and time that the stream entered the destination port.

Forwarding Status

When applicable, this field explains why a medianet-enabled device did not forward packets as expected. For example, when the device drops packets, this field provides a Status of “Dropped” and a Reason such as “Bad TTL.”

The device manufacturer provides the Status and Reason descriptions. Two other descriptions provided in this field, Value and Extended, are not defined, and can vary depending on the Status and Reason.

When a forwarding status is available, this field contains a blue “i” icon. Position your mouse pointer over the “i” to review the information.

ID

The ID number of the stream leg. Matches the ID number from the Midstream Legs page.

Ingress Interface

The interface where traffic enters a device.

IP Address

The IP addresses of the devices that sent and received the stream leg, and a link to more information.

Jitter, Max Jitter

Packet delay that distorts the quality of a voice conversation. Either the average or the maximum value for the midstream leg.

Location

The Locations of the devices that sent and received the stream leg. Can be <Unassigned> or another defined Location.

Media Type

The type of media in the stream leg: Audio or Video.

Packet Loss

The percentage of data packets that were lost in transit. These packets were sent but never received at the destination.

Packet Rate

The number of data packets that are received per second. UC Monitor uses this value to determine whether an RTP stream is audio or video for medianet-enabled devices that do not report a codec.

Packets Dropped

The number of data packets that reached the destination, but then were discarded.

Packets Lost

The number of data packets that were lost in transit. These packets were sent but never received at the destination.

Packets Received

The number of data packets in a stream.

Port

The port number through which the devices sent and received the stream leg.

SSRC

The contents of the SSRC field in the RTP header. Also a unique identifier of the source of the stream leg.

Start

The date and time the stream left the source port.

TTL

(Time to Live) A counter embedded in data to prevent a data packet from circulating through the network indefinitely. The counter decrements each time that the packet passes through a router or a switch.

Chapter 5: How to Manage the Database

UC Monitor uses a MySQL database for data storage. The database and the management console reside on the same server.

Periodic maintenance ensures that product functionality and performance are unaffected by database size. UC Monitor automatically purges data and optimizes database keys in the following situations:

- During scheduled database maintenance.
- When the CA UCM Inspector service starts on the management console.

Best Practice: For databases larger than 10 GB in size, defragment the *<install path>* drive every month. Before starting the defragmentation process:

- Maintain at least 20 percent of the drive as free disk space.
- Stop all CA UCM services, including the CA UCM MySql51 service. You can restart these services after defragmentation is complete.

This section contains the following topics:

Recommended Database Limits

The amount of data that can be stored in the database depends on the volume of call activity on your network. We recommend the following limits on data storage to avoid degraded performance. The database can accommodate 500 million rows per data table. We recommend no more than 200 million rows per data table, to allow for spikes in growth.

Call Volume	10 million calls per month	6.6 million calls per month	3.3 million calls per month
Data Type			
Interval data. Collected during regular monitoring at 15-minute intervals by the collector. Includes incident data.	5 months	8 months (default)	15 months

Call Volume	10 million calls per month	6.6 million calls per month	3.3 million calls per month
Summary data. Generated by the management console for long-range reports such as the Capacity Planning reports.	5 months	8 months (default)	15 months
Call data. Data about individual calls.	5 months	8 months (default)	15 months
Defined Call Watch data. Data from watched phones.	5 months	8 months (default)	15 months
Automatic Call Watch data. Data from automatically watched phones in Avaya environments.	3 days	7 days (default)	14 days
Midstream device data. Medianet flow metrics and device information. Recommendations are based on an average of three midstream devices per 3-minute call.	1 day	2 days (default)	4 days
Abandoned call data. Data from calls that were abandoned before they were completed.	Although some information about abandoned calls can be helpful, retaining too many of this type of call can lead to degradation of report performance. By default, data from abandoned calls is stored for three months.		

Change Database Settings

A UC Monitor administrator can perform the following database maintenance tasks:

- Change the data retention settings.
- Schedule system maintenance.
- Arrange to send SNMP traps or email warnings when available disk space falls below a threshold.

Follow these steps:

1. Click Administration, Console, Database, Maintenance in the navigation bar.

   The Database Maintenance page opens.

2. Complete the following fields:

   - **Save interval data for**. The length of time to store five-minute or 15-minute data. The default is eight months.

- **Save summary data for**. The length of time to store summary data. The management console periodically generates summary data, which is used for long-range reporting. The default is eight months.
- **Save call data for**. The length of time to store call data. The default is eight months. Store call data for at least as long as Call Watch data due to dependencies.
- **Save abandoned call data for**. The length of time to store data about abandoned calls. The default is three months.
- **Save call watch (Defined) data for**. The length of time to store data from your Call Watch definitions. The default is eight months. Do not store Call Watch data for longer than you store call data, due to dependencies.

  Note: Call Watch definitions apply only to Cisco IP phones.
- **Save call watch (Automatic) data for**. The length of time to store data from Avaya endpoints, which are watched automatically. The default is one week. Do not store Call Watch data for longer than you store call data, due to dependencies.
- **Save midstream device data for**. The length of time to store data from medianet-enabled devices, which is generated every 15 seconds. The default is two days.
- **Run system maintenance every**. The day of the week and the time at which system maintenance is performed. The default setting is Sunday at 12:00 AM (00:00).
- **When disk free space falls below**. The minimum allowable amount of available disk space. When the amount of free disk space falls below the threshold, UC Monitor sends a notification to the specified recipient. The default threshold is 5 GB.
- **Email warnings to**. Send an email message when the available disk space falls below the specified threshold. Provide the email address of the recipient.
- **Send SNMP traps to**. Send an SNMP trap when the available disk space falls below the specified threshold. Provide the name of the server or the IP address to receive the SNMP trap.

3. Click Save.

Purge Data from the Database

UC Monitor automatically purges data from the database during scheduled maintenance (see page 24). However, an administrator can purge selected data on demand. Purged data is *permanently* removed from the database. You *cannot* recover purged data.

Follow these steps:

1. Click Administration, Console, Database, Purge Data in the navigation bar.

   The Purge Data page opens.

2. Select from the following choices:

   - **Collected interval data**. Purge all five- or 15-minute data from regular monitoring, including all incident data.
   - **Collected summary data**. Purge all summary data that the management console generated for long-range reporting.
   - **Collected call watch data**. Purge all data from watched phones.
   - **Collected call and call watch data**. Purge all data from detailed call records and from watched phones.

     Note: If you enable this purge setting and also select "Purge prior to this date/time," UC Monitor retains data from the past 30 days. All other call and Call Watch data is purged. To purge all phone data, select "Purge all selected data."
   - **Collected midstream device data**. Purge all data from medianet-enabled devices.
   - **Abandoned calls**. Purge all data from abandoned calls.
   - **Purge all selected data**. Purge selected data across all dates.
   - **Purge prior to this date/time**. Purge data from a specific time frame. Enter a date and time before which all data is purged. Use the following format:

     `MM/DD/YYYY HH:MM:SS`

3. Click Purge.

   The Purge Data page opens.

4. Click Continue.

   The selected data is purged.