CA Unified Communications Monitor

Administrator Guide

Version 3.4

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.

Documentation Changes

The UC Monitor Administrator Guide is undergoing a significant renovation, and, as a result, is drastically smaller than the Administrator Guide that shipped with version 3.3.

Rather than one large book, the Technical Information team is providing smaller role-based work flows (called use cases) that specifically address the topics you need to perform your job better. These use cases are available in the CA Unified Communications Monitor bookshelf on CA Support Online.

The following use cases replace information that was previously available in the Administrator Guide:

- Managing Collectors in Avaya and Cisco Environments
- Managing Collectors in Microsoft Lync Environments
- Creating Location Definitions
- Adding Call Servers to the Database
- Adding Voice Gateways and Other Media Devices to the Database
- Creating Call Server Groups
- Creating and Assigning Call Setup Thresholds
- Creating and Assigning Call Quality Thresholds
- Managing Codec Thresholds

Contents

Chapter 1: What is UC Monitor?

CA Unified Communications Monitor (UC Monitor) tracks the performance of VoIP systems and unified communications systems. UC Monitor employs passive monitoring to maintain a continuous record of the call setup traffic, call audio and video quality, and performance associated with the following endpoints:

- IP phones
- Audio and video clients
- Call servers
- Voice gateways
- Midstream devices

UC Monitor reports let you view and analyze collected data. You can configure automatic actions to gather more information for troubleshooting and diagnostics. You can set performance thresholds, with automatic alerts to let you know about declines in call quality, failed calls, or call server issues.

UC Monitor can help you with all of these challenges, and can also help you perform quick diagnostics and troubleshooting when issues inevitably arise. In most enterprises, application performance issues are commonly, but often incorrectly, blamed on the network. UC Monitor helps you determine the true source of VoIP performance degradation. You can avoid the costly, and often unnecessary, infrastructure upgrades that are often the default solution to performance issues.

UC Monitor helps you gauge how well your unified communications hardware and software deliver services to the end user.

- Proactively monitor VoIP and video call quality and call setup metrics.
- Know immediately when users cannot complete calls and when audio or video quality is low.
- Receive a notification when call quality fails to meet a threshold.
- Receive a notification when a call setup is slow.
- Gather call performance data from a targeted endpoint (see definition on page 60) for use in troubleshooting an issue.
- Gather data from unidirectional traffic flows from medianet-enabled devices, such as switches and routers.

- Access call performance data in formatted reports that are easy to understand and analyze for detailed metrics.
- Leverage a full suite of analytics and reporting by registering UC Monitor as a data source for CA Performance Center.

Chapter 2: Configuring the Management Console

Management console configuration includes basic administrative tasks such as changing the default administrator password, and creating schedules for sending UC Monitor reports to designated recipients.

This section contains the following topics:

Launch the Management Console

Take the following steps to launch the web-based management console.

Follow these steps:

1. Perform one of the following:
   - Navigate to the management console in a web browser window. Enter the IP address of the management console in the Address field. Use the following syntax:

     `http://<IPaddress>/UCMonitor/`
   - Click the UC Monitor icon on the desktop of the management console computer.

   The UC Monitor Login web page opens.
2. Type the default user name and password:
   - User name: admin
   - Password: admin

Important: For better security, change the password.

More information:

Change the Default Password and User Name (see page 10)

Change the Default Password and User Name

UC Monitor security features prevent unauthorized users from gaining access to your network data, SNMP community information, and sensitive records. But your system is only as secure as your own practices. To help secure your system, change the default user name and password associated with the administrator role.

Note: After you register UC Monitor as a data source for CA Performance Center, you cannot use the management console to change the password. Use CA Performance Center for this task.

Follow these steps:

1. Click Administration, Security, Users in the navigation bar.

   The User List opens.
2. Select the default administrator, admin.
3. Click Edit.

   The User Properties page opens.
4. Type a new password in the Password and Confirm Password fields.
5. Click Save.

Tip: You can use this procedure to change the passwords assigned to the user accounts you define for your UC Monitor system.

More information:

Managing UC Monitor Security (see page 15)
Users (see page 16)

Change the Properties of the Management Console

When you installed your UC Monitor system, you configured NIC cards and LAN connection settings for the management console. The management console detects these connections and displays their properties on the Console Settings page. Verify that the management console uses the correct connections for management and monitoring.

The availability of settings you can change depends on the following:

- Whether you have a standalone or distributed deployment
- Whether you are monitoring an Avaya, Cisco, or Microsoft environment

Follow these steps:

1. Click Administration, Console, Settings in the navigation bar.

   The Console Settings page opens.

2. Complete the following fields, and then click Save:

   - **Console Name**. The name of your management console, not the host name of the server.
   - **Phone Number Format/Mask**. The format to use when displaying directory numbers on report pages.

     Use the # symbol for the portions of the directory numbers you want to display in the management console. Use the letter X for the portions that you want to mask, or hide. For example, specify (###) ###-#XXX to see a directory that looks like the following in reports:

     (888)543-2XXX

   - **SIP URI Format/Mask**. The format to use when displaying the SIP URI on report pages. Select a format for the portions of the identifier, usually an email address, to display in the management console.

     The default is to show the entire URI. You can also select:

     - Show Name/Hide Domain. For example, jdoe@X
     - Hide Name/Show Domain. For example, X@ca.com
     - Hide All. For example, X@X

   - **SMTP Server Name**. The address of the SMTP server responsible for sending email messages on your network. UC Monitor uses this information to send email messages automatically in response to Incidents.

     If an SMTP server is not configured locally, UC Monitor does not send email messages.

   - **Reply Address**. The email address that appears as the From address in emails from the UC Monitor management console.

     The default address is UCMonitor@[*server hostname*]. As a best practice, replace "UCMonitor" in the default address with the name of the management console. You will be able to distinguish between email from multiple consoles.

     When a user sets up an email report schedule and defines an email address for the schedule, that email address overrides this Reply Address.

     Note: Some mail servers automatically disable all links in email from unknown addresses. We recommend changing the Reply Address to a real email address that is known to your email server. Otherwise, recipients receive a warning indicating that email may be phishing messages. The default Reply Address cannot be added to the Safe Senders list, which requires a .com suffix.

- **NIC**. Either 1 or 2. The priority of this adapter in the Adapters and Bindings Network Connections list. The management NIC must be listed first.

  Important: To monitor Avaya, do not change the default settings.

- **Management/Monitor**. The IP addresses of the management and monitor Network Interface Cards (NIC), which you assigned during installation.
  - The management address is for the NIC card that the management console uses to connect to the network. This NIC must have priority 1 in the Adapters and Bindings Network Connections list.
  - The monitor address applies to a NIC on the collector that is only used to monitor Cisco call traffic.
- **IP Address**. The IP address assigned to each adapter.

Manage Email Schedules

Operators with permission to view a report can email the report in PDF format to specified recipients. These operators can change or delete email schedules they created, and they can unsubscribe themselves from scheduled email messages.

UC Monitor operators cannot change report schedules created by other operators or by the administrator. That function requires administrator account permissions. Administrators can change and delete email schedules that they created or that were created by UC Monitor operators.

Use the OPTIONS menu to create an email schedule. Use the following procedure to change or delete email schedules.

Follow these steps:

1. Click Administration, Console, Scheduled Email in the navigation bar.

   The Scheduled Email List opens. Email schedules created by the UC Monitor user who is logged in are visible in the list. The administrator can see all schedules.

2. Take the following steps to change an email schedule:

   a. Select the schedule you want to change and click Edit.

      The Scheduled Email Properties page opens.

   b. Complete the following fields and then click Save.

   - **Send To**: Enter email addresses in the following format: <name>@<domain>.
   - **Reply To**: The email address of the user who configures the email schedule. This option is available only when the administrator has configured a “Reply To” address in the user properties.
   - **Subject**: A descriptive subject for the emailed report. Include the report title and Locations or components included in the report.

- **Message**: (*Optional*) A message to accompany the emailed report.
- **Time Zone**: Select the time zone of the intended recipient.
- **Send Now**: Select this option to send the email immediately.
- **Send on a Schedule**: Select this option to send the report on a regular basis. When selected, the following options appear:
  - **Send Daily**: Send the email once per day. If enabled, reveals check boxes where you can select the day of the week to send the report. By default, the report is mailed every weekday (Monday through Friday) at 0:30 hours in the time zone of the management console. The time frame of the daily report is the previous day.
  - **Send Weekly**: Send the email once per week. By default, the report is mailed every Sunday at 01:00 in the time zone of the management console. The time frame of the weekly report is the previous week (Sunday through Saturday).
  - **Send Monthly**: Send the email once per month. If enabled, reveals menus where you can select the day of the month to send the report. The monthly schedule sends the report on the first day of each month at 01:30 in the time zone of the management console. The time frame of the monthly report is the previous month. This option is available only for Capacity Planning reports.
- **Output Orientation**: Select whether the email displays the report in portrait format or landscape format.
- **Page Size**: Select a page size that accommodates the amount of data in the report. For example, for a report in the Landscape orientation, select the Legal paper size, which is wider than the Letter size.

3. Take the following steps to delete an email schedule:
   a. Select the schedule you want to delete and click Delete.
   b. Click Delete to confirm the deletion.

      The schedule is removed from the list. Reports are not emailed to the designated recipients.

Chapter 3: Managing UC Monitor Security

UC Monitor security integration with CA Performance Center is similar to that of other data sources. CA Performance Center provides centralized management of user accounts, permissions, SNMP profiles, and groups among all CA data sources. Centralized user account and group management tasks make it easy to share user access permissions for different CA Performance Center data sources among IT teams.

To take advantage of the centralized management feature, register UC Monitor as a data source for CA Performance Center. Registration lets CA Performance Center assume certain management tasks for UC Monitor and makes those tasks accessible to users with the appropriate administrative product privileges.

- *Before UC Monitor is registered as a data source*, the administrator uses the UC Monitor management console to view, add, edit, and delete user accounts, roles, and SNMP profiles.
- *After UC Monitor is registered as a data source*, the administrator is redirected to CA Performance Center for all administrative tasks associated with users, roles, permissions, and groups. All users and roles defined in the system, including users and roles from other CA Performance Center data sources, are displayed on the UC Monitor Administration pages. However, you manage users and roles from the CA Performance Center console.

This section contains the following topics:

Register UC Monitor as a Data Source

To centralize the management of groups, users, and roles, and to view UC Monitor data in CA Performance Center, register UC Monitor as a data source for CA Performance Center. The process of registering the data source automatically integrates user and role management.

You can register up to four UC Monitor data sources with one CA Performance Center instance. The UC Monitor data views in CA Performance Center represent aggregated data from all UC Monitor data sources.

You use the CA Performance Center console to register data sources.

Follow these steps:

1. Log in to CA Performance Center as a Default Tenant (global) Administrator.
2. Click Admin, Data Source Settings, Data Sources on the navigation bar.

   The Manage Data Sources page displays the current list of registered data sources.
3. Click New.

   The Data Source Administration dialog opens.
4. Select Unified Communications Monitor from the Source Type list.
5. Enter the Host Name of the UC Monitor server on which the database is installed.

   The hostname is the IP address or DNS hostname of the server. For data sources in a distributed configuration, supply the hostname of the management console.
6. Select the Protocol and Port for the CA Performance Center web service to use to contact the corresponding UC Monitor Web Service. By default, HTTP over port 80 is used. Use HTTPS and port 443 if your network is using SSL for communications.
7. (*Optional*) Provide a Display Name that identifies the data source. If you are registering multiple UC Monitor data sources, you can change the default data source names to help identify them in CA Performance Center.
8. Confirm whether the Web Console address is the same as the Host Name. If it is not, take the following steps:
   a. Clear the Same as Data Source check box.
   b. Complete the Host Name, Protocol, and Port fields with the information you provided in steps 5 and 6.
9. Click Save to save the registration.
10. Click Save & Add Another to register another data source.

    CA Performance Center lists the data sources you registered in the Data Source List.

Users

The administrator creates user accounts for the operators who access UC Monitor reports and functions, and assigns them roles and product privileges. The main access levels that you can change involve role-based permissions to view reports and initiate a Call Watch or traceroute investigation.

UC Monitor provides two predefined users with different roles and product privileges. Before you register UC Monitor with CA Performance Center, the User List displays only the predefined users. After registration, the User List displays the predefined users and users for other data sources that are registered with CA Performance Center.

The User List provides the following information.

User Name

A name to identify this user account. The user account defines the credentials of a person who is authorized to operate UC Monitor and to perform certain tasks. Each user definition contains a user name and an associated email address, role, and product permission level.

Two user names are predefined:

- admin (the administrator)
- user (the default product user)

If you assign users to the predefined user accounts, change the default passwords.

Note: Previous versions of UC Monitor had different predefined user names: nqadmin and nquser. If you upgraded from a previous version, your User List still contains the old user names.

Role

The role assigned to the user: IT Manager, IT Operator, or a custom role.

Privilege

A defined level of access to product functionality and configuration: Administrator or User.

- Administrator: Performs all functions, including all administrative tasks: creating and editing Locations, media devices, thresholds, Call Watch definitions, incident responses, roles, and user accounts.
- User: Views the pages and performs basic functions selected by an administrator. User permission does not provide access to administrative functions.

Description

A description of the user account, such as the user's full name and office location.

Status

The status of the user: Enabled, Disabled, or Built-In (for the predefined user accounts).

More information:

Change the Default Password and User Name (see page 10)

Manage User Accounts

Before you register UC Monitor as a data source for CA Performance Center, use the management console to create, change, and delete user accounts. Verify that user accounts are not shared. Results are unpredictable when more than one user is logged in with the same user account. Page and view settings can interfere with each other when accessed simultaneously on different computers.

Important: After you register UC Monitor with CA Performance Center, use CA Performance Center to manage users, product permissions, and roles.

Follow these steps:

1. Click Administration, Security, Users in the navigation bar.

   The User List opens.

2. Perform the following to create or change a user account:

   a. Click New to create a user account, or select the user you want to change and click Edit.

      The User Properties dialog opens.

   b. Complete the following fields:

      - **Name**: A name to identify this user account.
      - **Description**: (*Optional*) A description of the user account, such as the user's full name and office location.
      - **Email Address**: The email address of the user. Used as the "Reply to" address in emails that the user schedules.
      - **Password**: A password for the user account. A password is not required, but is recommended for security purposes. Blank passwords are accepted.
      - **Confirm Password**: Retype the password you entered in the Password field.
      - **Time Zone**: The time zone where the user works and views reports, relative to Greenwich Mean Time (GMT). The default time zone is UTC (coordinated universal time), which is the same as GMT. For more information, see How to Select a Time Zone (see page 19).
      - **Role**: The role assigned to the user: IT Manager, IT Operator, or a custom role. For more information, see Roles (see page 20).
      - **Product Privilege**: A defined level of access to product functionality and configuration: Administrator or User. For more information, see Users (see page 16).
      - **Enabled**: Indicates that the user account is active, and ready to be used to access the features specified by the role and permission level.

c. Click Save to save the user account. The User List displays the new user account or your changes.

d. Click Save & Add Another to save the user account and create another user.

3. Select a user and click Delete to delete a user account. You cannot delete the predefined user accounts, admin and user.

   a. Click Delete. The Confirm Delete page opens.

   b. Click Delete. The user account is deleted from the User List.

How to Select a Time Zone

The administrator can select a time zone so that a user can view report data with time values that correspond to the user's physical location.

Most time zone options are arranged into geographically related groups, such as Africa, America, Asia, Atlantic, Europe, and Pacific. Multiple options for "America" are available, including America/Cancun, America/Jamaica, America/New_York. All options let you assign a time zone based on the user's proximity to a well-known city or country.

A group labeled Etc/ contains time zones that are not geographical in nature, but that instead indicate a position relative to the "zero hour." For example, the group includes Etc/UTC, Etc/GMT, Etc/GMT-1, Etc/GMT+1, and so on. Use these options in the following situations:

- when you do not know which city or country the user is closest to
- when your enterprise uses standard (POSIX) time zones

The Etc/ options adhere to the POSIX standard, which uses positive values west of Greenwich, England. Many users expect to see positive time values east of Greenwich. For example, the Etc/GMT+4 option corresponds to four hours behind UTC (west of Greenwich) rather than four hours ahead of UTC (east of Greenwich).

Various well-known and common time zone designations are available, such as the following:

- EST5EDT: Eastern Standard Time/Eastern Daylight Time, or five hours behind GMT
- MST7MDT: Mountain Standard Time/Mountain Daylight Time, or seven hours behind GMT
- CET: Central European Time

Roles

Roles define the permissions allocated to a user, as a means of protecting sensitive information. For example, you can use roles to limit the number of UC Monitor operators who can view the Calls report, which can identify the endpoints that made calls, which numbers were called, and when calls were made. Create custom roles to suit your enterprise needs.

UC Monitor provides two predefined roles that you can use or modify. Before you register UC Monitor with CA Performance Center, the Role List displays only the predefined roles. After registration, the Role List displays the predefined roles and roles created for other data sources that are registered with CA Performance Center.

The Role List provides the following information for each defined role.

Role Name

A custom role or one of the following predefined roles:

- **IT Manager**: Role assigned to the user with permission to install and configure the UC Monitor system. Has permission to view all reports and set up and launch a Call Watch and a traceroute investigation. The role is assigned to one user, such as a VoIP System Administrator. However, a backup user can be assigned for emergency situations to avoid configuration errors and duplication of effort.
- **IT Operator**: Role assigned to a user with permission to view Performance reports, incidents, and Call Watch reports. Cannot set up or launch a Call Watch or change UC Monitor configuration.

Note: Previous versions of UC Monitor had different predefined roles: Network Operator and Network Manager. If you upgraded from a previous version, your Role List still contains the old role names. The old roles may have fewer permissions in CA Performance Center.

Description

A description of the role, such as a list of duties that are associated with the role.

Status

The status of the role: Enabled or Disabled.

Users

The number of user accounts to which the role is assigned.

Manage Roles

You can create roles to customize the product areas that a UC Monitor operator can view. For example, you can modify a role to assign permission for different areas of access. Before you register UC Monitor as a data source for CA Performance Center, you can create, change, and delete roles from the UC Monitor management console.

Important: After you register UC Monitor with CA Performance Center, use CA Performance Center to manage users, product permissions, and roles.

Follow these steps:

1. Click Administration, Security, Roles in the navigation bar.

   The Role List opens.

2. Perform the following to create or change a role:

   a. Click New to create a role, or select the role you want to change and click Edit.

      The Role Properties page opens.

   b. Complete the following fields:

      - **Name**: A name for the role.
      - **Description**: (*Optional*) A description of the role, such as a list of duties that are associated with the role.
      - **Enable Role**: Indicates that this role is enabled and ready to be assigned to a user account.
      - **Area Access**: Product features to which users with this role have access. Select one or more areas.

        The areas listed correspond to reports that can be viewed and product functionality that can be accessed. For example, the Call Watch option allows a user to view the Call Watch Real-Time report. The Call Watch Setup option enables a user to configure and launch a Call Watch.

        Note: When you upgrade from a previous version of UC Monitor, new options and areas often become available. These options are not enabled for roles that you created with a previous version of the product. You can, however, manually enable the options for these custom roles.

   c. Click Save to save the role definition. The Role List displays the new role or your changes.

   d. Click Save & Add Another to save the role definition and create another role.

3. Perform the following to delete a role. You cannot delete a role that is assigned to a user account.
   a. Review the Users column to verify that the role is not assigned to a user. If it is, assign a different role to that user before deleting the role. For more information, see Manage User Accounts (see page 18).
   b. Select the role you want to delete.
   c. Click Delete. The Confirm Delete page opens.
   d. Click Delete. The role is deleted from the Role List.
4. (*Optional*) Assign an enabled role to a user account. For more information, see Manage User Accounts (see page 18).

SNMP Profiles

UC Monitor uses SNMP to query the MIBs of Cisco voice gateways and Avaya call servers for performance information. SNMP profiles are definitions that contain the information necessary to enable secure queries of device MIBs using SNMP. These definitions provide SNMP parameters to UC Monitor while ensuring data security.

When you register UC Monitor with CA Performance Center, any profiles that were created in the data source are added to CA Performance Center. The reverse also occurs: Profiles already established in CA Performance Center are shared among all registered data sources. Naming conflicts are resolved, and changes to a profile are propagated to all registered data sources during synchronization.

Note: After you register UC Monitor with CA Performance Center, you can use CA Performance Center to manage SNMP profiles for all data sources.

The SNMP Profile List provides the following information for every SNMP profile you create.

SNMP Profile

The name assigned to this profile.

SNMP Version

The version of SNMP associated with this profile. One of the following:

- SNMPv1/SNMPv2C
- SNMPv3

Authentication

The authentication protocol used to contact devices associated with this profile. One of the following:

- None (do not attempt authentication)
- MD5 (Message-Digest Algorithm 5)
- SHA (Secure Hash Algorithm)

Privacy

The encryption protocol used for data flows sent to devices associated with this profile. One of the following:

- None (do not encrypt communications). This option is assigned when no authentication is enabled for the profile.
- AES (128-bit encryption)
- DES (Data Encryption Standard)
- Triple DES

Use as Default

Indicates whether the collector uses this profile first to attempt SNMP polling in the following situations:

- When it discovers a new Avaya Communication Manager or voice gateway
- For any device that supports SNMP polling by the collector but does not have an associated SNMP profile

Manage SNMP Profiles

SNMP profiles supply information that the collector needs when it uses SNMP queries to contact Cisco voice gateways or Avaya Communication Manager call servers. Create an SNMP profile for each SNMP community or each SNMPv3 secure device MIB. UC Monitor provides one default profile (public) for SNMPv1 and SNMPv2C.

You can create, change, and delete SNMP profiles from the UC Monitor management console.

Note: Do not create SNMP profiles for monitoring a Microsoft-only environment.

Follow these steps:

1. Click Administration, Security, SNMP Profiles in the navigation bar.

   The SNMP Profile List opens.

2. Perform the following to create or change an SNMP profile:

   a. Click New to create a profile, or select the profile you want to change and click Edit.

      The SNMP Profile Properties page opens.

   b. Complete the following fields. Different fields are available for each supported version of SNMP.

      - **Profile Name**: Type a name to identify this SNMP profile. Profile names must be unique, cannot be duplicated across SNMP versions, and are not case-sensitive.
      - **SNMP Version**: Select the version of SNMP to use: SNMPv1, SNMPv2C, or SNMPv3. This field is available only for creating a profile.
      - **Port**: Identify the port to use to make SNMP connections to devices associated with this profile. The default should typically be used: Port 161.
      - **Use as Default**: Select this check box to enable the collector to use this profile first when it discovers a new Avaya Communication Manager or voice gateway, or to contact devices that support SNMP polling but do not have an associated SNMP profile.

        A default profile is required. The only way to remove the default designation from one SNMP profile is to designate another profile as the default. Only one profile can have the default designation at a time.
      - **Community Name**: (*SNMPv1/SNMP/v2*) Type the secure SNMP community string that lets the collector query the MIB of this gateway device. The community name must provide read-only access to the device MIB. In the default SNMP profile, the community name is public. Type the community string again in the Verify Community Name field.
      - **User Name**: (*SNMPv3*) Type the user name that enables secure access to the media devices or servers associated with this profile.
      - **Context Name**: (*SNMPv3*, *Optional*) Type the name for the context of the SNMP session. The SNMP agent on the associated device uses the context to control which MIBs or MIB content (rows) are exposed for the SNMP session.
      - **Authentication Protocol**: (*SNMPv3*) Select the authentication protocol to use to contact devices associated with this profile.
      - **Authentication Password**: (*SNMPv3*) Provide the password to use for authentication using SNMPv3 and the selected authentication protocol. Type the password again in the Verify Authentication Password field.

- **Privacy Password**: (*SNMPv3*) Type the password to use when exchanging encryption keys. Type the password again in the Verify Privacy Password field.

c. Click OK. The profile appears on the SNMP Profile List.

3. Perform the following to delete a profile.

   a. Verify that the profile is not assigned to a voice gateway. If it is, reassign the device to a different profile.

   b. Verify that the profile is not designated as Use as Default. If it is, designate a different profile as the default.

   c. Select the profile you want to delete and then click Delete.

   d. Click OK to confirm the delete. The profile is removed from the SNMP Profile List.

4. Reload the collector to synchronize with settings on the management console.

5. (*Cisco only*) Assign a new profile to the associated voice gateway.

   Note: Do not assign a profile to Avaya call servers. The collector tries each profile in turn, beginning with the default profile, until it contacts the Communication Manager.

Chapter 4: Incidents and Incident Responses

UC Monitor uses *incidents* to report degraded conditions in VoIP call performance.

UC Monitor performance thresholds represent boundaries of acceptable VoIP performance. Performance thresholds trigger incidents. Incidents are records of information that is created when a performance threshold is crossed. Incidents are assigned sequential case numbers and reported on the Incident Report page. Each type of incident uses its own sequence.

Incident responses are associated with specific performance thresholds. You can set up automatic a*ctions f*or each incident response.

- Call Quality incidents can trigger email and SNMP trap actions.
- Call Performance incidents can trigger email, SNMP trap, and traceroute actions.
- Call Setup incidents can trigger email, SNMP, and traceroute actions.
- Call Server incidents can trigger email and SNMP trap actions.
- Call Server Group incidents can trigger email, SNMP, and traceroute actions.
- Collector incidents can trigger traceroute actions.
- Poor Call Quality incidents automatically trigger Call Watch investigations.

By default, performance thresholds do not trigger actions. When you customize thresholds, you can associate actions to incident responses. The response actions include network-specific parameters, such as email addresses that receive automatic notifications. An administrator can specify one of the following responses for an incident:

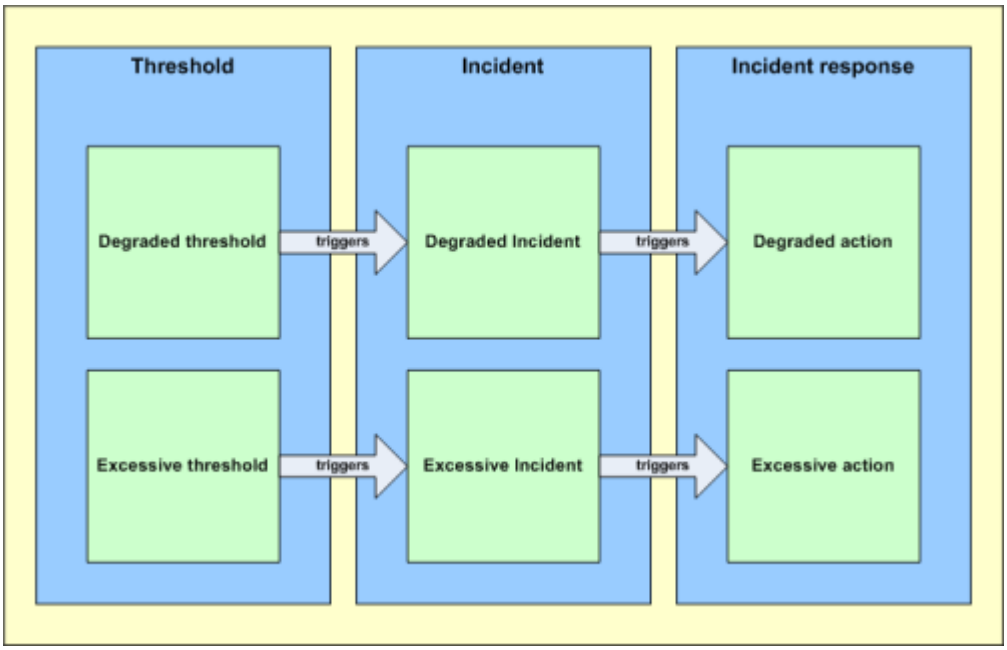
- An action that occurs when performance exceeds the degraded threshold
- An action that occurs when performance exceeds the excessive threshold

Important: Understand the difference between expected performance and unusual, or truly degraded, performance. Otherwise, incidents for an actual network anomaly can be lost amid a long series of incidents that are raised continually for normal performance conditions.

This section contains the following topics:

How Incidents Trigger Responses

UC Monitor creates an incident when it detects a condition on the network that exceeds a threshold. If an action is associated with the threshold condition, UC Monitor launches that action automatically, as shown in the following diagram:



Keep in mind the following details about incidents, incident responses, and actions:

- UC Monitor creates an incident the first time a threshold is crossed.
- UC Monitor creates another incident for the same violation only after the first incident is closed.
- To trigger an incident, a violation must exceed minimum severity and duration criteria.
- A UC Monitor administrator can associate an incident response with the incident type.
- For a few incidents, such as the Abnormal Termination incident, no applicable metrics are monitored for improvement so that the incident can be closed. Therefore, the incident is briefly opened to trigger automatic actions and is then immediately closed. The accompanying email or SNMP trap notification indicates that the incident is open, but in fact closure is pending.

- The traceroute investigation action is configured as an incident response action for call setup or call server group incidents only.

  The results of a traceroute investigation for other types of incidents, such as call quality, are not helpful. Traceroutes begin at the collector, which is located so closely to the call server that little is determined from the route for call traffic.

  For call server group incidents, the collector attempts to run a traceroute to the key phone at the affected Location.

A traceroute investigation can also be launched independently of an incident.

How Incidents are Closed

An incident remains open until it is automatically closed. For example, the severity of the condition changes, but the metrics still violate the degraded or excessive threshold. The incident is updated to reflect the change in severity, but the incident is not closed.

Incidents are closed when:

- They are open for 24 hours. If the problem still occurs after 24 hours, a new incident is opened.
- The performance condition that violated the threshold has not been detected for one full clock hour of data collection. A full clock hour is not the same as 60 minutes of time. A full clock hour starts at the beginning of an hour and ends at the beginning of the next hour.

Incident types can change. A call quality threshold violation overrides a call setup violation when they affect the same pair of reporting components. An incident remains open for that pair, but the type of incident changes to call quality when a call quality threshold violation is detected.

Note: You can acknowledge an incident for a degraded performance condition and not be aware that the performance condition has deteriorated further. A degraded incident can change to severe status while still appearing as acknowledged in incident reports. As a best practice, acknowledge only those incidents that you have taken steps to address.

How Thresholds and Incidents Work Together

The following is a fictitious example of how performance thresholds, incidents, and incident responses work together:

1. A call server cluster at the Austin, TX, network location becomes unavailable due to a LAN connectivity issue.
2. Several users dial out with their IP telephones and are routed to a backup call server cluster in Phoenix.

3. The delay-to-dial tone call setup excessive threshold of 2000 milliseconds is exceeded.
4. UC Monitor creates one call setup incident for all affected telephones at the Austin Location.

   The call setup incident launches two associated incident response actions:

   - Sending an email to notify a network engineer at the Austin location that a call setup threshold was exceeded.
   - Automatically launching a traceroute investigation to the key phone at the Austin Location.
5. The network engineer at the Austin site clicks a link in an email message. The link opens a page of incident reports, where the engineer can quickly drill down to find the affected call server cluster.
6. From the incident report, the engineer can easily access the Investigation Details page. This page allows easy comparison of the baseline route to the current route to find the connectivity issue.

When an incident or Investigations report does not include sufficient information to resolve the problem, the engineer can launch a Call Watch for more information.

How to Respond to an Incident

Incidents and incident responses are useful for troubleshooting in the following ways:

- Incidents maintain a record of conditions at the time a problem occurs.
- Incident responses automatically gather information that helps you troubleshoot a problem, reducing the mean-time-to-repair (MTTR).

An email about an incident contains a notification that a threshold was crossed. The message also contains a link to the incident report, where you can drill down into detailed information.

Status updates are available for SNMP trap notifications. A UC Monitor administrator can configure them as incident response actions. They also include a notification that performance for a certain component has returned to normal after a recent threshold condition that was also reported. For each incident reported in an incident response email message, one or more links to associated UC Monitor reports are included.

When you receive an email notification or SNMP trap in response to an incident, perform one or more of the following actions to troubleshoot the poor performance.

- Click links provided in the notification to view the relevant incident report.
- Drill down for more information about the incident, such as the status of call servers.

- Click the Related Reports link to an associated investigation report. Review the Traceroute Investigations report to see whether the path of the call setup traffic resembles the one shown in the Baseline Traceroute Details.
- Launch a manual traceroute investigation for more information about the route between the affected endpoint and its call server or voice gateway.
- Initiate a Call Watch for the affected endpoints.
- Acknowledge the incident to reduce its priority and to let other operators know that the issue is addressed.

Acknowledge Incidents

Acknowledging an incident reduces its priority in reports and indicates to others that the incident was reviewed. If necessary, you can unacknowledge an acknowledged incident, to raise its priority in reports.

Follow these steps:

1. Click Monitoring, Incidents in the navigation bar.

   The Incidents Overview page opens.

2. Select the check box of the incident you want to acknowledge in the Acknowledged column.

3. Click Apply.

   The Severity status indicator identifies the acknowledged incident.

Note: You can acknowledge an incident for a degraded performance condition and not be aware that the performance condition has deteriorated further. A degraded incident can change to severe status while still appearing as acknowledged in incident reports. As a best practice, acknowledge only those incidents that you have taken steps to address.

View Incident Details

When call setup or call quality performance metrics exceed a threshold, UC Monitor displays a list of incidents on the Incidents Overview. Click the link for an incident to view the full incident report.

Incident reports show details of the related performance degradation. They have a maximum time frame of 24 hours. You can view incidents that were active during the time frame of interest.

Follow these steps:

1. Access the Incidents Overview in one of the following ways:
   - Click a link in the incident notification.
   - Click Monitoring, Incidents in the navigation bar.

   The Incidents Overview opens.
2. In the ID column, click the number for the incident whose details you want to view.

   The Incident Details page opens, and displays information that is already narrowed to show the affected Locations and a media device or call server. An alarm icon indicates when the incident was reported.

Manage Incident Responses

UC Monitor provides one default incident response, Default, which is not associated with an action. You can configure different responses for each Location, for each media device, for each call server or call server group, or for pairs of Locations and media devices. You apply the responses to call performance or call server incidents by associating the responses with different thresholds for the various types of incidents.

You can add an action to the default incident response and to incident responses you created. You can associate an incident response with more than one action.

You can modify an incident response in the following ways:

- Add an action.
- Change or delete an action.
- Change the threshold parameters that control when the response is launched.

You can create, modify, and delete incident responses in the UC Monitor management console.

Follow these steps:

1. Click Administration, Policies, Incident Responses in the navigation bar.

   The Incident Response List opens.

2. Perform the following steps to create or change an incident response:

   a. Click New to create an incident response, or select the response that you want to change and click Edit.

      The Incident Response Properties page opens.

   b. Type a name for the incident response in the Name field. The name helps you identify the response in the list of responses on the Threshold Properties page.

   c. Click New to add an action, or select the action that you want to change and click Edit.

      The Add or Edit Action to Incident Response page opens.

   d. Select the Action Type, which determines the other selections on this page:

      - **Send Email**. Lets you supply the email address of the person to notify when the associated threshold is violated. You can specify multiple email addresses, separated by commas or semicolons.
      - **Send SNMP Trap**. Lets you supply parameters for an SNMP trap to send to a third-party network monitoring operating environment.
      - **Launch Traceroute Investigation**. Lets you run an automatic traceroute to collect extra data about routing from the affected Location or voice gateway. The Launch Traceroute Investigation action is designed for call setup and call server group incidents only.

e. Set the Minimum Conditions for Taking Action:

- **Severity**. Select the threshold severity level that can trigger this action when crossed: degraded or excessive. Severity does not apply to the automatic actions initiated in response to collector incidents, call server incidents, or call server group incidents. These actions are always performed. Incidents of these types always have a severity of "excessive."
- **Duration**. Select the interval during which a monitored metric must violate the threshold before the action is launched. Use this option to launch actions either more or less quickly in response to threshold violations.

  For example, select 30 minutes to launch an action when latency exceeds the threshold during a 30-minute interval. It does not matter how many times during the interval that the threshold is crossed. It matters only that the condition still exists at the end of the selected duration.

f. Set the parameters that control the recipient and format of the notification. The available parameters vary depending on the selected Action Type:

- **Recipients**. Provide the full email address of the person to receive an automatic email notification about this particular type of incident. Select someone who is most likely to respond quickly and accurately to remedy the problem that caused the incident. You can specify multiple email addresses, separated by commas or semicolons.
- **Time Zone**. Select the time zone of the recipient. The default time zone corresponds to the locale where the UC Monitor management console is installed.
- **Send SNMP Trap to**. The IP address or hostname of the computer to receive the SNMP trap. UC Monitor includes a MIB file that contains unique OIDs. You can import them into your trap receiver. The file is located in the following directory on the management console:

  `<install path>\CA\VoIPMonitor\MIB\NETQOS-VMTRAP-MIB.txt`

  Tip: To send a trap to more than one computer, create additional actions within the same response, one for each additional trap destination.
- **SNMP Profile**. Select the SNMP profile to use for the trap.
- **Severity Updates.** Select when to send SNMP traps:
  -- **Send update traps when Incident severity changes**: Send an SNMP trap if the incident severity changes, but the incident remains open. Also send an SNMP trap when a new incident is opened.
  -- **Send only Incident open and close traps**: Send an SNMP trap only if a new incident is opened or if an incident is closed.

  Note: Some incident types do not have a severity parameter, such as the Poor Call Quality incident, or their severity is always excessive. The option to send only open and close traps is always used for these incidents.

- **Send Test Trap**. Click to send a trap to the IP address you entered in the "Send SNMP Trap to" field. Results of the test appear at the top of the Add Action to Incident Response page.

g. Click OK.

The action appears on the Incident Response Properties page.

h. Select an action and click Delete to remove an action from a response.

i. Click Save to save the response and return to the Incident Response List.

j. Click Save & Add Another to save the response and add another action to the incident.

3. Perform the following steps to delete an incident response. You cannot delete a response that is used in a threshold.

a. Verify that the incident response is not assigned to a threshold. If it is, assign a different incident response. For more information, see Manage Call Server Thresholds.

b. Select the incident response that you want to delete. You can select multiple responses.

c. Click Delete. The Confirm Delete page opens.

d. Click Delete. The response is deleted from the Incident Response List.

4. Assign the incident response to a threshold.

More information:

Change the Properties of the Management Console (see page 10)
SNMP Profiles (see page 22)

Chapter 5: Managing the UC Monitor Database

UC Monitor uses a MySQL database for data storage. The database resides on the same computer as the management console.

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 nightly and weekly scheduled database maintenance.
- When the CA UCM Inspector service starts on the management console.

This section contains the following topics:

What Types of Data are Stored?

The UC Monitor database stores several different types of data, each with its own tables, row counts, and storage periods. UC Monitor stores data in the following directories:

<install path>\CA\MySql51\data\voip
<install path>\CA\MySql51\data\netqosvoipconsole

Interval data

Data that is collected during regular monitoring at five-minute intervals or 15-minute intervals by the collector. Incident data is included in this category.

Summary data

Data that the management console generates periodically. Used for certain long-range reports, such as the Capacity Planning reports.

Call data

Data about individual calls, such as call legs and sessions.

Abandoned call data

Data from calls that were abandoned before they were completed.

Call Watch data

Data from watched phones during a Call Watch.

Midstream device data

Medianet flow metrics and device information, such as stream legs and interface names.

View Database Status

A full, or nearly full, hard drive affects the reporting performance of existing data and the collection of new data. The Database Status page provides information about the rows of data in the database. Row totals are itemized by data category. The number of new rows over the past day and the past seven days is provided to help you calculate database growth.

Disk Space

Identifies the hard drive where UC Monitor is installed and how much disk space is free on that computer. We recommend having at least 6 GB of free hard disk space on the drive where the management console is installed. By default, a warning is sent when free hard disk space falls below 5 GB.

Table Growth

The rate at which the database is growing. Sorted by data type:

- Interval data
- Summary data
- Call data
- Abandoned call data
- Call Watch data
- Midstream device data

Rows in database

The number of rows in the database. For Call Watch data, includes all watched calls that the collector has seen, whether they are in progress or not.

Rows for past day

The number of rows of data that were collected over the past 24 hours. For Call Watch data, calls still in progress are not included. An end time is required. To have a known end time:

- The call is completed.
- The collector detected the call completion and reported it to the management console.
- The management console processed the results.

Because delays can occur during reporting, the number of rows for the past day and the past seven days may be undercounted.

Rows for past 7 days

The number of rows of data collected in the past seven days. For Call Watch data, does not include calls that are in progress. An end time is required. The same rules apply as to "Rows for past day."

Total duration

The difference between the oldest and newest row in the relevant database table.

Recommended Database Limits

The amount of data that can be stored in the UC Monitor database depends on the volume of call activity on your network. We recommend the following limits on data storage to avoid performance degradation. The UC Monitor database can accommodate a maximum of 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
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

Call Volume	10 million calls per month	6.6 million calls per month	3.3 million calls per month
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, UC Monitor stores data from abandoned calls 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- 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 related to abandoned calls. The default is three months.
- **Save call watch (Defined) data for**. The length of time to store Call Watch data from your Call Watch definitions. The default is eight months. Store Call Watch data for a smaller length of time, or for the same length of time, as 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 Call Watch data from automatically watched calls. Calls from Avaya endpoints (see definition on page 60) are automatically watched. The default is one week. Store Call Watch data for the same length of time, or less, as 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. System maintenance includes database backup and restore operations. 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**. Select this check box to send an email message when the available disk space falls below the specified threshold. Type the email address of the recipient.
- **Send SNMP traps to**. Select this check box to send an SNMP trap when the available disk space falls below the specified threshold. Type 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 daily and weekly maintenance. Set the maintenance schedule on the Administration, Console, Database, Maintenance page. 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**. Purges all five- or 15-minute data from regular monitoring, including all incident data.
   - **Collected summary data**. Purges all summary data that the management console generated for long-range reporting.
   - **Collected call watch data**. Purges all data from watched phones.
   - **Collected call and call watch data**. Purges 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**. Purges all data from medianet-enabled devices.
   - **Abandoned calls**. Purges all data from abandoned calls.
   - **Purge all selected data**. Purges selected data across all dates.
   - **Purge prior to this date/time**. Purges 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.

Manually Back Up and Restore the Database

UC Monitor automatically performs weekly database maintenance, which includes database backup and restore operations.

You can manually back up and restore the database for debugging purposes, before upgrading the UC Monitor software, or when directed to do so by a CA Technical Support representative.

Follow these steps:

1. Navigate to Administrative Tools, Services in the Control Panel.

   The Services window opens.

2. Stop the following services:

   - CA UCM MySql51
   - CA UCM Console Communicator
   - CA UCM Inspector

   Note: Do not stop the CA UCM Collector service.

3. Copy the <*install path*>\CA\MySql51\data directory to a backup location to back up the database.
4. Replace the <*install path*>\CA\MySql51\data directory with the most recent backup version to restore the database.
5. Restart the services that you stopped.

Hard Drive Maintenance

UC Monitor contains several tables that it consistently accesses for read/write (I/O) operations. These tables occupy most of the disk space on the drive where the management console is installed. The I/O operations cause disk fragmentation over time.

We recommend that you perform the following tasks to maintain the hard disk drive (HDD).

Regular defragmentation

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.

Regular backups

CA Performance Center data sources constantly write to the HDD. During data-seek operations in support of report compilation, the drive heads move about, simultaneously writing and reading. As with any HDD, this stress over time can lead to failure. To recover quickly with minimal data loss, schedule a regular database backup.

More information:

Change Database Settings (see page 40)

Appendix A: Working with Groups, IP Domains, and Tenants in CA Performance Center

Consider the usefulness of organizing your Locations and devices into IP domains, groups, or tenants. These organization tools serve several purposes:

- Organize managed items in a way that facilitates reporting.
- Control the managed items and associated data that each UC Monitor operator can view.
- Enable the monitoring of multiple enterprises with overlapping IP addresses as separate entities.

IP domains and groups are supported in CA NetQoS Performance Center version 6.1 and CA Performance Center. Tenants are supported in CA Performance Center. UC Monitor must be a registered data source to enable these features.

Only a user with the administrator role in CA Performance Center or CA NetQoS Performance Center can create and edit IP domains, groups, and tenants.

This section contains the following topics:

What are IP Domains?

CA Performance Center supports monitoring by IP domain. *IP domains* are logical groupings that identify data collected from different devices and networks. Monitoring by domain means that IP addresses with associated interfaces or applications that belong to separate customer networks are monitored separately. When combined with appropriate permissions, IP domains are monitored from a single console, but users view data only for the domains that they monitor.

IP domains function much like groups to contain managed items. Like groups, they are created in CA Performance Center, but the task of assigning items to domains is performed in the UC Monitor data source.

IP domains are optional in a standard CA Performance Center installation. However, IP domains are required when you want to deploy CA Performance Center in a multi-tenant environment.

Note: For complete information about managing domains, see the *CA Performance Center Administrator Guide*.

How IP Domains Work

IP domains let you address potential IP address conflicts. Domain identifiers indicate that two managed items that otherwise appear as duplicate IP addresses are actually two *different* managed items. For example, a router with a single IP address could have multiple interfaces, each belonging to a different enterprise. The DNS identity of each interface would determine its IP domain. Data from items in the domain would be reported for a single tenant corresponding to the interface owner.

The domain dimension lets CA data sources function in a service-provider environment. The same software monitors multiple networks as separate entities. The domain lets data collectors associate managed items and data with the appropriate service provider customer, or *tenant*.

Domain monitoring is enabled for each data source as soon as it is registered. However, domain identifiers are not visible in the data sources until at least one custom IP domain definition has been created in CA Performance Center. The following managed item types are associated with the Default Domain once domain monitoring is enabled:

- Devices
- Interfaces and interface addresses
- Networks
- VoIP Locations

The data sources that monitor these item types report up a domain identifier and other properties during synchronization with CA Performance Center. A data source can associate an item with a domain by including a domain ID property. Any item whose domain ID is not reported is automatically placed in the Default Domain.

CA Performance Center users with the Administrator role can create custom IP domains. They are sent down to the data sources during synchronization, where they are available for use during data collection configuration. Domain definitions are shared among data sources that are registered to the same CA Performance Center instance.

In the Groups tree, the Domains group is contained within the Inventory group, which is itself a subgroup of the Tenant. The Domains group includes the Default Domain and any custom domains that you have created.

Items that are not assigned to a custom domain in a data source are associated with the Default Domain. This assignment is transparent to users who are not using custom IP domains to identify monitored traffic.

How Do IP Domains Work with UC Monitor?

The task of creating IP domain definitions is performed in CA Performance Center. But the UC Monitor administrator determines the IP domain assignments of monitored items by selecting the appropriate IP domain for each collector.

After IP domain definitions are synchronized with data sources, they are available for use during data collection configuration. Define at least one custom IP domain in CA Performance Center to expose the necessary parameters in the UC Monitor management console.

The IP domain definitions that are synchronized to UC Monitor are assigned to collectors. A collector associates all discovered items with the default IP domain until the administrator assigns a custom IP domain in the collector Properties dialog. These items are then automatically associated with the custom IP domain, but only as they are rediscovered. IP domain assignments are not applied retroactively.

Endpoints (see definition on page 60) are discovered during monitoring. Locations and call server groups are not. You manually edit Location definitions to select a custom IP domain for the IP Domain field. Otherwise, Locations are placed in the default IP domain.

After you create an IP domain, the Location List reflects the new IP domain after the first synchronization. New default Locations for the <External>, <None>, and <Unassigned> categories are included in the list so that one of each appears in each domain. Each IP domain, including the default IP domain, must retain these Locations so that all endpoints detected in call traffic can be properly classified. IP domain designations also appear in report views, where an IP Domain column indicates domain identity.

Enable IP Domain Monitoring at the Collector

After you define an IP domain in CA Performance Center and data source synchronization has occurred, the IP Domain field is available in the collector Properties dialog. The collectors that you add to a distributed system also have this field. Use this field to associate a selected IP domain with the performance data taken from calls running between monitored endpoints (see definition on page 60).

Follow these steps:

1. Click Administration, Data Collection, Collectors in the navigation bar.

   The Collection Device List opens.

2. Select a collector.

3. Click Edit.

   The Collection Device Properties page opens.

4. Select the appropriate domain from the IP Domain field.

5. Click Save.

6. Repeat steps 2 through 5 for each collector. Each collector creates an association with the same IP domain for all phones and devices that it discovers.

7. Reload the collectors to send them the domain information.

   After you configure the system, the IP domain designation is included for each endpoint where it appears in reports. You can also verify IP domain identity in the Location List or Voice Gateway List.

Note: IP domains are populated with managed items when items are discovered from call traffic. You manually assign IP domains to Location definitions because Locations are not discovered. For more information, see Change Domain Assignments (see page 49).

Enable IP Domain Monitoring at the Lync Collector

When you configure a Lync collector in a Microsoft environment, data is automatically associated with the default IP domain.

The following tips are best practices for Microsoft customers who use multiple domains.

- Each monitoring server is automatically discovered in the default IP domain. All of its data is associated with the Locations and media devices in that IP domain.
- Change the IP domain association of each Lync collector server, which rediscovers call servers and media devices for that domain.
- Create or import Location definitions for the IP domain. You can perform this task before or after the collector IP domain is updated. From this point on, all data that is received from the Lync collector is associated with the proper IP domain.

- Across all IP domains, the initial data collection from each monitoring server (for example, from each MSP customer) is discovered in the default IP domain. Ideally, instances of overlapping data are brief.
- Do not use the default IP domain for user permissions.
- You can delete call servers and media devices that are associated with the default IP domain.

Using IP Domains as Permission Groups

As a best practice, add IP domains to user accounts to let users see the items in the domains. Permission to see an item in an IP domain automatically grants access to all other items in that domain. You do not need to grant explicit permission for each item in an IP domain. Similarly, do not add the All VoIP Locations domain to user permissions in a multiple-domain environment. Doing so implicitly grants that user access to data from all IP domains.

Another best practice is to grant the administrator permission to see all IP domains. This action simplifies IP domain administration. For example, the administrator can see IP domain identifiers for all collectors, Locations, call servers, and voice gateways. By contrast, individual users only need access to one IP domain.

Avaya trunk groups do not have IP domain identifiers. As a result, they are not included when you add IP domains to user account permissions. Instead, you add Avaya trunk groups as individual permission groups. Locations, media devices, and call servers are managed items, with IP domain identifiers based on your collector configuration. Avaya trunk groups are treated as groups in CA Performance Center, and groups do not have IP domain identifiers.

Change IP Domain Assignments

The process of classifying collected data in the UC Monitor database prevents Location and IP domain designations from being applied retroactively. Subnets that were already in the database when they were added to a Location definition remain categorized as <Unassigned> in historical data views. These same subnets are correctly placed in the Location in new views. Similar logic applies to the use of custom IP domains. Those same subnets are associated with custom IP domains when new calls are made, with no effect on data already collected.

When you create an IP domain in CA Performance Center, all Locations that were previously defined are associated with the default IP domain. You can edit Locations to remove subnets, select the custom IP domain, and then add the subnets back to the Locations. This manual procedure is often time-consuming. We recommend the following work flow instead.

Follow these steps:

1. Export the current list of Location definitions, as discussed in Export a List of Locations.
2. Verify the contents of the exported .csv file.
3. Delete all Location definitions, as discussed in Manage Location Definitions.
4. Select the new IP domain in the Properties dialog, as discussed in Enable IP Domain Monitoring at the Collector (see page 48).
5. Import the .csv file, as discussed in Import Location Definitions.

Delete IP Domains

Like the associations between performance statistics and managed items, IP domain associations are stored with items in the UC Monitor database. As a result, you cannot delete IP domains from UC Monitor. Deleted IP domains are marked as inactive in UC Monitor and not exposed in reports that display new data. For example, you can deregister and then reregister the UC Monitor data source. At the first synchronization, the inactive IP domain is sent to CA Performance Center because managed items in the UC Monitor database retain the association.

In most cases, the following work flow is recommended.

Follow these steps:

1. Delete the IP domain from CA Performance Center. For more information, see the *CA Performance Center Administrator Guide*.
2. Change the assignment in the IP Domain field for the deleted domain. For more information, see Change Collection Device Properties.

   Note: Select another IP domain for the collector. Otherwise, the collector associates items with the default IP domain.

   Data that was previously collected and associated with the deleted IP domain remains associated with it and is displayed as such in historical reports.

What are Groups?

The Groups feature is a powerful tool that lets administrators organize data and control who can view it. When a performance issue is reported, the permission groups that are assigned to user accounts let operators effectively analyze data in a logical flow. From a group, operators can drill down to information about one item in the group.

The administrator can create a custom group structure to organize managed items in CA Performance Center. Groups act like filters to organize related items and make reported data more useful. For example, a group can represent a physical location, a device and its interfaces, or a group of similar devices. Custom groups let operators view the items they must monitor while limiting their access to the selected data.

Properly configured, groups can prevent CA Performance Center operators from viewing selected data for security reasons. The administrator can selectively grant user access to data that falls within their area of responsibility. Groups can also facilitate performance monitoring, reporting, and troubleshooting.

Tenants include special types of system groups to maintain separation among customer deployments. Tenants can also contain entire custom grouping structures.

Types of Groups

Groups are organized into a hierarchical tree structure. The Groups tree helps you define relationships, policies, and dependencies among services, devices, applications, locations, and users within your organization. The following list summarizes the types of groups shown in the Groups tree:

System Groups 

Are read-only groups automatically created by CA Performance Center based on information provided by data sources. These groups cannot be edited (as indicated by the "lock" symbol). But they can be viewed, applied as permission groups to user accounts, or copied to custom or site groups.

Custom Groups 

Create hierarchical levels and organize items into logical relationships within the Groups tree. Custom groups at the top level of the Groups tree typically represent geographical, topological, or functional divisions within your organization. Lower-level custom groups (or subgroups) typically represent managed item types, such as devices, services, or applications. Or these subgroups can represent the job functions of IT staff.

Only administrators can create and edit custom groups. They filter the data presented in CA Performance Center dashboards and views. The group context for a dashboard or view determines the data that is presented.

Site Groups 

Are special custom groups based on sites, such as branch offices, or on physical locations, such as regions or cities. Site groups let you create navigation functions within CA Performance Center dashboards to present views across all sites. They also provide a granular context to apply to dashboards. For example, after you create a site group for each of your sites, a single dashboard can report on each site individually. We strongly recommend creating a site group for each data center within your enterprise and for other major infrastructure locations.

Group References 

Are read-only copies of system or custom groups. When you copy a group to another location in the Groups tree, a group reference appears. User permissions can be allocated using group references. Using references lets you create a group structure once, and then copy that structure to other parts of the Groups tree. Changes to group references can only be made to the original custom group, but they are propagated to all reference locations.

Select a group reference to access a link to the original group. Clicking the link expands the node in the Groups tree and opens the Properties tab for the original group.

Recommendations for UC Monitor Groups

Use UC Monitor groups to organize your call servers, media devices, voice interfaces, and Locations. Properly organizing your devices and Locations into groups lets you:

- Manage and organize UC Monitor reports.
- Assign UC Monitor user permissions appropriately.

Set up groups that resemble the reporting structure of your IT organization, the geography of your organization, or the logical structure of your system. To ensure group validity, always position call servers and media devices at the nodes in the Groups tree where access permissions are applied. Groups can contain multiple levels of subgroups. A user with permission to view a group can also view all of its subgroups.

You cannot manage groups in the UC Monitor management console. To create and edit groups for Locations and devices, register UC Monitor as a data source for CA Performance Center. After registration is complete, access to the group management interface requires you to log in to CA Performance Center with administrator privileges.

Note: For complete information about managing groups, see the *CA Performance Center Administrator Guide*.

Working with Avaya Trunk Groups

During SNMP polling by the collector, the Avaya Communication Manager reports Avaya trunk group names. Administrators typically use these group names when configuring the system through the Avaya Site Administration (ASA) interface. This practice can easily lead to redundant trunk group names, which then appear identical in reports.

We recommend using the ASA interface to assign unique names that make each trunk group readily distinguishable in CA Performance Center reports. You can change names after monitoring has begun. No report data is lost because internal identifiers correlate the previous names with the new ones.

Important: You can add an IP domain to a user account as a permission group. You add Avaya trunk groups with that IP domain assignment as individual permission groups. These trunk groups are treated as groups in CA Performance Center. Groups do not have explicit IP domain identifiers.

More information

What are IP Domains? (see page 45)

Working with Cisco Trunk Groups

In a Cisco environment, use trunk groups to reflect your actual usage and routing patterns in UC Monitor reports.

Trunk groups are not discovered from the call servers or from network traffic, but are instead created as groups of voice interfaces in CA Performance Center. You can see them on the CA Performance Center Inventory tab.

Create group rules that automatically place gateway voice interfaces into custom groups, which you designate as trunk groups using a clear naming convention. These special trunk groups can only contain items of the voice interface type.

Cisco administrators must periodically verify the voice interface capacity values from a device MIB. This information can be viewed on the Voice Gateway Properties page. The Voice Interface reports use the information in the Channel Capacity column to calculate interface usage as a percentage of capacity. These reports are less accurate when the device MIB incorrectly reports the gateway voice channel capacity.

As a best practice, verify that all known gateway voice interfaces have the number of channels correctly configured. The collector typically can get this capacity information from polling the gateway. If it changes, however, this information is not updated in the device MIB. To verify Cisco voice interface capacity data, see Managing Voice Gateways.

UC Monitor operators can see unexpected items in reports when you do not carefully create groups and user account permissions. Specifically, do not place gateway voice interfaces in groups that you then copy into subgroup containers. An operator with permission to view a container group can also see all its subgroups. As a result, that operator can see the same interface group twice in the Top Trunk Groups report: where it appears in its own group, and where it appears in its container group.

This behavior is unavoidable because the Trunk Group reports do not handle container groups the same way that they handle trunk groups. Specifically, only the custom groups that (directly) contain at least one voice interface are identified as trunk groups. To UC Monitor, a voice interface that belongs to a trunk group *and* to a subgroup is included twice in the Top Trunk Groups report. The voice interface does not appear to be a duplicate because only one instance is a member of a trunk group.

To avoid duplication of trunk groups in the Trunk Group reports, verify that trunk groups contain only voice interfaces. When a non-voice interface item is detected, the group is not handled as a trunk group. And then either:

- Do not place trunk groups into container groups that you then copy into other positions in the Groups tree.
- Assign permissions at the level of each specific trunk group, not above it, at the container level.

What are Tenants?

By default, all managed items and their data are associated with the Default Tenant. Adding custom tenants to CA Performance Center lets you create separate CA Performance Center monitoring environments that you administer from a single user interface. A *tenant* represents a customer environment that a managed service provider administers. Each tenant environment is independent and effectively functions as a separate instance of CA Performance Center. Each instance can contain multiple users and roles that are not shared among tenants.

The basic tenant definition contains a few parameters to identify the MSP customer and let other operators access managed items and configuration for the customer. Each tenant must contain at least one IP domain. You or the tenant administrator can then set up as many of the following definitions as required to manage the enterprise infrastructure and applications:

- SNMP profiles
- Additional user accounts
- Roles
- Custom groups
- Custom dashboards
- Custom menus

Custom IP domains provide the means of associating managed items with their tenants. A valid tenant definition contains at least one custom IP domain. As soon as a valid tenant exists in CA Performance Center, all items whose IP addresses match the tenant domain are associated with that tenant.

Glossary

ACOM

The total echo return loss on the network. ACOM measures how significantly the voice gateway reduced the echo. ACOM includes echo reduction that occurs with or without the activity of an echo cancellation device.

all channels busy

The percentage of the reporting interval for which all active channels in a trunk group carried traffic.

analog telephone adapters (ATA)

A device used to connect a standard telephone to a computer or network so that the user can make calls over the internet. ATAs are typically cheaper than specialized VoIP phones that connect directly to a computer's USB port. An ATA typically supports one or two ports.

Answer Seizure Ratio (ASR)

The number of successfully answered calls compared to the number of call attempts.

Application Enablement Services (AES)

The Avaya application server that provides system management APIs.

audio/visual conferencing server

A server in a Microsoft Lync environment that enables audio and video (multi-party) conference calls. Also referred to as an A/V MCU.

Automatic Number Identification (ANI)

A feature of telephony that lets subscribers display or capture the telephone numbers of calling parties.

burst

The points in a data stream when a high percentage of packets is lost or discarded due to packets arriving late.

burst density

The percentage of packets within burst periods that are lost or discarded.

burst duration

The average duration of all high-loss periods in a data stream.

busy-hour call attempts (BHCA)

The number of calls attempted at the busiest (peak) hour of the day.

busy-hour call completions (BHCC)

The number of calls completed at the busiest (peak) hour of the day. BHCC is a measure of the throughput capacity of a VoIP network.

call detail record (CDR)

Storage of information about the endpoints of a call and other aspects of call control and routing.

call leg

A discrete segment of a call connection in a VOIP network. A logical connection between a router and an endpoint.

call management record (CMR)

Storage of information about the quality of the streamed audio of a call.

call minutes

The number of minutes that calls were active during the selected time period.

call path

The path, or route, a call takes between the origination and destination endpoints in a network.

call setup

A series of connections that occur between a telephone placing a VoIP call and the active call server. The call server is responsible for certain signaling to the telephone that allows it to play a dial tone and make the call. The call server also establishes a connection to the destination endpoint in the PSTN. The call setup protocol defines the messages that are passed among the call server, gateway, and endpoints.

call setup failures

The calls that fail to connect during the setup phase. Expressed as a percentage of all calls that were attempted during the monitoring interval.

call setup protocol

Protocols involved in the call setup process: SIP, SCCP, H323, and MGCP.

calls attempted

All calls that the monitored system tried to place, either successfully or unsuccessfully. This metric is the primary unit of measurement for the Call Volume Audio views.

calls completed

The number of audio-only calls that were successfully completed during the selected time frame. Includes calls from endpoints within the monitored system and calls from *outside of* the system to endpoints *inside of* the system.

channels out-of-service

The number of channels in a trunk group that are out of service.

Cisco CallManager cluster

A group of physical servers, running Cisco Unified Communications Manager (CallManager), to work together as an IP PBX system.

Cisco IP Communicator

A Microsoft Windows-based softphone application for making voice and video calls.

Cisco Performance Monitor

A feature of Cisco routers and switches that enables reporting of quality metrics for a medianet environment.

codec

Codecs (the term is short for coder-decoder) convert an audio signal into compressed digital form for transmission and then back into an uncompressed audio signal for replay.

concealment

A technique for masking the effects of packet loss in VoIP communications. Also known as packet loss concealment (PLC).

concealment ratio

The percentage of frames in a data stream that are concealment frames, which the endpoints generate to conceal packet loss. Includes both early and late packets.

conference ID

Identifier for a voice gateway call.

connection attempts

The number of times a connection to the server is attempted before timing out.

controller LAN board (C-LAN)

G650 voice gateways can have C-LANs defined and running on the device as separate call servers. Each C-LAN has a dedicated IP address, which appears in UC Monitor reports as a call server. However, the actual call server is the Communication Manager, which is usually installed on a separate media server.

conversational MOS

The Mean Opinion Score (MOS) based on metric factors from both directions of data flow.

currently missing phones

The percentage of endpoints that were registered to a server in the group, but are no longer registered to any server in the group, and were never observed to have been formally unregistered.

delay

see latency (see page 63)

delay to dial tone

The amount of time it takes for a user to hear a dial tone after picking up the receiver of an IP telephone. During the call setup phase of a VoIP call, the device receives messages from the call server to play a dial tone. Users can think that the system is not working when dial tone is delayed.

Differentiated Services Code Point (DSCP)

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

digital telephone

Digital telephones convert analog sound into digital format at the handset. Digital telephones do not include web browsers or more advanced applications generally available from IP telephones.

directory number (DN)

A telephone number.

echo

The phenomenon of your voice coming back to you, as if you were repeating yourself. In a VoIP network, echo is accentuated by the amount of delay in the network.

Echo Return Loss (ERL)

Reduction in the echo level produced in the circuit without an echo canceler. The degree or amount of loss reflects the volume of the echo that remains, and a measurement of how significantly echo was reduced.

Echo Return Loss Enhancement (ERLE)

An enhancement in the echo return loss that an echo canceler produces. An echo canceler removes the echo portion of a VoIP call signal as it exits the tail circuit and heads into the WAN. Also referred to as *cancellation loss*.

echo tail length

The “length” of echo cancellation processing. Based on the distance between a voice gateway and the endpoint. Typical values range from 8 milliseconds to 32 milliseconds.

edge server

In a Microsoft Lync environment, a server running in the perimeter network to provide connectivity for external users and public instant messaging connections. The edge server ensures that users outside the firewall are authorized before they obtain access to the Lync deployment. The edge server also provides media relay for audio/visual streams where direct connection is not possible.

egress interface

The interface where traffic exits a device.

endpoint

An endpoint is any device where a media stream begins or ends, such as telephone, softphone, telepresence, voice gateway, media device, and video camera.

erlang

In telephony, a statistical measure of the volume of telecommunications traffic. Traffic of one Erlang refers to a single resource being in continuous use, or two channels being at fifty percent use, and so on.

failover

Failover is the process of switching to a backup server or system when the primary server or system fails, is offline, or becomes unavailable.

Flexible NetFlow

The next generation in flow technology from Cisco. Flexible NetFlow enables the delivery of medianet data to UC Monitor.

front-end server

In a Microsoft Lync environment, a server that typically performs call processing functions. Microsoft Lync supports a pool of one or more front-end servers working together to perform functions such as call processing.

frozen period

The average length of frozen video instances.

frozen video frequency

The frequency of long and noticeable frozen video periods for an entire session. Expressed as a percentage of session time.

G.107

An ITU-T standard for reporting VoIP conversational call quality. UC Monitor uses this standard to calculate MOS from the voice gateway's perspective at the end of an IP-PSTN call.

G.711

A high-performance, high bit-rate codec (64 Kbps) often used for its excellent voice quality. Because it does not use compression, G.711 requires more bandwidth than some other common codecs.

gap density

The percentage of lost or discarded packets in the gaps between bursts in a data stream.

gap duration

The average duration of periods of good performance (low loss) between periods of data loss in a data stream.

gatekeeper

An optional component of a VoIP network that provides services such as endpoint registration, address resolution, admission control, and user authentication.

gateway

A device that provides the conversion interface between the PSTN and an IP network.

Grade of Service (GoS)

An estimation of the probability that a VoIP call receives a busy signal. The GoS value (a decimal fraction) is always expressed with reference to the busy hour when the traffic intensity is the greatest. GoS is reported from the perspective of the origination Location or gateway device (the outgoing direction).

group overflows

The number of outgoing calls presented to the trunk but not carried. *Overflow* calls arrived when all trunks in the trunk group were busy, but were not queued on the trunk group. This value does not include calls that were denied service on the trunk group because of authorization failures.

H.323

An ITU standard protocol for call setup. UC Monitor supports gateways that use this protocol to communicate with Cisco Unified Communications Manager.

ingress interface

The interface where traffic enters a device.

Interactive Connectivity Establishment (ICE)

A mechanism for SIP-based VoIP clients to successfully traverse the variety of firewalls that may exist between a remote user and a network.

jitter

Packet delay that distorts the quality of a voice conversation.

jitter buffer

Buffers that attempt to reduce or eliminate network jitter by caching packets. If jitter exceeds caching capacity, packets are lost (jitter buffer loss).

jitter buffer delay

Delay that the jitter buffer introduces while it holds one or more packets to reduce variations in packet arrival times.

jitter buffer loss

The packets that are lost when jitter hinders the caching capacity of the jitter buffer.

jitter buffer over runs

The number of times that jitter exceeded the maximum size setting of the jitter buffer. Packets arrive too quickly to be contained by the jitter buffer. Over runs usually result in packet loss.

jitter buffer under runs

The number of times that the jitter buffer became empty. Packets arrive too slowly to be contained by the jitter buffer. Under runs usually indicate that delays are too lengthy for the buffer setting.

keepalive

A message sent by one device to another to verify that the connection between the two is operating, or to prevent the connection from breaking.

latency

One-way delay. Calculated from the origination party to the destination party. Includes propagation delay, network delay, and packetization delay.

Listening MOS

The Mean Opinion Score, which is based on call legs traveling toward the endpoint to reflect listener perception of quality.

Mean Opinion Score (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.

mean time to repair (MTTR)

Time required to repair a failed component or device. MTTR is also defined as "mean time to recovery," which is the amount of time required for a device to recover from a failure.

media device

Specialized devices to route calls from the PSTN, handle conference calls, or transcode media streams. Examples include voice gateways, mediation servers, conferencing servers, and unified messaging servers.

Media Gateway Control Protocol (MGCP)

Signaling and call control protocol used in a distributed VoIP system.

media processor

The IP termination point for audio. It performs the conversion between time-division multiplexing (TDM) and IP. The audio payload is encapsulated in RTP, then UDP, then IP.

media relay

An edge server function used with interactive connectivity establishment to provide end-to-end delivery of media streams where direct connectivity between two IP endpoints is not possible.

medianet

A medianet is an IP architecture that enhances the performance of video, voice, and data, and automates many aspects of configuration.

mediation server

Handles calls from the PSTN and interoperates with media devices that are outside the Microsoft Lync environment, such as other IP telephony environments.

midstream device

A medianet-enabled device, such as a router or switch, that sends NetFlow data to UC Monitor to report on the quality of audio or video streams.

narrowband codec

Compresses and decompresses traditional speech, covering frequencies 300 to 3400 Hz, to more easily fit over an IP network.

NetFlow

Developed by Cisco, this network protocol collects IP traffic information.

network congestion

Occurs when a network device carries so much data that the QoS deteriorates. Network congestion can result in packet loss and delay.

network delay

Transport delay produced by intervening network equipment, such as routers and switches.

Network MOS

MOS listening quality value that is based only on network factors, such as codec, packet loss, packet reordering, packet errors, and jitter.

noise level

(*Microsoft only*) The average portion of an audio signal that is noise and not actual voice data. Measured in decibels.

origination/destination

The origination phone initiates the call. The destination phone receives the call.

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.

packetization delay

Delay introduced by a codec.

port mirroring

On a network switch, the port mirroring function sends copies of network packets from one port to another switch or port for analysis. The port mirroring function on Cisco switches is named Switched Port Analyzer (SPAN).

post-dial delay

The amount of time from when a user enters the last digit of a telephone number to when the user hears a ring or busy signal.

POTS

Plain Old Telephone System. The voice-grade telephone service that is the basic form of residential and small business service connection to the telephone network in most parts of the world.

presence

In a unified communications environment, the ability for users to know the status and availability of other users.

propagation delay

Delay produced by the physical distance that packets travel in a data transmission.

PSTN

Public Switched Telephone Network. The network of the world's public circuit-switched telephone networks, in much the same way that the internet is the network of the world’s public IP-based packet-switched networks.

Publisher

Required member of the Cisco Unified Communications Manager cluster that publishes database (config) updates to other members of the cluster. In failover situations, the Publisher can take over call processing functions from the Subscriber.

Quality of Service (QoS)

QoS provides different priorities, or throughput levels, for different applications, users, or data flows on a packet-switched telecommunications network.

Quality Report Tool (QRT)

A problem-reporting tool for Cisco IP phones, which allows users to easily report audio and other general problems with their IP phone. Many Cisco phones have a QRT softkey.

queue abandons

Calls that were removed from the Trunk Group Queue.

queue overflows

The number of calls that arrived when all slots in the Trunk Group Queue were busy.

Real-Time Control Protocol

An IETF standard for providing out-of-band statistics and control information for an RTP flow. Generally sent over the next highest odd-numbered port as the corresponding RTP flow. RTCP provides feedback on the QoS in media distribution.

Real-Time Transport Protocol (RTP)

An IETF standard for delivering audio and video over the Internet. Generally sent on an even-numbered UDP port.

R-value

R-value is a number, or score, that is used to quantitatively express the subjective quality of speech in a VoIP network. The R-value can range from 1 (worst) to 100 (best), and is based on the percentage of users who are satisfied with the quality of a test voice signal after it passed through a network from a source (transmitter) to a destination (receiver). In many cases, an R-value is mapped to a MOS, which is used most frequently when referring to VoIP call quality.

sending/receiving

All endpoints that are involved in a call are, at some point, a sender and a receiver. During a call, all endpoints send data (talk) and receive data (listen).

sequence falls

The number of times that at least one packet arrived out of order.

sequence jumps

The number of times that at least one consecutive packet was lost.

Session Initiation Protocol (SIP)

A signaling protocol for setting up and tearing down multimedia communication sessions such as voice and video calls.

severely concealed seconds

The number of call seconds that had more than 5 percent concealment events from the start of the data stream.

signal level

The average audio signal level in decibels (dBm0).

Simple Network Management Protocol (SNMP)

Protocol for managing devices on IP networks. A network that is managed by SNMP consists of a managed device, an agent on the managed device, and a network management system on the manager.

SIP Enablement Services

The SIP proxy server for Avaya SIP endpoints.

SIP trunking

A service offered by an Internet Telephony Service Provider that permits businesses with a PBX to use VoIP outside the enterprise network by using the same connection as the Internet connection.

Skinny Call Control Protocol (SCCP)

A proprietary Cisco messaging protocol that is used between clients (phones) and the Cisco Unified Communications Manager in a VoIP environment. SCCP passes messages using TCP and port 2000.

stream leg

Unidirectional stream of packets.

Subscriber

A server in the Cisco Unified Communications Manager cluster that typically performs call-processing functions.

successful call ratio

Number of successful call completions divided by the number of call attempts.

Time to Live (TTL)

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.

traceroute

A diagnostic tool that displays the route (path) and measures the transit delays of packets across an IP network

trunk group

A group of trunks serving the same special purpose. The term commonly is applied to voice Private Branch Exchange (PBX) trunks.

trunk group ID

The trunk group number for a voice gateway call in a Call Watch. The phone number of the endpoint that sends data through the gateway cannot be identified while the call is in progress. The trunk group ID is substituted for the phone number and displayed in the Phone Number field until the phone number is identified.

unified communications

The convergence of multiple modes of communication (such as phone, video, and email) within applications and infrastructure to allow people, teams, and organizations to communicate more effectively.

Uniform Resource Identifier (URI)

A user's SIP phone number. A SIP URI may resemble an email address, such as sip:john.smith@ca.com.

VG 224 gateway

A Cisco gateway device that lets analog phones connect to an IP PBX, which typically supports 24 analog phones. All phones are assigned the same IP address with different port numbers.

video bit rate

The number of bits sent per second for an entire video stream. Bit rates provide a gauge of codec performance.

video frame decoding time

The average amount of time for decoding frames in a stream. A slower decoding rate can be the result of conditions on the endpoint, such as lack of CPU resources, and can affect call quality.

video frame loss

The average number of unique consecutive images, or video frames, lost due to corruption and error concealment for the entire system. Video frames can span multiple packets.

video frame rate

The average number of frames that were sent or received per second for an entire stream.

video jitter

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

video latency

The maximum time for a video packet to travel between the calling parties. Measured from end-to-end in one direction. Calculated by taking the average round-trip time for a call leg in a given video call and dividing it in half.

video packet loss

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

VLAN ID

The ID of the virtual local area network (VLAN) that carries RTP packets.

voice gateway

A router or switch with a specialized card that enables VoIP calls to and from the PSTN.

Voice over IP (Voip)

A set of technologies, protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

VoIP trunk

A large bandwidth channel that handles multimedia data and forms the backbone of a network. In telephone exchanges, a trunk simultaneously transmits data and voice packets from one point to another.

weighted average

A computation for an average value that takes into consideration the number of observations.
For example, to compute the value of average jitter across sites in your network, use the following calculation:

(site1 avg + site2 avg + site3 avg + site *N* avg) divided by *N*

where *N* is the number of sites.
To compute weighted average, use the following calculation, which allots more weight to sites with more jitter:

(*o*1(s1) + *o*2(s2) + *o*2(s3)+ o*N*(s*N*)) divided by (*o*1 + *o*2 + *o*3)
where *N* is the number of sites and *o* is the number of observations.

wideband codec

Compresses and decompresses wideband speech, such as high-definition voice, to more easily fit over an IP network.

Index

J

L

M

N

P

R

S

T

U

V