# CA Unified Communications Monitor

## Installation Guide

Version 3.3

# 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 7

## Chapter 2: System Requirements 9

Supported Operating System ....9
Supported Web Browsers ....9
Hardware Requirements for a Distributed System ....10
Hardware Requirements for a Standalone System ....11
Virtual Machine Requirements ....12
Firewall Requirements ....12
System Scalability ....13

## Chapter 3: Configuring the Hardware 15

Configure the Server for the Management Console ....15
Configure the Server for the Collector ....16
Configure the Server for a Standalone System ....16
Configure Network Interface Cards ....17
Configure Medianet-enabled Devices ....19

## Chapter 4: Installing the Software 21

Installation Prerequisites ....21
Install the Management Console ....22
Install the Collector ....22
Install All Components on One Server ....23

## Chapter 5: Post-Installation Tasks 25

Request a Product License ....25
Install Updates ....25
Change the Host Name ....25
Update the List of Trusted Internet Sites ....25
Synchronize the System Time ....26
Perform Configuration Tasks from the Management Console ....27

## Appendix A: Preparing an Avaya Environment 29

Architecture for Avaya Deployments ....30

Bandwidth Considerations ..... 31

Appendix B: Preparing a Cisco Environment 33

Architecture for Cisco Deployments ..... 33
Tips for System Scalability ..... 34

Appendix C: Preparing a Microsoft Lync Environment 35

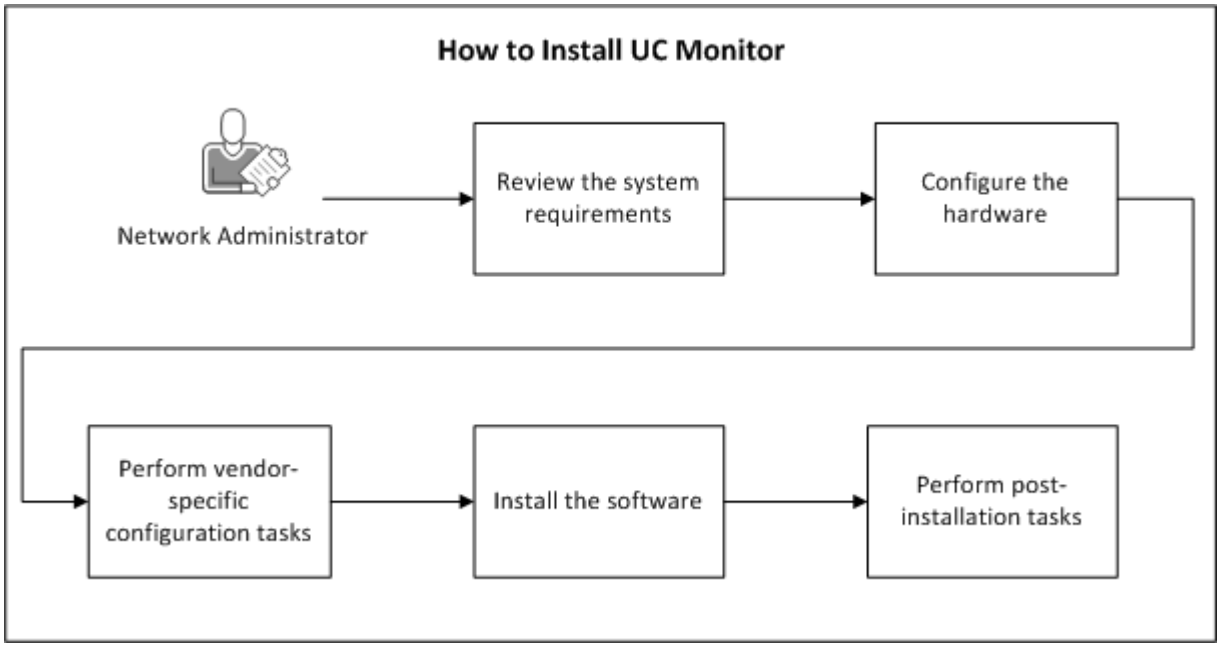
Architecture for Microsoft Deployments ..... 36
Bandwidth Considerations ..... 36

Appendix D: Example of UC Monitor in a Multi-Vendor Environment 39

Index 41

# Chapter 1: Introduction

The following diagram illustrates the process of installing and configuring the hardware and software for CA Unified Communications Monitor (UC Monitor), version 3.3:




The following topics describe the process of installing and configuring the hardware and software for UC Monitor:

- Review the system requirements (see page 9)
- Configure the hardware (see page 15)
- Perform vendor-specific configuration tasks:
  - Avaya environments (see page 29)
  - Cisco environments (see page 33)
  - Microsoft Lync environments
- Install the software (see page 21)
- Perform post-installation tasks (see page 25)

# Chapter 2: System Requirements

## Supported Operating System

All servers that host UC Monitor components have the following operating system requirements.

**Management console in a distributed system, or the server in a standalone system**

Microsoft Windows Server 2008 R2, Standard or Enterprise Edition

- Install the Application Server role with the following role services:
  - Web Server (IIS) Support, with IIS 6 Management Compatibility
  - COM+ Network Access
- Install and enable the following items:
  - SNMP
  - The most recent service pack and important updates

**Standard collector or small-site collector in a distributed system**

Microsoft Windows Server 2008 R2, Standard or Enterprise Edition

- Install and enable the following items:
  - SNMP
  - The most recent service pack and important updates

**Important**: UC Monitor version 3.3 supports Microsoft Windows Server 2008 R2. Although you can install the product on Microsoft Windows Server 2003, we cannot guarantee performance.

## Supported Web Browsers

Access to the management console is supported for the following browsers:

- Microsoft Internet Explorer 7 or 8
- Mozilla Firefox 9.x
- Google Chrome

Other browsers or versions may work but have not been tested with UC Monitor.

# Hardware Requirements for a Distributed System

In a *distributed* system, the collectors and the management console are installed on separate servers.

**Management Console**

The management console server contains the MySQL database and supports approximately ten standard collectors or 30 small-site collectors. CA has tested UC Monitor on servers with the following specifications. CA supports the management console on servers from any vendor, when the servers conform to these specifications, at minimum:

- Two Intel E5520 Xeon quad-core 2.66 GHz, 1333 MHz FSB processors
- 24 GB of RAM
- Six 146-GB SAS hard drives in RAID 5 configuration
- 300 GB of space on the installation drive (to accommodate potential database growth)
- Intel Copper GB or Intel Fiber GB network interface card
- PCI Express x16 slot expansion card
- Two 10/100/1000 Mbps Ethernet RJ-45 ports
- Intel 82576 Gigabit Ethernet Controller

**Standard Collector**

CA has tested UC Monitor on servers with the following specifications. CA supports the collector on servers from any vendor, when the servers conform to these specifications, at minimum:

- Intel E5520 Xeon quad-core 2.66 GHz, 1333 MHz FSB processor
- 3 GB of RAM
- Three 146-GB SAS hard drives in RAID 5 configuration
- 300 GB of space on the installation drive (to accommodate potential database growth)
- Intel Copper GB or Intel Fiber GB network interface card
- PCI Express x16 slot expansion card
- Two 10/100/1000 Mbps Ethernet RJ-45 ports
- Intel 82576 Gigabit Ethernet Controller

**Small-site Collector**

A distributed, *small-site*, system is available for deployments with multiple sites of 1,000 phones or fewer. CA supports the small-site collector on servers from any vendor, when the servers conform to the following specifications, at minimum:

- Intel Celeron E1500 2.2 GHz, 800 MHz FSB processor
- 2 GB of RAM
- SATA II 3.5-inch hard drive
- Intel Copper GB or Intel Fiber GB network interface card
- 10/100/1000 Mbps Ethernet RJ-45 port
- Two Intel single-port 82576 PCI-E Gigabit Ethernet Controllers

# Hardware Requirements for a Standalone System

A *standalone* system consists of one server on which the management console and collector are installed. CA supports UC Monitor components on servers from any vendor, when the servers conform to the following specifications, at minimum:

- Two Intel E5520 Xeon quad-core 2.66 GHz, 1333 MHz FSB processors
- 24 GB of RAM
- Six 146-GB SAS hard drives in RAID 5 configuration
- 300 GB of space on the installation drive (to accommodate potential database growth)
- Intel Copper GB or Intel Fiber GB network interface card
- PCI Express x16 slot expansion card
- Two 10/100/1000 Mbps Ethernet RJ-45 ports
- Intel 82576 Gigabit Ethernet Controller

# Virtual Machine Requirements

UC Monitor is supported in virtual environments.

- You can install UC Monitor components on virtual machines that meet or exceed the hardware requirements.
- To achieve equal performance in an environment that stresses a physical server, more memory is required on a virtual machine than on a physical server. Physical servers outperform virtual machines in the area of disk I/O. UC Monitor tasks the disk I/O heavily. You can expect less-than-equal performance on a virtual machine.
- In a Cisco environment, send SPAN traffic to the monitor NIC. For more information, see the following topics:
  - Configure Network Interface Cards (see page 17)
  - Preparing a Cisco Environment (see page 33)
- To install the UC Monitor software on a virtual machine, follow the instructions in Installing the Software (see page 21).

**More information:**

Hardware Requirements for a Distributed System (see page 10)
Hardware Requirements for a Standalone System (see page 11)

# Firewall Requirements

UC Monitor uses several ports and protocols to enable communications among the management console, collectors, and monitored systems. Use the following information to ensure that communications can pass active firewalls in your network.

**TCP port 1000**

Open this port for communication from the management console to the collectors. The management console sends instructions, data-collection parameters, and other configuration information to the collectors. The CA UCM Collector Communication Service uses this port.

**TCP port 1001**

Open this port for communication from the collectors to the management console. The CA UCM Console Communicator service uses this port.

**TCP port 9000**

Open this port to allow CDR data from the Avaya Communication Manager.

**UDP port 162**

Open this port to let the collectors send SNMP traps to a trap receiver.

**UDP port 5005**

Open this port to allow RTCP data from Avaya endpoints.

**UDP port 9995**

Open this port when monitoring medianet environments.

**Internet Control Message Protocol**

Enable ICMP to let the collector send traceroutes to an endpoint.

The default port settings are stored in the UC Monitor database and in the Windows Registry on the collector server. You can change these ports when necessary. For assistance, contact CA Technical Support.

# System Scalability

Some VoIP equipment vendors discuss scalability in terms of the number of IP phone users or the expected number of calls. Others use the terms busy hour call completions (BHCC) and busy hour call attempts (BHCA). These terms represent the number of calls or call attempts that can be processed during the busiest hours of the day.

The UC Monitor components, particularly the collector, support a BHCA of 25,000. In laboratory testing, the collector handled a higher BHCA. The collector is designed to handle temporary situations where the volume of VoIP traffic is far greater than normal.

# Chapter 3: Configuring the Hardware

When configuring the hardware, you need the following types of cables.

**Power cable**

Connects the UC Monitor server to a power supply, preferably a UPS.

**Management NIC cable**

One of the following types:

- Copper NIC cable
- Gb fiber NIC cable

When plugged into a switch, the management NIC provides network access to the UC Monitor server and it enables remote viewing of the management console.

**Monitor NIC cable**

Collects network traffic from a SPAN port on the switch.

## Configure the Server for the Management Console

The management console and the collectors are installed on separate servers in a distributed system. The following procedure describes how to configure the server for the management console.

**Follow these steps:**

1. Connect one end of the power cable to the power outlet on the server.
2. Connect the other end of the power cable to a power supply.
3. Connect one end of the management cable to a NIC on the server.
4. Connect the other end of the management cable to an appropriate switch.
5. Turn on the server.
6. Configure the monitor and management NICs. For more information, see Configure Network Interface Cards (see page 17).
7. Configure medianet-enabled devices. For more information, see Configure Medianet-enabled Devices (see page 19).
8. Configure the server for the collector. For more information, see Configure the Server for the Collector (see page 16).

# Configure the Server for the Collector

The management console and the collectors are installed on separate servers in a distributed system. You can have a maximum of ten standard collectors per management console, or 30 small-site collectors per management console. The following procedure describes how to configure the server for the collector.

**Follow these steps:**

1. Connect one end of the power cable to the power outlet on the server.
2. Connect one end of the monitor and management cables to NICs on the server.
3. Connect the monitor cable to the SPAN port.
4. Connect the management cable to the management console server.
5. Turn on the server.
6. Configure the monitor and management NICs. For more information, see Configure Network Interface Cards (see page 17).
7. Configure medianet-enabled devices. For more information, see Configure Medianet-enabled Devices (see page 19).

# Configure the Server for a Standalone System

In a standalone system, the management console and the collector are installed on the same server.

**Follow these steps:**

1. Connect one end of the power cable to the power outlet on the server.
2. Connect the other end of the power cable to a power supply.
3. Connect one end of the monitor and management cables to NICs on the server.
4. Connect the other end of the monitor cable to the switch where call servers are connected.
5. Connect the other end of the management cable to another switch, to enable network access to the management console.
6. Configure the monitor and management NICs. For more information, see Configure Network Interface Cards (see page 17).
7. Configure medianet-enabled devices. For more information, see Configure Medianet-enabled Devices (see page 19).

# Configure Network Interface Cards

After connecting the hardware, configure the network interface cards (NICs) on the collector and management console computers. In a standalone system, all configuration takes place on one computer.

- On each collector computer, set up network connections for the management and monitor NICs.
- On the management console computer, set the priority of the management NIC.
- Assign a static IP address, subnet mask, and default gateway to the management NIC.

**Note**: The other NICs on the collector, including the monitor NIC, do not transmit data to the network. The IP addresses assigned to them do not need to be valid for the network to which they are connected, nor do they require a default gateway assignment.

*When you purchase hardware from CA Technologies*, the NIC settings are configured by a CA representative. Use the following procedure to verify the settings or update them as necessary.

*When you purchase hardware from a different vendor*, perform the following procedure.

**Follow these steps:**

1. Navigate to the Network Connections window from the Control Panel on the collector and management console computers.
2. Review the names of the LAN or High-Speed Internet Connections. If necessary, change the default names to correspond to the interfaces, as shown in the following table:

   **Copper Ethernet adapter**

   Default name: Local Area Connection 2

   New name: Management

   **Copper Ethernet adapter**

   Default name: Local Area Connection 3

   New name: Monitor

   **Gigabit fiber port**

   Default name: Local Area Connection

   New name: Fiber Monitor

   **Tip**: You can identify devices by disconnecting the cable from the back of the device and noting which interface status changes to "disconnected" in the Network Connections dialog.

3. Disable unused monitor NICs:
   a. Right-click the NIC.
   b. Select Disable.
4. Click Advanced, Advanced Settings.
5. Click the up arrow to move the management NIC to the first position in the Connections pane. This action sets the priority and enables UC Monitor to operate correctly.
6. Clear the following “Internet Protocol (TCP/IP)” check boxes for the monitor NIC:
   - File and Printer Sharing for Microsoft Networks
   - Client for Microsoft Networks
7. Click OK.
8. Navigate to the Control Panel and select Network Connections, Local Area Connection.
9. Click Properties on the General tab.
10. Select Internet Protocol (TCP/IP) and click Properties.
11. Select “Use the following IP address” and enter an IP address, subnet mask, and default gateway.
12. Select “Use the following DNS Server addresses” and supply the IP address for the DNS server.

    **Note**: Do not use a DHCP address.
13. Repeat steps 11 and 12 for the monitor NICs, using the following suggested values:

    **Monitor NIC**

    IP address: 1.1.0.0

    Subnet mask: 255.0.0.0

    **Fiber Monitor NIC**

    IP address: 1.1.0.1

    Subnet mask: 255.0.0.0

# 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 the Flexible NetFlow protocol. Medianet data appears in the Midstream Devices reports.

Configure your medianet-enabled devices as follows. We recommend that you consult your network engineer or device vendor when configuring your devices for medianet.

For more information about using the Performance Monitor commands described in the following table, consult the *Cisco IOS Media Monitoring Command Reference* guide.

| Component | Description |
|---|---|
| IPv4 | Configure the devices for IPv4 routing. |
| 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.<br>To configure the duration of the collection interval for a Performance Monitor policy, use the interval duration command in monitor parameters configuration mode. |

| Component | Description |
|---|---|
| Flow Monitor | When possible, use the predefined RTP record format (default-rtp) for the Flow Monitor record format.<br>When you create a custom record format, use at least use the following collect and match Performance Monitor commands when creating the record:<br>■ match ipv4 protocol<br>■ match ipv4 source address<br>■ match ipv4 destination address<br>■ match transport source-port<br>■ match transport destination-port<br>■ match transport rtp ssrc<br>■ collect ipv4 dscp<br>■ collect ipv4 ttl<br>■ collect transport packets lost counter<br>■ collect transport rtp jitter mean<br>■ collect transport rtp jitter maximum<br>■ collect interface input<br>■ collect interface output<br>■ collect application media packets counter<br>■ collect application media packets rate |
| Flow Exporter | In the Flow Exporter configuration, set the export destination (the collector) and the SNMP index-to-name mapping.<br>■ To configure the destination for a Performance Monitor Exporter, use the destination command in config-flow-exporter configuration mode.<br>■ To configure the interface-table option for a Performance Monitor Exporter, use the option command in config-flow-exporter configuration mode. |

# Chapter 4: Installing the Software

*When you purchase hardware from CA Technologies*, all components are delivered with the UC Monitor software installed. Do not install the software.

*When you purchase hardware from a different vendor*, install the UC Monitor software on all management console and collector servers.

**Important**: Do not install UC Monitor on a computer on which CA Performance Center is installed.

## Installation Prerequisites

Before you install the UC Monitor software, perform the following tasks:

- Prepare your Avaya, Cisco, or Microsoft environment.
- Install CA Performance Center in your environment. UC Monitor is a data source for CA Performance Center. CA NetQoS Performance Center 6.1 is also supported.
- Disable the following types of third-party software on all servers that host UC Monitor components:
  - Anti-virus
  - Anti-spyware
  - Server monitoring and maintenance tools such as SMS, SUS, or MoM
- Restart all servers to ensure that available operating system patches are applied.
- Obtain the UC Monitor setup file, UCMSetup3.3.xxx.exe, from CA Technical Support.
- Extract or copy the UCMSetup3.3.xxx.exe file to the servers on which you want to install the software.
- Verify that the setup program has permission to run:
  a. Right-click the setup program and select Properties.
  b. Click Unblock.
  c. Click OK.

**More information**

Preparing an Avaya Environment (see page 29)
Preparing a Cisco Environment (see page 33)

# Install the Management Console

Distributed systems have separate servers for the UC Monitor management console and the collectors. Use this procedure to install the management console for a distributed system.

**Follow these steps:**

1. Double-click the setup program.

   The Welcome window opens.

2. Click Next.

   The License Agreement window opens.

3. Read and accept the license agreement, and then click Next.

   The Choose Install Set window opens.

4. Select Unified Communications Monitor Management Console, and then click Next.

   The Choose an Install Folder window opens.

5. (*Optional*) Click Choose to select a different installation location. The default is C:\CA.

6. Click Next.

   The Pre-Installation Summary window opens.

7. Confirm your selections, then click Install.

   The installation process begins. Messages indicate the progress of the installation. When installation is complete, the Install Complete window opens.

8. Select "Yes, restart my system now," then click Done.

9. Run the setup program on the collector computers (see page 22).

   Your system is ready for post-installation tasks (see page 25).

# Install the Collector

Distributed systems have separate servers for the UC Monitor console and the collectors. Use this procedure to install the collectors in a Cisco or Avaya environment.

**Note**: Do not install a collector in a Microsoft Lync environment. For more information, see Architecture for Microsoft Deployments (see page 36).

**Follow these steps:**

1. Double-click the setup program.

   The Welcome window opens.

2. Click Next.

   The License Agreement window opens.

3. Read and accept the license agreement, and then click Next.

   The Choose Install Set window opens.

4. Select Unified Communications Monitor Collector, and then click Next.

   The Choose an Install Folder window opens.

5. (*Optional*) Click Choose to select a different installation location. The default is C:\CA.

6. Click Next.

   The Pre-Installation Summary window opens.

7. Confirm your selections, then click Install.

   The installation process begins. Messages indicate the progress of the installation. When installation is complete, the Install Complete window opens.

8. Select "Yes, restart my system now," then click Done.

   Your system is ready for post-installation tasks (see page 25).

# Install All Components on One Server

A *standalone* system contains one server that hosts the UC Monitor console and collector. Use this procedure to install the management console and the collector on one server.

**Follow these steps:**

1. Double-click the setup program.

   The Welcome window opens.

2. Click Next.

   The License Agreement window opens.

3. Read and accept the license agreement, and then click Next.

   The Choose Install Set window opens.

4. Select Unified Communications Monitor Standalone, and then click Next.

   The Choose an Install Folder window opens.

5. (*Optional*) Click Choose to select a different installation location. The default is C:\CA.
6. Click Next.

   The Pre-Installation Summary window opens.
7. Confirm your selections, then click Install.

   The installation process begins. Messages indicate the progress of the installation. When installation is complete, the Install Complete window opens.
8. Select "Yes, restart my system now," then click Done.

   Your system is ready for post-installation tasks (see page 25).

# Chapter 5: Post-Installation Tasks

## Request a Product License

You should have received a product license when you purchased UC Monitor. A license lets the console display the collected data. Without a license, UC Monitor still collects data, but that data is not available in reports.

If you do not have a product license, contact the CA Customer Care Team at CA Support Online for assistance with registering the software.

## Install Updates

Install all important updates, including the most recent service pack, that are available for the Microsoft Windows operating system.

Install any UC Monitor updates available from the CA Support Online website.

## Change the Host Name

For the collectors in a distributed system, change the host name assigned by CA Technologies. A naming convention similar to the following can help you identify the collector computers:

```
<CollectorName>-<ManagementConsoleName>-<Location>
```

For example:

```
ComMgr1-MainOffice-NYC
```

## Update the List of Trusted Internet Sites

Add the console computer to the list of trusted Internet sites. The process varies by browser. The following instructions are for Microsoft Internet Explorer.

**Follow these steps:**

1. Launch Internet Explorer on the console computer.
2. Click Tools, Options.
3. Click the Trusted Sites icon on the Security tab.

4. Click Sites.
5. Enter **http://localhost** in the "Add this Web site to the zone" field.
6. Click Add.

# Synchronize the System Time

Synchronize the system time among all servers where you installed UC Monitor components. Perform the following steps on each server.

**Follow these steps:**

1. Right-click the date or time on the right edge of the taskbar and select "Adjust date/time."

   The Date and Time dialog opens.
2. Click the Internet Time tab.
3. Click "Change settings."

   The Internet Time Settings dialog opens.
4. Select the check box labeled "Synchronize with an Internet time server."
5. Select the server with which you want to synchronize. The default is time.windows.com.
6. Click Update Now.

   The system time is synchronized with the selected server.
7. Click OK in the Internet Time Settings dialog.
8. Click OK in the Date and Time dialog.

**Note**: If you have collection devices in different time zones, set each device to its local time zone. Times are converted to Greenwich Mean Time (GMT).

# Perform Configuration Tasks from the Management Console

Perform the following configuration tasks from the UC Monitor management console:

- Organize phones, endpoints, gateways, and other network components into Locations.
- Add collection devices.
- Customize collector thresholds.
- Customize performance thresholds.
- Enable incidents to trigger response notifications.
- Register UC Monitor as a data source for CA Performance Center.
- Configure SNMP profiles for Cisco voice gateways.
- Configure users and their roles.

**Note**: For more information, see the UC Monitor online help or the *CA Unified Communications Monitor Administrator Guide*.

# Appendix A: Preparing an Avaya Environment

UC Monitor monitors unified communications deployments that rely on the Avaya Communication Manager for call processing. The collector monitors voice calls made with the following Avaya components:

- Desk phones and soft phones
- Communication Manager, including Aura Communication Manager
- Avaya voice gateways

Both the collector and the management console are required for monitoring an Avaya unified communications environment.

Avaya endpoints, including voice gateways, send frequent call-quality reports directly to the collector while calls are in progress. The quality data is sent as RTCP packets. Using SNMP, the collector periodically polls the Communication Manager for device information. The Communication Manager can be configured to send CDR data to the collector after each call is completed.

Many Avaya gateways have an AVAYA_RTP_MIB that can be polled with SNMP. However, RTCP is supported for *all* Avaya gateways. Therefore, UC Monitor relies primarily on RTCP for collecting metrics in an Avaya environment. No switch port or SPAN is required.

An Avaya network administrator performs several tasks to prepare an Avaya environment for monitoring with UC Monitor:

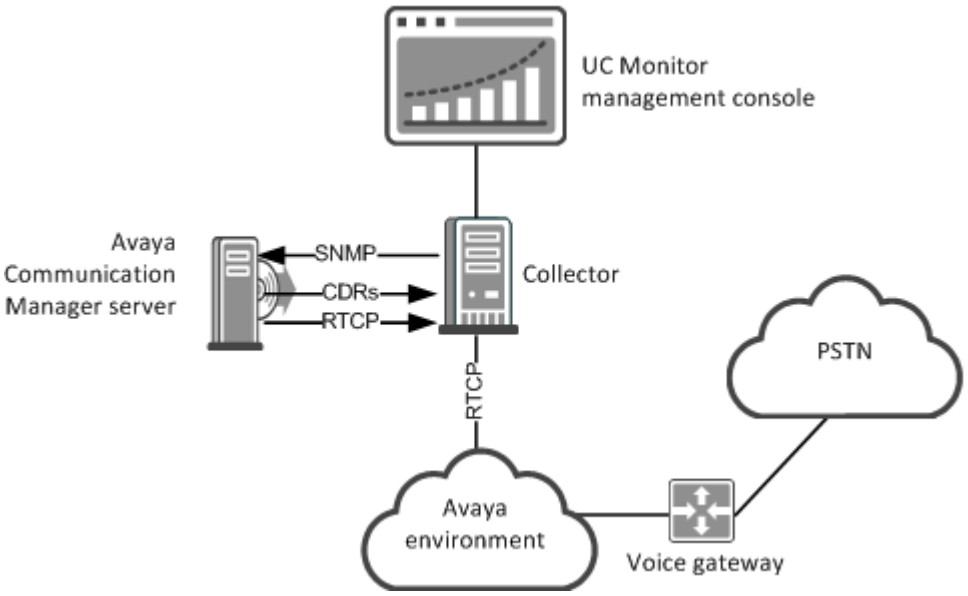
- Enabling access to SNMP agents.
- Enabling Avaya endpoints to send RTCP data to the UC Monitor collector, which takes the role of the RTCP Monitor in an Avaya system.
- Configuring the UC Monitor collector as a CDR recipient.
- Using the Trunk Group Measurement Selection page (in the Communication Manager web interface) to identify the trunk groups that you want to monitor.

**Note**: Detailed instructions for these tasks are provided in the use case titled "Preparing an Avaya Environment Before Installing CA Unified Communications Monitor." You can find the use case on the UC Monitor bookshelf on https://support.ca.com (see page 3).

# 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 less 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.

**More information**

Example of UC Monitor in a Multi-Vendor Environment (see page 39)

# 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.

# Appendix B: Preparing a Cisco Environment

UC Monitor monitors unified communications deployments that rely on the Cisco Unified Communications Manager for call processing. Cisco endpoints report quality data to their call server at the completion of every call. The UC Monitor collector inspects these flows for performance metrics. The collector transmits to the management console only the data necessary to calculate and report call setup and call quality.

A Cisco network administrator performs several tasks to prepare a Cisco environment for monitoring with UC Monitor:

- Enabling the Call Stats setting in a voice-quality-enabled SIP profile.
- Enabling the collection of call detail records (CDRs) and call management records (CMRs).
- Enabling the internal web server on IP phones.
- Configuring SPAN ports to mirror voice traffic to the collector.

**Note**: Detailed instructions for these tasks are provided in the following documents on the UC Monitor bookshelf on https://support.ca.com (see page 3).

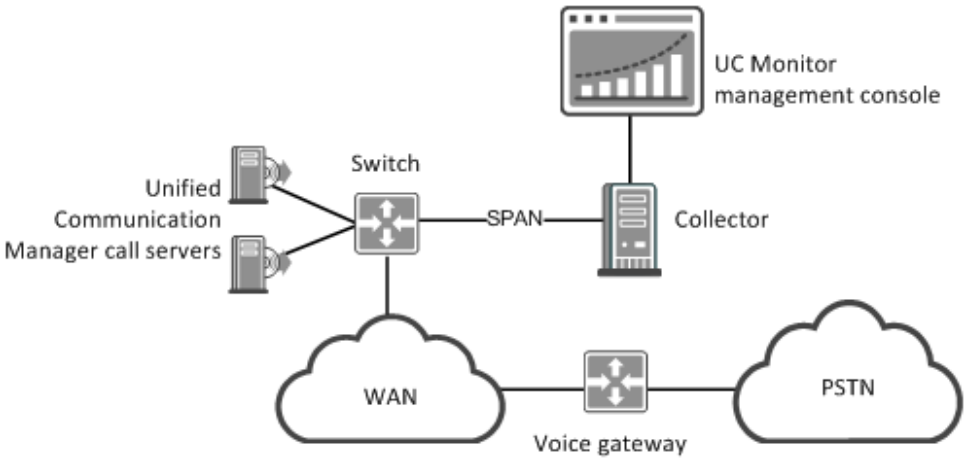
- Use Case: *Preparing a Cisco Environment Before Installing UC Monitor*
- Guide: *CA Best Practices for Data Acquisition*

## Architecture 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:




**More information**

Example of UC Monitor in a Multi-Vendor Environment (see page 39)

# Tips for System Scalability

Cisco recommends that you deploy Unified Communications Manager 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.

**More information:**

System Scalability (see page 13)

# Appendix C: Preparing a Microsoft Lync Environment

UC Monitor supports VoIP and video deployments that use Microsoft Lync Server 2010. 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. Instead, the standard system can process VoIP and video calls. Audio and video calls are integrated with other Microsoft Office applications, such as Outlook and SharePoint, 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.

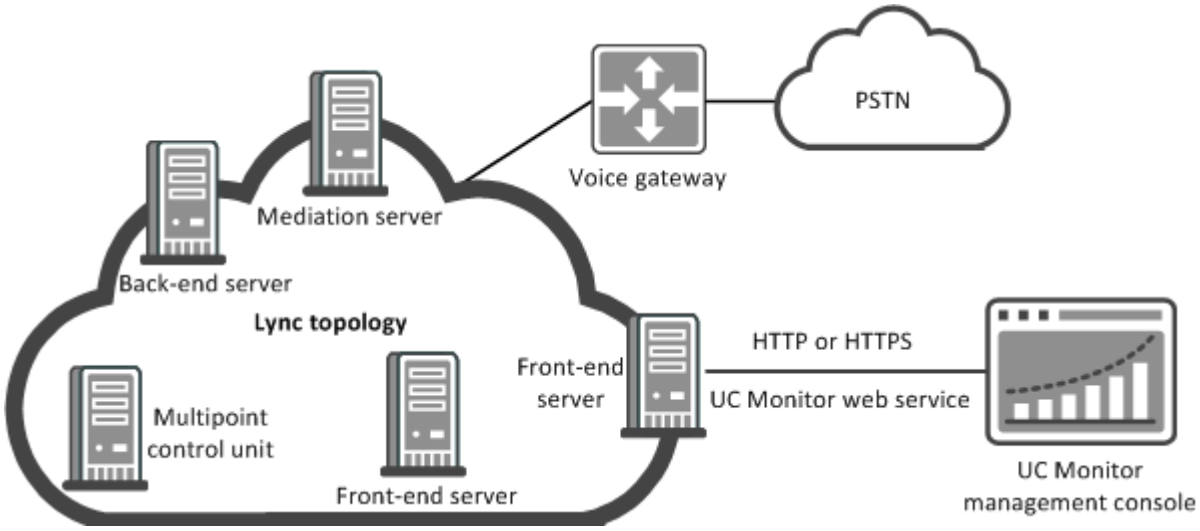
A Lync network administrator can configure HTTPS or use authentication certificates to enable secure communication between Lync servers and UC Monitor. UC Monitor does not require HTTPS or authentication certificates, but your environment may require them.

**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 UC Monitor collector, UC Monitor leverages data that from the Microsoft front-end server or standalone Standard Edition server.

In a Microsoft Lync environment, the front-end server 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 Microsoft collection devices, see the use case titled *Managing Collectors in a Microsoft Lync Environment*.

# Bandwidth Considerations

In our testing, we took measurements of quality report size and volume 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**

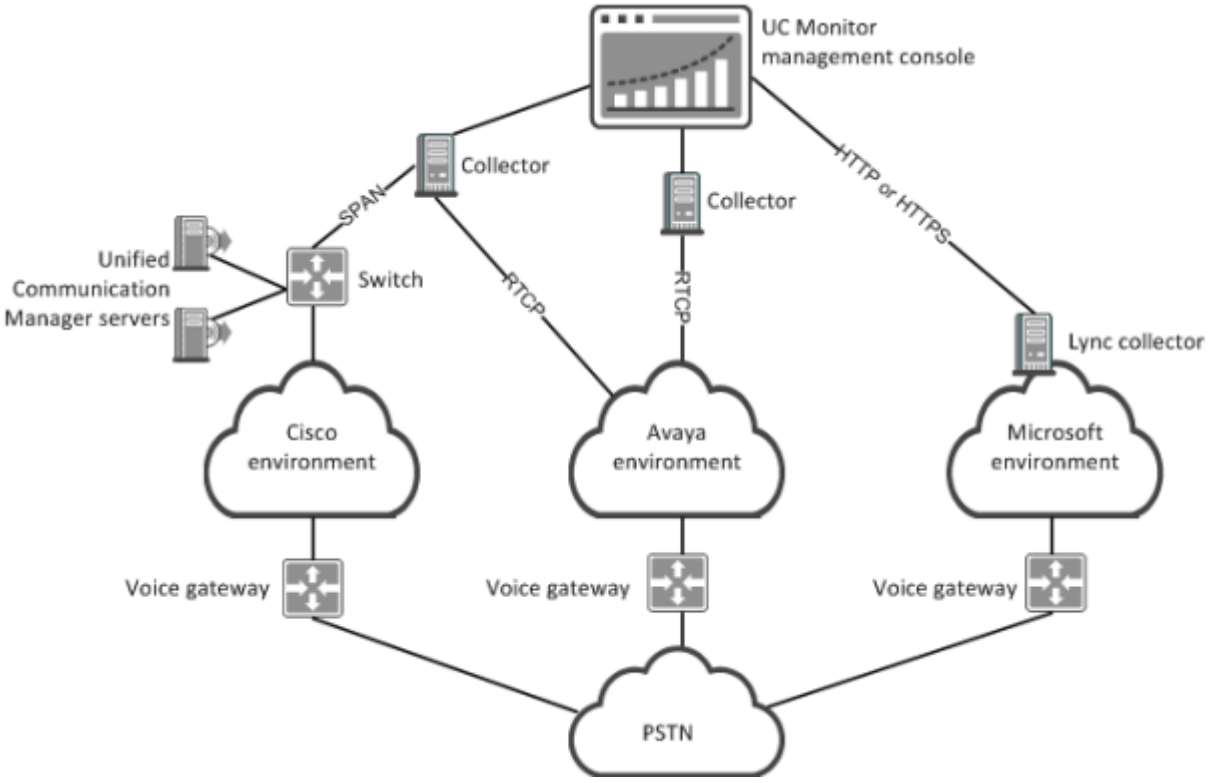
12.5 reports per second multiplied by 5300 bytes per report = 66250 bytes per second = 530 kbps

# Appendix D: Example of UC Monitor in a Multi-Vendor Environment

You can use a standalone system or a distributed system to monitor an environment that includes a combination of Cisco, Avaya, and Microsoft components. In the distributed architecture, UC Monitor components are deployed on at least three servers:

- At least one server for the collectors that gather or receive Cisco or Avaya data.
- One Microsoft front-end server to be designated as the Lync collector, which sends call quality data to the management console.
- One server for the management console.

The following diagram illustrates a Cisco-Avaya-Microsoft environment:



# Index


## A

Avaya environments
- architecture • 30
- bandwith requirements • 31
- configuring • 29

## B

browser support • 9

## C

Cisco environments
- architecture • 33
- configuring • 33
- scalability • 34

collectors
- configuring the servers • 16
- installing the software • 22

configuring medianet devices • 19
configuring network interface cards • 17
configuring the management console • 15

## F

firewall requirements • 12

## H

hardware requirements • 10, 11
host name, changing • 25

## M

management console
- configuring the server • 15
- installing the software • 22

medianet devices, configuring • 19
Microsoft Lync environments
- architecture • 36
- bandwidth • 36

## N

network interface cards, configuring • 17

## O

operating system support • 9

## P

post-installation tasks • 25

## S

software
- installing on one server • 23
- installing the collector • 22
- installing the management console • 22
- prerequisites • 21

system time, synchronizing • 26

## V

virtual system requirements • 12