NetQoS
Performance First

NetQoS® Unified Communications Monitor v3.0 User Guide

www.netqos.com

NetQoS Unified Communications Monitor User Guide

DV30UG-0

The contents of this document are for informational purposes only and subject to change without notice. No liability is assumed for technical or editorial omissions contained herein.

Required Notices of Third Party Copyright and License Information

The Vovida Software License, Version 1.0
Copyright (c) 2000 Vovida Networks, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names “VOCAL”, “Vovida Open Communication Application Library”, and “Vovida Open Communication Application Library (VOCAL)” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact vocal@vovida.org.
4. Products derived from this software may not be called “VOCAL”, nor may “VOCAL” appear in their name, without prior written permission of Vovida Networks, Inc.

THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-

INFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL VOVIDA NETWORKS, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT DAMAGES IN EXCESS OF $1,000, NOR FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1994 The Regents of the University of California. All rights reserved.

1. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
2. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
3. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
4. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
5. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS," AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

@(#)COPYRIGHT 8.1 (Berkeley) 3/16/94

Portions of the Product were created using source code governed by the Mozilla Public License (MPL).

The source code for the portions of the Product governed by the MPL is available from http://www.mozilla.org under those licenses. Modifications to the source code are provided by NetQoS and are available from: http://www.netqos.com/support/ssp

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Contents

PREFACE

About This Document

This document provides information and procedures to help you effectively use NetQoS Unified Communications Monitor. It includes technical information about unified communications technologies to help you understand how NetQoS UC Monitor works to ensure the performance and health of your VoIP and video system.

UC Monitor has been updated to provide a broader range of monitoring and reporting features, including additional support for unified communications deployments by different product vendors. Some of the capabilities of previous product releases have been enhanced.

The *User Guide* contains the following chapters:

Chapter	Description
Chapter 1, “Introduction”	Describes the UC Monitor approach to monitoring voice and video over IP and explains how it works.
Chapter 2, “VoIP and Video Concepts”	Provides background information about unified communications and detailed information about the UC components that you can monitor.
Chapter 3, “Using NetQoS UC Monitor”	Describes the features you will be using to monitor your system and provides step-by-step instructions for performing troubleshooting tasks and diagnostics.
Chapter 4, “UC Monitor Reports”	Explains the metrics that NetQoS UC Monitor gathers and rates and helps you interpret data and navigate reports.
Appendix A, “Calculating a Mean Opinion Score”	Provides background information about how the MOS data that the UC Monitor product collects is calculated.
Appendix B, “Integration with the NetQoS Performance Center”	Describes how you can view data collected from your UC system in the NetQoS Performance Center product and outlines the latest cross-product integration features.
Appendix C, “Viewing Events in the Event Manager”	Provides an overview of UC Monitor support for the NetQoS Event Manager.

Related Documentation

In addition to this book, you can find useful information in the following publications:

Document	Description
UC Monitor Release Notes	Summarizes product features, supported VoIP hardware, and open issues.
UC Monitor Administrator Guide	Provides task-based information for UC Monitor Administrators to help them install the product, configure the system, and set reporting parameters.
UC Monitor online Help	Provides context-sensitive Help that can be accessed from the Help link in the UC Monitor user interface.

The product documentation is available in PDF format on the server where the UC Monitor Management Console is installed. Find the PDF files in the following location:

```
D:\NETQOS\UCMonitor\WebSite\Docs
```

The current versions of the PDF files for the product documentation, including the Release Notes, are always available on the NetQoS Self-Service Portal.

Conventions

The following conventions are used in this book:

- In instructions, **boldface** type highlights information that you enter or GUI elements that you select.
- All syntax and literal examples are presented in this typeface.
- In syntax, path names, or system messages, text enclosed in angle brackets (<>) represents a variable, as shown in the following example:

  `net time /setsntp:` <*ntpserver*>

Providing Documentation Feedback

We want to help you use our products effectively so that you can work quickly and efficiently. By telling us about your experience with this document, you can help us achieve that goal. Send an email message with your feedback to our technical publications team at the following address: docfeedback@netqos.com

CHAPTER 1

Introduction

NetQoS Unified Communications Monitor ensures the availability and performance of your voice over IP (VoIP) or unified communications (UC) system. By passively monitoring the call setup traffic and call audio or video quality associated with your IP phones, audio and video clients, call servers, and voice gateway devices, the UC Monitor system keeps a continuous record of VoIP and video call setup performance and call quality.

UC Monitor reports make it easy to view and analyze the data it collects. You can configure automatic actions to gather additional information for troubleshooting and diagnostics. And you can set performance thresholds, with automatic alerts to let you know about declines in call quality, failed calls, or call server issues before end-users have time to submit a Help Desk ticket.

This chapter provides an overview of the UC Monitor software and hardware and describes major product features. It contains the following topics:

- "Features and Benefits"
- "How the UC Monitor System Works"

Features and Benefits

NetQoS UC Monitor tracks and measures VoIP and video call performance from one end of the network to the other without using desktop or server agents. It performs end-to-end call performance monitoring for unified communications systems from Cisco Systems, Microsoft, and Avaya. With a NetQoS UC Monitor system, you can:

- Gauge how well your UC hardware and software are delivering services to the end user.
- Proactively monitor VoIP and video call-quality and call-setup metrics.

  You'll know immediately if users can't make calls, or if they're likely to think that the audio or video quality is low, based on industry-standard quality metrics.
- Receive a notification when call quality fails to meet a threshold.
- Receive a notification when call setup is slow, or when users cannot make calls.
- Gather call performance data from a single, targeted phone for use in troubleshooting an issue.
- Access call performance data in formatted reports that are easy to understand, analyze, export, and mine for detailed metrics.
- Leverage a full suite of analytics and reporting fueled by the most comprehensive data collection available by registering the UC Monitor data source with the NetQoS Performance Center.

The UC Monitor product provides a set of features that allow you to monitor call performance in your network, helping you to identify and resolve problems with your UC system.

UC Monitor Feature	Benefit
Measures how well the UC system is performing for end-users.	Proves system value and user quality of experience
Summarizes the performance of all calls in the system, including calls to and from the PSTN.	Monitors end-to-end performance
Automates the troubleshooting process, isolates problems, and eliminates finger-pointing within the IT organization	Solves end-user problems faster
Easily scales to monitor large VoIP or UC deployments.	Provides built-in flexibility
Provides safeguards to avoid false alarms; sends alerts only when call performance problems affect a designated minimum number of calls or call minutes.	Requires few operators
Integrates with the NetQoS Performance Center to provide a single, Web-based console to manage converged networks.	Simplifies system management

Product Components

The UC Monitor system includes both hardware and software components. The basic components are a **collection device**, a Web-based **console**, and a **database**.

The *UC Monitor Collector* (called simply *the Collector*) is a data collection device that, when attached to a mirror port or SPAN port on a core switch, monitors data flows to and from a Cisco Unified Communications Manager (CallManager®) call server or cluster of call servers. It inspects network traffic and collects data related to voice or video over IP performance. Specifically, it inspects any packets that use the MGCP, SIP, H.323, or SCCP protocols. The Collector sends data to the UC Monitor *Management Console* at regular intervals for storage, analysis, and reporting.

Without using a switch SPAN session, the Collector can also monitor Avaya UC deployments by means of both passive and active monitoring technologies. It receives and processes call-quality reports from Avaya endpoints and call data records from the Avaya Communication Manager and also polls supporting devices for information.

NetQoS UC Monitor also supports a second data collection device: the Microsoft® Office Communications Server 2007 Quality of Experience Monitoring Server, which can be configured to send call audio and video quality data to the UC Monitor Management Console. (The equivalent collection device in OCS R2 is the Front-End Server, which performs the functions of the QoE Monitoring Server.) In this architecture, the Microsoft server is called an *OCS Collector*.

The following table summarizes the UC Monitor components:

Component	Description
Collector	Device (hardware and software) that monitors VoIP network traffic in Cisco IP telephony and Avaya Communication Manager environments. Performs the following functions: • Collects VoIP-related performance data • Aggregates and sends the data to the Management Console
Management Console	Device (hardware and software) that processes, stores, and reports on VoIP-related network data. A database component that uses a MySQL server. A Web interface that enables you to: • Define the phone subnets to be monitored and send this configuration information to the Collector. • Create UC Monitor users and assign them roles with associated permissions to view reports and initiate diagnostic actions. • View reports. • Initiate diagnostic actions, such as the Call Watch feature.

You can install multiple NetQoS Collectors and have them all communicate with the same Management Console. Or you can install all the required components for monitoring Cisco or Avaya UC deployments as a single hardware device.

- In a **Standalone** system, the UC Monitor Collector and Management Console are installed on the same server.
- In a **Distributed** system, the Collector(s), any other collection devices, and the Management Console are installed on different servers.

For monitoring in a Microsoft Office Communications Server 2007 environment, the Collector component is not required. A separate chapter on installing and configuring the required Microsoft collection device is included in the *UC Monitor Administrator Guide*.

Also see the *Administrator Guide* for specific information about the recommended ratios for these components and the retention rates for the collected data.

How the UC Monitor System Works

NetQoS UC Monitor performs both **passive** and **active monitoring** of UC system health and call quality.

The **Collector** performs passive, agentless monitoring of Cisco call setup traffic passing through a switch. By passively observing VoIP-related packets and performing packet inspection of selected packets as they pass from the network into the call server(s) and out again, it can measure call setup time, jitter, and much more. From that data, it automatically discovers the call servers, media devices, such as voice gateways, and IP telephones that are running on a network and tracks call setup performance and call quality.

The same Collector can also monitor calls made by Avaya endpoints, which send frequent in-progress call-quality reports to their call server, the Avaya Communication Manager. The Communication Manager, in turn, sends the reports to the Collector.

The **OCS Collector** is actually a receptacle for call quality information reported by Microsoft audio and video endpoints. When configured as a UC Monitor collection device, this Microsoft server forwards the VoIP and video quality metrics it receives from Office Communicator endpoints and other supported devices to the UC Monitor Management Console for analysis and reporting.

Thresholds allow the UC Monitor software to detect performance exceptions and send alerts. UC Monitor processes measure and analyze the performance of VoIP-related call setup protocols, including SCCP, H.323, SIP, and MGCP. At regular intervals, supported collection devices send relevant call quality data back to the database at the **UC Monitor Management Console** for analysis and reporting:

- The **Collector** retains and transmits only the data that NetQoS UC Monitor needs to calculate and report the call setup and call quality metrics from calls made using Cisco or Avaya hardware.
- The **OCS Collector** receives end-of-call quality reports from the audio and video endpoints in the Microsoft Office Communications Server 2007 UC system, posts them in batches to a Web service on the UC Monitor Management Console, and also saves them as call data records (CDRs).

In a Cisco environment, the Collector also actively monitors the performance of voice gateways. By means of SNMP polling, it contacts voice gateway devices to gather data about call performance and gateway interface utilization. It runs a traceroute test to each voice gateway every four hours to provide baseline traceroute data. If you set up a Call Watch, the Collector actively polls Cisco IP phones and gateways for in-call quality statistics.

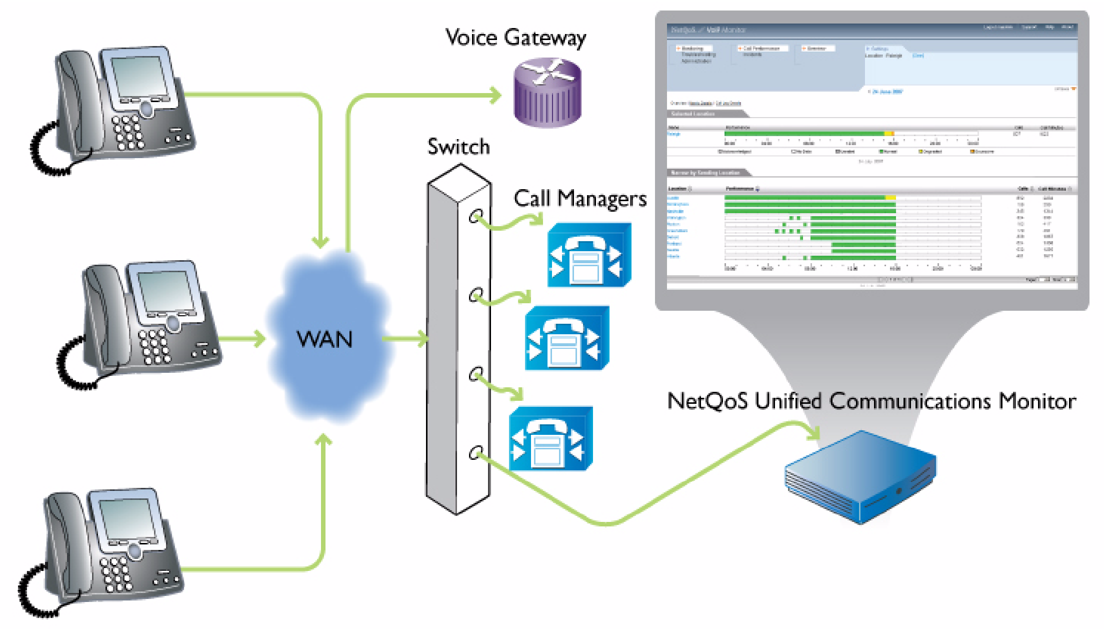
System Architecture

The UC Monitor system doesn’t actually “listen” to phone conversations. Most call performance measurements are derived from data flows to and from the call servers. For example, each Cisco IP phone reports quality data to its call server at the completion of every call; the UC Monitor Collector inspects these flows and calculates performance metrics. Similarly, each Microsoft Office

Communicator instance reports end-of-call quality metrics to a monitoring server, the OCS Collector, while Avaya endpoints that normally report these metrics to their call server are instructed to send this data to the Collector instead.

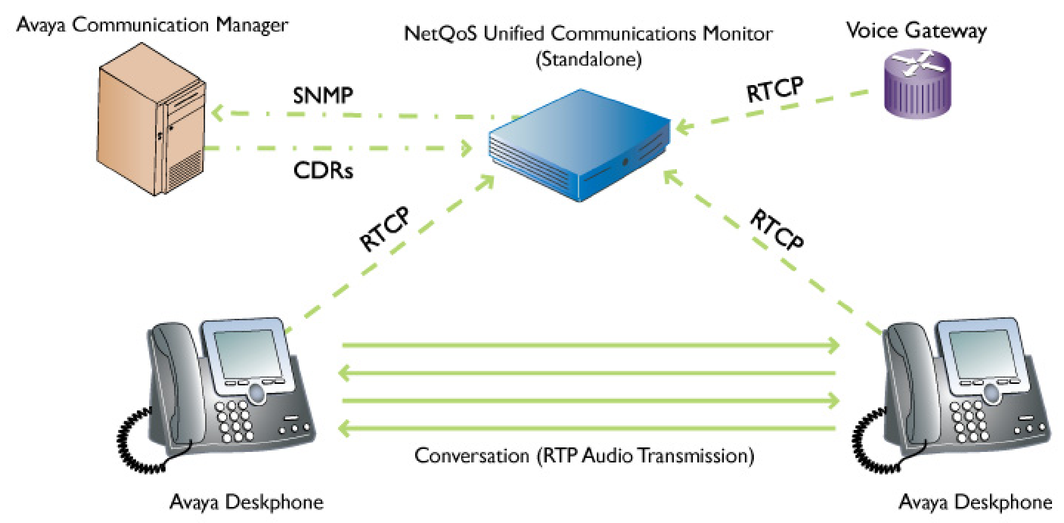
UC Monitor also gathers call quality and call setup data from media devices that support VoIP, and it times data flows between the calling phone and call server or media device to evaluate call setup performance.

Here's an illustration showing UC Monitor architecture and configuration for monitoring Cisco Unified Communications Manager. The UC Monitor Collector monitors call traffic through a SPAN port on a switch where Cisco call servers are connected:

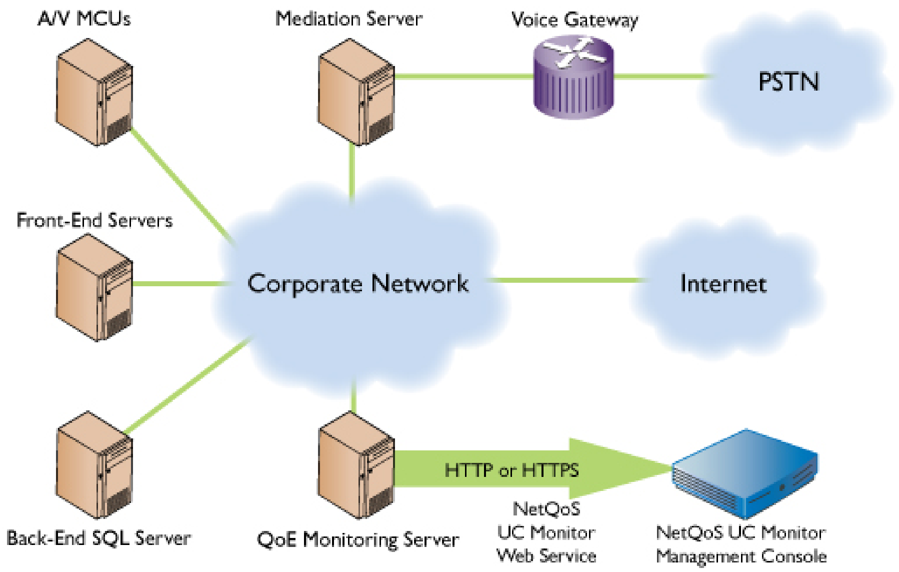


More information about switch SPAN port configuration is available in the *UC Monitor Administrator Guide*.

The architecture for monitoring Avaya is slightly different. No switch SPAN session is required; instead, endpoints (phones, communicator applications, softphones, and voice gateways) send quality reports directly to the Collector via RTCP, and the Collector polls the Communication Manager for information using SNMP:


Avaya Communication Manager
NetQoS Unified Communications Monitor (Standalone)
Voice Gateway
SNMP
CDRs
RTCP
RTCP
RTCP
Conversation (RTP Audio Transmission)
Avaya Deskphone
Avaya Deskphone

Yet another architecture is deployed in the Microsoft Office Communications Server 2007 environment:



No UC Monitor hardware is actually installed in the secure Office Communications Server 2007 network. In pre-R2 environments, an optional Microsoft server role, the Quality of Experience Monitoring Server, is installed to collect call quality information from supported VoIP and video endpoints at the end of each call. It uses a secure connection to post this information to a Web service running on the UC Monitor Management Console. For OCS R2 and later, the Front-End servers collect and forward this information from the endpoints.

VoIP and Video Call Performance Monitoring

NetQoS UC Monitor measures and tracks call audio and video performance and alerts you whenever performance levels fall below a default or custom threshold. Call performance monitoring consists of two components:

- **Call setup** monitoring, to make sure users are able to initiate and complete calls.
- **Call quality** monitoring, to gauge the clarity of the audio or image in the conversation.

To a user making a VoIP telephone call, each of these components contributes to a perception of that call's quality. The term *call performance* is meant to be comprehensive because a user's impression of quality is comprehensive. That's one reason why NetQoS UC Monitor performs comprehensive, end-to-end monitoring of your UC system.

Another reason for this approach is that "unified communications" is a simple term that can mask a complex reality. To start with, in a UC system, the audio and video signals travel over your data network and are therefore subject to the complexities and fluctuations of all the other traffic sharing the links. Multiple equipment vendors have implemented functions using multiple, sometimes proprietary, protocols. A single VoIP call might involve two IP phones and their call server, or it might involve a telephone in the PSTN, an IP phone, a voice gateway, and a call server; problems with call setup or call quality can occur at any of several network locations.

Collector Capabilities

In a Cisco or Avaya UC deployment, the standard UC Monitor Collector uses passive and active monitoring techniques to collect and aggregate call performance data.

For Cisco monitoring, the Collector passively monitors call setup flows at two points in their passage through the network:

- between VoIP phones and their call server, the Unified Communications Manager
- between call servers and voice gateways

Each Collector also performs the following types of monitoring when Cisco hardware is deployed:

Data Source	Method	Description	Protocols Monitored/ Used
Call setup flows and call quality flows	Passive	Collection and analysis of relevant network flows	SCCP, SIP, MGCP, H.323
IP phones	Active	Polling phones for call-quality metrics; traceroute testing every four hours for selected phones	HTTP
Voice gateways	Active	Polling of MIBs for management data; traceroute testing every four hours	SNMP

If an end-user reports a performance issue, you can initiate extra data collection for troubleshooting by setting up a Call Watch. During a Call Watch, the Collector actively monitors a selected Cisco IP phone that represents a particular network location, gathering data that helps you resolve the problem quickly.

When monitoring Avaya UC equipment, the Collector automatically performs Call Watch data collection from all call activity. Typically, call-quality data is collected every five seconds during an active call; the frequency of data collection is dependent on a Communication Manager setting. The resulting performance data is reported separately per call in the Call Watch Overview Report, and it is also included in the call performance charts that are displayed in the Call Performance Overview Report. See "VoIP Call Watch Monitoring" on page 8 for more information about this type of monitoring.

The UC Monitor product provides a great deal of data to help you fully understand the performance of your unified communications system, but it also summarizes the data in overview reports, rapidly conveying an overall impression of system performance.

Call Activity Monitoring

In addition to performance, NetQoS UC Monitor also monitors the call activity on your data network, providing a rich set of data about call volume, voice gateway and interface utilization, and the relative success rate of the calls attempted by network users. Any successful VoIP and video implementation relies heavily on bandwidth availability, which means that you need to be able to gauge and even predict network usage patterns to ensure adequate provisioning. And the last thing you need is to pay the full subscription price for underutilized links.

In the Capacity Planning section of the Management Console, UC Monitor reports provide data about the following:

- Call Attempts
- Call Completions
- Grade of Service
- Call Failures during setup (with the cause code)
- Utilization of voice gateways and of individual gateway voice interfaces

One significant metric used in gauging the size and capacity of your VoIP deployment is the busy hour call attempts, or BHCA. UC Monitor call activity reports provide the BHCA and BHCC—the busy hour call completions—for your network to help you with capacity planning.

VoIP Call Watch Monitoring

The UC Monitor Call Watch feature collects data from real-time monitoring of all calls made with Avaya Communication Manager and of selected Cisco IP phones for diagnostics. The Call Watch data is presented in a separate report, the "Call Watch Overview Report".

This feature is distinct from the core monitoring functionality of the UC Monitor product, which is largely passive monitoring based on the collection of all available VoIP-related data. Call Watch is performed on demand for selected phones in Cisco environments, and automatically for all calls made with supported phones or endpoints in the Avaya (Aura) Communication Manager environment.

In Cisco deployments, you can instruct the Collector to actively collect detailed, real-time call data for all calls made by a single, selected IP phone (or multiple phones). You set up a Call Watch definition by selecting a phone directory number (DN) and the duration of the watch period. See "Using the Call Watch Feature" on page 48 for more information.

Note: Call Watch is not supported in Microsoft-only UC environments.

Recommendations

When deploying unified communications, it is very important to measure its impact on your other business-critical applications and on your network infrastructure. You need to monitor and document the volume of voice and video traffic flowing across the network, who is generating it, and when. We support and recommend running UC Monitor in the same environment where you've deployed other NetQoS products, such as NetQoS SuperAgent, NetQoS NetVoyant, or NetQoS ReporterAnalyzer.

The **NetQoS Performance Center** lets you view reports of UC Monitor data alongside data views from the complementary monitoring products mentioned above. Security features, such as user accounts and their access permissions, are shared among NetQoS products and can be centrally administered if you register these products with the NetQoS Performance Center. Appendix B, "Integration with the NetQoS Performance Center" on page 151 discusses the integration of UC Monitor data with the NetQoS Performance Center.

NetQoS SuperAgent monitors TCP application performance. Automatic baselining and thresholds give you a deep understanding of how well your applications are performing. You'll be able to judge the impact of VoIP on the performance of your other critical applications.

NetQoS NetVoyant is an SNMP polling application that provides latency, jitter, and packet loss analysis for UDP streaming audio transmissions by running IP SLA (SAA) tests. In addition to several key VoIP metrics that you can test using NetVoyant, you'll also get SNMP statistics from your Cisco Unified Communications Manager servers.

NetQoS ReporterAnalyzer uses Cisco NetFlow to report on VoIP bandwidth consumption on every WAN link alongside other network protocols on the same links. You'll see real-time analysis and alerts for VoIP traffic if it exceeds rate, volume, or utilization thresholds, and you'll get help with capacity planning through trend data that will help you understand VoIP's growth over time. Plus, because ReporterAnalyzer gives you visibility into the traffic that is actually flowing over each link, you can use it to determine whether network components are correctly assigning VoIP traffic to the highest tier of QoS.

The **Event Manager** feature of the NetQoS Performance Center can accept Incident data from NetQoS UC Monitor and display it in the Event List and in the Map. UC Monitor events can be correlated with event data from other NetQoS data sources to help you quickly diagnose the root cause of performance issues. "Viewing Events in the Event Manager" on page 169 describes the relationship between UC Monitor Incidents and events.

CHAPTER 2

VoIP and Video Concepts

This chapter provides technical background information about unified communications—specifically, the voice and video over IP technologies monitored by NetQoS Unified Communications Monitor. This chapter will help you understand the challenges you face in delivering a high-quality user experience when acccessing the UC system. And the topics in this chapter also provide information that will help you understand the data that NetQoS UC Monitor collects and reports.

This chapter contains the following topics:

Understanding Unified Communications

The term “unified communications” is a relatively new one, and it’s still being defined. For NetQoS Unified Communications Monitor, the term refers to integrated applications to enable communications that extend beyond telephone service, and that use existing IP network infrastructure. UC represents the convergence of multiple modes of communication within applications and infrastructure to allow people, teams, and organizations to communicate more effectively.

The IP network provides the unifying factor for UC. Because UC relies on a converged network, often with multiple and extremely diverse applications vying for the same network resources, network performance is a critical enabler for all UC applications. And because UC is all about communications among people, assessing the user’s quality of experience when interacting with UC system components is the key to the delivery of these new services. If users have so little confidence in system performance that they avoid using the new, integrated modes of communication, UC is virtually useless.

NetQoS UC Monitor draws from the network-performance expertise of NetQoS engineers to extend the NetQoS *performance-first* approach to UC systems. As a result, it was designed to monitor UC applications and devices and measure their performance from the user’s perspective.

VoIP on Your Network

Many businesses rapidly lose sales opportunities if the phones go down for even a few minutes each month. Even if the success of your enterprise isn’t dependent on the ability to make and receive telephone calls, VoIP traffic still requires premium handling for the following reasons:

- **Network users are accustomed to excellent performance from their phone service**. It’s been excellent ever since they first picked up a telephone in their parents’ house. They will notice—and probably complain—if the quality of their VoIP phone calls dips even slightly.
- **VoIP is a real-time application**. As such, it is very sensitive to latency, jitter, and packet loss. The network infrastructure is not designed to carry real-time application traffic.

VoIP still behaves like an emerging technology. Things haven’t completely settled down; standards are still being adopted and challenged; multiple vendors still sell you components that don’t play nicely together. These factors can create major application performance issues on converged networks. As a result, even a limited VoIP deployment requires ongoing, VoIP-specific monitoring, frequent call quality evaluation, trending, and troubleshooting.

In the following sections, we’ll discuss voice and video over IP in more detail and outline the UC Monitor approach to monitoring these technologies.

Unique Characteristics of VoIP Traffic

What do you need to know about VoIP traffic and VoIP behavior before it takes you, and your other network applications, by surprise?

For one thing, VoIP can be a significant consumer of bandwidth. The performance of your other applications may deteriorate once the VoIP traffic is running across the same network links because it sends data at a fixed rate, with no throttling mechanism. VoIP has a fair amount of header overhead and sends data continuously in two directions. Depending on several factors, such as the codecs you're using and the levels of phone usage, VoIP traffic can really fill up your network. Your TCP applications gracefully back down under conditions of congestion. VoIP can starve them out.

VoIP uses the Real-time Transport Protocol (RTP), which rides on top of the User Datagram Protocol (UDP). RTP applications typically send packets at a fixed rate, and because UDP is a connectionless protocol, there's no retransmission or reordering of data. That means that if a packet is dropped, it's gone, and the signal can't be retransmitted. If a whole group of packets is dropped at once, entire portions of a conversation between two IP phones can be lost.

You need to approach VoIP as an application that's highly delay-intolerant, and whose quality depends on delivery with minimal latency, jitter, and packet loss.

Video Performance on the Network

It's important to remember that *unified communications* is not interchangeable with VoIP. A VoIP-only system may be a valuable enhancement to the communications infrastructure at your enterprise, but it's not unified communications. When you add video over IP to that same system, you begin to make the key integrations and enhancements that allow the system to deliver a lot more value to users.

Although applications that use video to deliver enhanced customer support, security monitoring, or communications among end-users are becoming more and more mainstream, you still need to proceed with caution when considering a large-scale deployment. This is true for several reasons. Even more than is the case with VoIP, video requires your network to be expertly tuned, adequately or even overprovisioned, and carefully monitored.

The chief reason to delay implementation of desktop video, for example, is that it's still widely considered to be a nice-to-have, and not a critical, application. Its status means that users won't bother to use it at all if it doesn't perform well. Implementation of a video-monitoring system is tricky for the opposite reason: poor performance could compromise security, with potentiallly dire consequences.

Video conference participants at your organization are inevitably consumers of cable or satellite television at home, which means they are used to a very high-quality image and near-perfect synchronization of the audio with that image. Thus, the rule of thumb to follow with video is that if you can't deliver it with excellent performance, there's not much point in delivering it at all.

Video is also very finicky. Like VoIP, it has stringent performance requirements. Its real-time, streaming behavior resembles VoIP, but some of the same performance metrics that affect VoIP call quality have a more powerful effect on video. For example, packet loss might cause a syllable or two to drop out of a phone call, but a viewer of a video sees pixillation and probably a slow or frozen image.

Jitter on a phone call makes the audio sound scratchy or garbled, but jitter during a video conference both distorts the image and scrambles the speech. The effects are both more noticeable and more annoying.

Perhaps the most significant challenge associated with video over IP is that video applications have a much greater throughput requirement than VoIP. Video packets are large to begin with, and a key point to bear in mind is that any video conference also has an audio component. A single video stream takes anywhere from 300 to 400 kbps in each direction. Add the audio, and you've got over **800 kbps** for combined video and audio streams.

On the LAN, video may perform quite well. However, a desktop video deployment means that some vide streams will be sent point-to-point, between a pair of users, while others may be multicast—for a video conference or Webcast, for example. Any slow link or busy interface presents a potential issue for these users. One of the most common reasons to use desktop video conferencing is to enable cross-site collaboration, which usually means video calls must travel across WAN links to reach coworkers at remote offices. When they compete for bandwidth with other application traffic, these data streams can easily create bottlenecks on WAN links and WAN-LAN interfaces.

Challenges of VoIP and Video Deployments

After you have your UC system up and running, the main, ongoing challenge you face is minimizing network **delay**, the latency that is created by all your common infrastructure components: packet queues, QoS queues, firewalls, NAT, encryption, to name the most common.

Properly configured QoS policies are critical to ensure other data applications do not contend with voice-allocated bandwidth, but they can add delay. Encryption technologies can introduce more latency by ignoring priority flags (ToS) and adding additional header information—IPsec headers, for example.

Non-uniform packet delays, or **jitter**, can be more detrimental to VoIP and video call quality than latency. When it isn't uniformly affecting every voice packet in a stream, delay creates jitter, which affects call quality as the signal starts to sound or look garbled. Jitter can also cause packets to arrive out of order, which introduces additional latency at the application layer when re-assembly of the signal occurs.

VoIP-endpoint buffers, network devices that support QoS, and RTP header compression can help minimize jitter. But there's always a tradeoff. RTP header compression, for example, adds latency due to the extra processing that's required on the routers.

Packet loss can also result from excess latency or jitter. When VoIP or video packets arrive too late to be contained by a jitter buffer or are too far out of order to be properly reassembled, packet loss occurs. VoIP and video are also more sensitive to packet loss than other network applications. Loss rates greater than 3% are considered intolerable when compared to plain old telephone service (POTS) phone calls.

Finally, specialized **VoIP equipment** creates a new monitoring and maintenance challenge. For example, you need to test and monitor your call servers to make sure they are performing well and can both handle the expected volume of voice traffic and route it properly.

NetQoS 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, any application performance issues are commonly, but often incorrectly, blamed on the network; it's then up to IT to prove that some other factor is at fault. The UC Monitor product can help you determine the true source of VoIP performance degradation and avoid the costly—and often unnecessary—infrastructure upgrades that are often the "catch-all" solution to performance issues.

VoIP and Video Protocols

Some of the protocols used by VoIP and video applications have unique, real-time characteristics. These need to be monitored separately from other network traffic because of their sensitivity to delay and jitter. Other VoIP protocols are proprietary, such as Cisco SCCP. The UC Monitor product can help you track the performance of traffic using Cisco proprietary protocols, as well as some protocols only used by VoIP-enabled media devices (specialized servers or routers called voice gateways—also called VoIP or media gateways).

A VoIP phone call occurs in two distinct phases:

- **Call setup**. A call server, such as Cisco Unified Communications Manager or Microsoft Office Communications Server 2007, and an IP phone or another media-enabled device set up everything needed to make the telephone connection between the person making the call (the caller) and the person receiving the call (the called party).
- **The call, or conversation**. The audio conversation is encoded by a codec, transmitted across the network, received, and decoded at the other end. If a video component is added, the video image is similarly encoded by a specialized video codec. Cisco and Avaya IP phones typically provide codec functionality, while in the Microsoft Office Communications Server 2007 environment, supported endpoints (primarily Office Communicator instances) can exchange audio data directly. For conference calls, the codecs reside on the Microsoft A/V Conferencing Server.

Different protocols are used in each phase of a VoIP or video call. And the UC Monitor product provides different metrics and separate reports for each phase to help you narrow the source of call performance issues. In the following topics, we'll discuss these phases and protocols in more depth.

Call Setup Protocols

The call setup phase of a VoIP phone call is misnamed; it includes both call establishment and call takedown. This phase of the call requires protocols that enable dial tone, number lookup, ringing, and busy signals before the call even occurs. In addition, the call setup protocols handle things that happen after the call, such as resource cleanup and statistical reporting.

Call setup protocols use TCP or UDP to transfer data during the setup and teardown phases of a telephone call. Each protocol uses a well-known port or ports to communicate with the call server. The messages are sent back and forth between the caller, called party, and call server. For calls that travel between a VoIP network and the PSTN, the call server converses with a voice gateway or other media device using a call setup protocol appropriate for that gateway. These messages, which vary in size and number, handle functions like mapping phone numbers to IP addresses, sending dial tones and busy signals, ringing the called party, and hanging up.

Many different call setup protocols are currently in use. Some are standardized, and some are proprietary:

H.323

Standardized by the International Telecommunications Union (ITU), H.323 is widely deployed and has been in use the longest of all the call setup protocols. H.323 is actually a family of telephony-based standards for multimedia, including voice and videoconferencing and in a VoIP environment, runs on voice gateways and other media devices to connect the VoIP network to the PSTN.

H.323 is robust and flexible, but its robustness comes with a cost: it has high overhead. It requires lots of handshakes and data exchanges for each function performed. Because it uses TCP for communication, setting up a call with H.323 can require many TCP flows. Be aware of this if you are investigating network performance issues during call setup. It can also require additional configuration on the voice gateway, which maintains the information about how calls are routed.

Media Gateway Control Protocol (MGCP)

Another commonly used call setup protocol, MGCP is standardized by the IETF in RFC 3435. MGCP differs from some of the other call setup protocols in that the endpoints or phones do not use MGCP to control the phone call. Instead, MGCP is typically used to allow a call server to control a voice gateway connection to the PSTN.

MGCP sends messages between the gateway and call server over UDP Port 2427. Because the call server is controlling the gateway, most of the call control intelligence resides in the call server. Unlike H.323-enabled devices, with MGCP, the call routing information is configured in the call server instead of in the gateway.

Session Initiation Protocol (SIP)

A lightweight protocol developed by the IETF in RFC 3261, SIP represents typical data-networking logic, which asks, Why use a heavyweight protocol (such as H.323) when a slimmed-down protocol that uses fewer flows will get the job done most of the time?

Although SIP can be carried over TCP or UDP, most implementations use TCP and Port 5060. SIP messages are similar to HTTP in that they are text-based and generally follow a request-response structure. In a Microsoft environment, SIP is used for call signaling, video setup, presence, and instant messaging (IM). Avaya uses it to enable interoperability with phones from other vendors or from the PSTN. Non-Avaya phones can register as SIP endpoints with the Avaya SIP Enablement Services server.

Proprietary Call Setup Protocols

Some VoIP equipment vendors have provided their own protocols to set up and take down VoIP calls. One example is SCCP (Skinny Client Control Protocol). “Skinny” provides a simple, lightweight call setup protocol for Cisco devices. It passes messages using TCP and Port 2000.

Although multiple protocols are currently in use for VoIP call setup and takedown, the industry trend is toward the adoption of SIP. Vendors such as Cisco and Avaya are providing SIP phone/endpoint support in their call servers and media devices, and the new Microsoft Office Communication Server uses SIP to enable unified communications and integrate with Windows.

VoIP Conversation Protocols

The conversation portion of the call needs to be converted from analog to digital, translated into packets, sent across the network in packet format, reassembled, and converted from digital back to analog. A number of different standards and protocols are currently used to enable the VoIP traffic to travel across the data network. However, in most cases the Real-time Transport Protocol (RTP) is used to transfer audio and/or video data between endpoints.

Typically, the call server sets up the call, enables the endpoints to locate each other, and informs them which codec to use. It then drops out of the picture while the endpoints communicate directly using RTP. This protocol is used in Microsoft, Cisco, and Avaya VoIP environments.

RTP, defined by the IETF in RFC 1889, was designed for applications that need real-time performance and that send data in streams with no acknowledgments. An Application-Layer protocol, RTP rides on top of UDP for transport. The header of each RTP datagram contains a timestamp, so the application receiving the datagram can reconstruct the timing of the original data. It also contains a sequence number so that the receiving side can deal with missing, duplicate, or out-of-order datagrams. These characteristics are critical to real-time, streaming communications.

Avaya phones use RTP for call audio data and a related protocol, RTCP (the Real-Time Transport Control Protocol), to communicate in-progress call quality statistics to a monitoring server. (In the case of NetQoS UC Monitor, the Collector is the monitoring server). RTCP was designed to report specifically on the statistics most critical to RTP performance, such as jitter and packet loss.

Encoding Standards

Codecs (the term is short for coder-decoder) encode and decode both ends of the conversation to allow the conversation to be sent and received across the network. They take the speech audio and transform it into a digital signal that can be sent across the network. Different codecs have different bandwidth requirements and different characteristics that can affect network performance.

Many of the commonly used codecs have been standardized by the ITU; the most popular are G.711 and G.729. In a Microsoft Office Communications Server 2007 system, two proprietary codecs (RTAudio and RTVideo) are used. They are included in the Office Communicator 2007 client software. Because these codecs use proprietary algorithms, any calls traveling between another phone system and the Microsoft system require transcoding, usually by means of a Microsoft Mediation Server and a server performing voice gateway functions, or a gateway-PBX combination.

The RTAudio and RTVideo codecs were designed to work together. They provide many features that other codecs lack. For example, they routinely attempt to detect and adjust their behavior to network conditions. When they detect a scarcity of bandwidth, these codecs automatically throttle the video stream so that maximum audio quality can be maintained. They can also operate in two distinct modes: wideband and narrowband. And unlike other common audio codecs, the Microsoft codecs are able to adjust bit rates in real time.

Avaya phones and endpoints support several codec types, including the most commonly used codecs (such as G.729 and G.711). The codec that they use is configured at the Avaya (Aura) Communication Manager, which assigns “codec sets” per IP Network Region. This design allows the Administrator to select the codecs most appropriate for each network topology.

Some VoIP audio codecs in common use, like G.711, do not employ any compression schemes. The lack of compression can reduce packet loss, but the codec therefore requires more bandwidth. Codecs that compress the data, such as G.729, require less bandwidth, but the compression process usually causes some degradation in signal quality and adds delay.

More about RTP

A VoIP or video call, like any telephone conversation, is bi-directional, which means that two RTP streams carry the conversation—one traveling in each direction between the caller and the called party. The path that these RTP streams take through the network and the impairments encountered along the way are important factors in determining the quality of the voice conversations. We discussed some of these impairments in "Challenges of VoIP and Video Deployments" on page 14.

To understand the potential impairments to a VoIP stream and the series of configuration tradeoffs required to fine-tune voice over IP, it is helpful to understand the composition of the RTP datagrams that transport the voice datagrams. All the fields related to RTP sit inside the UDP payload. Like UDP, RTP is a connectionless protocol. The software that creates RTP datagrams is not commonly part of the TCP/IP protocol stack, so applications are written to add and recognize an additional 12-byte header in each UDP datagram. The sender fills in each header, which contains four important fields:

- **RTP Payload Type** — Specifies the codec that is used. The codec is important so that the receiver knows to apply the same codec to decode the data payload.
- **Sequence Number** — Helps the receiving side reassemble the data and detect lost, out-of-order, and duplicate datagrams.
- **Timestamp** — Helps reconstruct the timing of the original audio or video. It also helps the receiving side determine variations in datagram arrival times, known as jitter.

  The timestamp brings real value to RTP. An RTP sender puts a timestamp in each datagram it sends. The receiving side of an RTP application notes when each datagram actually arrives and compares this value to the timestamp. The time between datagram arrivals should be the same or nearly the same, with little or no variation.

  However, depending on network conditions, there could be lots of variation in datagram arrival times. The term for variations in the arrival times of datagrams from the same stream, **jitter**, refers to a signal whose condition the listener would probably describe as "garbled." Using the RTP timestamp, the receiving side can easily calculate the level of jitter in the signal.
- **Source ID** — Enables the software at the receiving side to distinguish among multiple, simultaneous, incoming streams. Each sender in a VoIP conversation generates a unique source ID and places it in the RTP header.

Bandwidth Considerations and Tradeoffs

While the RTP header is important to support the real-time nature of the protocol, the accumulation of headers can add a lot of overhead, especially considering the size of VoIP codec payloads. A typical payload size when using the G.729 codec is 20 bytes, which means that the codec produces 20-byte chunks of the VoIP call at a predetermined rate, usually every 20 milliseconds. With RTP, two-thirds of the datagram is the header, because the total header overhead consists of

```
RTP (12 bytes) + UDP (8 bytes) + IP (20 bytes) = 40 bytes
```

The actual bandwidth consumed by a VoIP call is higher than it first appears. The G.729 codec, for example, has a data payload rate of 8 kbps. Its actual bandwidth usage is higher, however. When packets are sent at 20-ms intervals, its payload size is 20 bytes per datagram. To this, add the 40 bytes of RTP header and any additional Layer 2 headers. For example, Ethernet drivers generally add 18 bytes. The **Bandwidth Required** column in the table below shows a more accurate picture of actual bandwidth usage for some common codecs on an Ethernet network.

Codec	Nominal Data Rate	Typical Speech Packet Size	Bandwidth Required
G.711u	64.0 kbps	20 ms	87.2 kbps
G.711a	64.0 kbps	20 ms	87.2 kbps
G.729	8.0 kbps	20 ms	31.2 kbps
G.723.1 MPMLQ	6.3 kbps	30 ms	21.9 kbps
G.723.1 ACELP	5.3 kbps	30 ms	20.8 kbps

Some IP phones let you set the “delay between packets” or “speech packet size” parameter, which is the rate at which the sender delivers datagrams into the network. For example, at 64 kbps, a 20-ms speech datagram size implies that the sending side creates a 160-byte datagram payload every 20 ms. A simple equation relates the codec speed, the speech packet size, and the datagram payload size:

```
Payload size (in bytes) =

Codec speed (in bits/sec) * speech packet size (ms)
-----------------------------------------------------
           8 (bits/byte) * 1000 (ms/sec)
```

In this example:

```
160 bytes = (64000 * 20)/8000
```

For a given data rate, increasing the speech packet size causes the datagram size to increase as datagrams are sent less frequently to transport the same quantity of data. A speech packet size of 30 ms at a data rate of 64 kbps would require sending 240-byte datagrams.

Why don’t codecs just increase the speech packet size to produce larger datagrams, thereby reducing the impact of header overhead? The answer is that the increased speech packet size adds delay, which has a negative effect on call quality.

VoIP Hardware

UC Monitor can help you track the status and health of your VoIP hardware components, namely call servers, IP phones, and voice gateways or other UC-enabled media devices. Knowing that these devices are available isn't enough to ensure that they are performing well.

The UC Monitor Collector monitors flows between IP phones and their Cisco Unified Communications Manager (CallManager) or Avaya Communication Manager call servers and between the phones and their voice gateway devices.

A Microsoft Front-End Server or Quality of Experience Monitoring Server, once it has been configured to communicate with the UC Monitor Web service, serves as an "OCS Collector" to monitor call quality for Microsoft voice and video. Supported Microsoft systems use Office Communications Server 2007 or 2007 R2, either alongside or in place of a traditional PBX or IP PBX. Information about pool configuration is discovered, and call server groups automatically created on the basis of pool identity and membership.

NetQoS UC Monitor can obtain quality metrics from Cisco voice gateways via SNMP polling. In a Microsoft system, several types of device or server can take on the role of the gateway and provide quality metrics.

The topics in this section discuss UC Monitor support for various types of VoIP hardware.

Cisco Unified Communications Manager

A Cisco Unified Communications Manager (CallManager) IP telephony call server is part of the Cisco Unified Communications Solution, a comprehensive approach to data and phone network convergence. This call server provides call processing in a Cisco Unified Communications system and supports add-on features such as video and mobility services. It can communicate using the H.323 multimedia interoperability protocol with H.323-enabled voice gateways and sends calls to gateways when they are destined for endpoints in the PSTN. And it can use MGCP to communicate with gateways using that call setup protocol.

The Unified Communications Manager or CallManager server collects management data to help ensure accurate call routing and good voice quality. It also offers many security and failover capabilities, including clustering, in which multiple call servers are installed and managed as a single entity.

NetQoS Unified Communications Monitor tracks and reports on several metrics that apply specifically to Cisco call server call setup performance. These metrics are discussed in "Call Setup Metrics" on page 81. The Cisco-proprietary SCCP protocol is supported, in addition to the standard call-setup protocols used by Cisco devices for call setup—SIP, MGCP, and H.323. The UC Monitor product also has a full set of customizable thresholds to track specific aspects of call server status and health. Two threshold types apply to individual call servers, while two others apply to call server clusters. See "Understanding Call Server Thresholds" on page 34 for more information.

NetQoS UC Monitor supports Cisco CallManager/Unified Communications Manager versions 4.2 through 7.0.

Avaya Communication Manager

In an Avaya UC system, the Communication Manager handles voice and video call processing and performs all the tasks that would be provided by a PBX in a legacy system, plus conferencing, network management, and support for third-party hardware. It uses SIP to provide user presence status and integration with Microsoft Exchange and Microsoft LiveMeeting.

The most recent versions of the Communication Manager are integrated into the Avaya Aura product lines, which are offered in three different packages for different types of enterprises:

- Branch Edition—Supports a small UC system suitable for distributed enterprises with limited need for worker mobility or video capabilities.
- Standard Edition—Supports a full-featured UC system suitable for either a single-site deployment or for mid- to large-sized enterprises. Includes third-party integration features, mobility and video support, messaging, and presence, and scales easily.
- Enterprise Edition—Supports a full-featured UC system suitable for widely distributed and/or larger enterprises, and includes the same features as the Standard Edition, plus additional high-availability and failover options.

For the Standard and Enterprise editions, a separate server, the Session Manager, performs session-management tasks and allows users to log in from anywhere using a single SIP ID. The session-management option is not included in the Branch Edition, which still uses SIP for call processing.

If you are using the Avaya G650 voice gateway, the UC Monitor Collector identifies any Controller-LAN boards (C-LANs) running on the device as separate call servers. Each of these boards has a dedicated IP address, which then appears in UC Monitor reports as a call server. However, the actual call server (Communication Manager) is usually installed on a separate media server. Once calls have been monitored for a few hours, check your configuration and make sure the media server where the Communication Manager is running, the gateway device itself, and any C-LANs you want to monitor as separate devices are appropriately identified on the Call Server and Voice Gateway list pages.

NetQoS UC Monitor supports Avaya Communication Manager versions 3, 4, and 5.x, and Avaya Aura Communication Manager 5.2.

Microsoft Call Servers

The physical server that handles call processing in the Microsoft Office Communications Server depends on the system configuration:

- **Standard Edition Server**—The Front-End server with the “Standard Edition” server role has an expanded set of capabilities, handling call processing and also providing user contact and presence information.
- **Enterprise Edition Pool**—The functions performed by the Standard Edition Server are divided up and performed by multiple physical servers, which are organized in “pools.” The servers in the Front-End pool handle call processing.

As the main call-processing server, the Front-End server acts in a role somewhat analogous to the Cisco Unified Communications Manager, which is monitored as a “call server” in UC Monitor reports. However, when Office Communications Server 2007 is monitored, the server that actually sends the call quality (QoE) report for a particular call is featured in UC Monitor reports as a call server.

Therefore if you are monitoring Microsoft Office Communications Server 2007, you might see the QoE Monitoring Server being treated as a “call server.” But if you are running Office Communications Server 2007 R2, the Front-End Servers are treated as call servers.

Servers that belong to Enterprise Edition pools are treated slightly differently. The call server is often identified with the pool name in reports. Call server groups, which are useful for identifying Unified Communications Manager clusters in Cisco deployments, are created automatically when server pools are detected in Microsoft environments. Unlike the call server groups containing Cisco call servers, the automatically created call server groups cannot be edited, nor can they be used for Phone Status Change Incident reporting, which applies to Cisco only.

Voice Gateways

Voice or VoIP gateway devices (also called media gateways) come in many varieties. The key consideration in determining whether NetQoS UC Monitor can monitor the traffic from a given gateway device is whether it handles call routing from the PSTN. Such a gateway functions like an adaptor to connect a standard telephone to a data network so that a telephone user can make phone calls over the Internet.

A gateway device might perform conversions of voice data from analog to digital, and it uses protocols such as such as H.323, SIP, or MGCP to communicate directly with a VoIP call server. Voice gateways can also perform various router functions, including firewall functions.

From the perspective of the Collector, voice gateway monitoring is concerned with whether calls from the data network to the PSTN and calls from the PSTN to an endpoint on the data network are being successfully set up and taken down in a timely fashion, with acceptable call quality.

NetQoS UC Monitor can poll Cisco gateway devices for call status and call performance data, which it then uses in analyzing call performance. By default, it peforms routine traceroute testing of each new voice gateway detected from monitored call traffic. Information about voice interface utilization on each Cisco gateway is also collected. See “Gateway Voice Interfaces” below for more information.

In a Microsoft environment, gateways send call-quality data just as the IP phones and endpoints do. See “Microsoft Media Device Monitoring” on page 23 for more information.

NetQoS UC Monitor supports all Avaya voice gateways that send call-quality reports using RTCP. See “Avaya Communication Manager” on page 21 for information about how some voice gateways are identified in reports after the UC Monitor Collector has discovered them.

UC Monitor breaks calls into *call legs* because all VoIP calls involve a bi-directional data flow. A call involving a phone in the PSTN and one in the data network contains two directional legs between the IP phone and the voice gateway that sent the call to the analog phone in the PSTN.

UC Monitor can identify the location of the caller and of the called party and use that information to analyze each call leg. This information is critical in troubleshooting problems with gateway devices. For example, if users are reporting that calls from the PSTN have a problem with echo, data provided from UC Monitor Call Watch monitoring can help you tune the echo cancellation parameters on the affected voice gateway.

Microsoft Media Device Monitoring

In a Microsoft Office Communications Server 2007 deployment, several media server roles perform voice gateway functions and may be monitored as voice gateways. For example, a “hybrid” Mediation Server usually contains an interface directly to the PSTN, where other Mediation Servers are mainly transcoders between IP networks and have no communication with the PSTN.

Most media servers in a Microsoft Office Communications Server environment can be monitored for call quality statistics. However, they are treated differently than the voice gateway devices in a Cisco deployment. The Collector can query Cisco voice gateways using SNMP to get performance data about call legs that terminate at a gateway, and by default, it also performs regular traceroute testing of these devices, reporting information about network paths in the Investigations Report.

By contrast, in the Microsoft secure environment, SNMP polling of media devices cannot be performed, and traceroute requests are not allowed to reach their targets. But these devices do contribute to the call performance statistics shown in UC Monitor reports. If the Microsoft server handles calls, it reports quality statistics to the UC Monitor Management Server. Therefore, the various Microsoft devices that send quality reports are included in reports, listed in the Phone Details report, and displayed in a read-only list view in the Administration area of the UC Monitor Management Console.

We have tested with Microsoft gateway devices and Mediation Servers that use H.323, SIP, and MGCP.

Cisco Voice Gateway Support

Not all voice gateway device types are supported in this version of UC Monitor. For example, gateways that make a T1-CAS connection are not supported. NetQoS UC Monitor has been tested with Cisco gateways that use H.323, SIP, and MGCP.

In general, to achieve full support for UC Monitor features, a Cisco gateway device must allow SNMP polling.

The Cisco VG-224, a gateway device that allows analog phones to connect to an IP PBX (in this case, a Unified Communications Manager), is supported but requires configuration. Typically, the VG-224 device supports 24 analog phones, all of which are then assigned the same IP address with different port numbers. To allow for correct reporting on calls traveling through the VG-224, the UC Monitor Administrator must add it as a voice gateway definition. You should then be aware that the connected analog phones may generate additional abandoned call legs in UC Monitor reports if the handsets are not placed on hook correctly.

For a description of the types of gateway devices that are supported, with accompanying information about models that provide limited monitoring support, see the UC Monitor Release Notes.

Gateway Voice Interfaces

Information about voice interface utilization on each gateway is reported to help you understand traffic patterns and busy-hour load on these devices. Such interfaces are quite different from the typical router interfaces with which you are probably familiar. Cisco voice gateways support one or more interfaces to the PSTN. The most common interface is the digital Primary Rate Interface (PRI), which typically consists of 23 B (or voice) channels and one D (data) channel (in Europe, the typical configuration is 30 B channels plus one D channel). A T1 PRI can therefore support up to 23 concurrent calls because a dedicated channel is required for each call. PRI voice channels are sometimes grouped together as “trunks,” which may reside in a single PRI or span multiple PRIs.

Some voice gateways contain analog interfaces, such as FXO or FXS. These voice interfaces are treated similarly to PRI interfaces in UC Monitor reporting, but they usually have fewer channels.

In Cisco Unified Communications Manager, the term *trunk* is used in a proprietary manner to refer to an inter-cluster trunk (group of channels) or a call server-to-gateway trunk. Cisco uses the term *route group* to describe a mechanism to allow certain calls to be routed to the desired voice gateway interface. A route group can contain any number of gateway interfaces and can span multiple gateways.

For purposes of NetQoS UC Monitor, route groups are not distinguished as such in reports. The individual interfaces themselves, of all types, are referred to as *gateway voice interfaces*.

Note: Interface identification and per-interface statistics are not available for Avaya or Microsoft UC systems.

Voice Gateways and Call Watch Considerations

You can use the Call Watch feature to troubleshoot issues associated with your Cisco voice gateways. Enter the directory number (DN) of an IP phone that uses the gateway in question for the Call Watch definition. Reload the Collector to send it the new configuration data. Then call that phone using a mobile phone. See “Setting Up a Call Watch” on page 50 for more information.

Your network’s trunking equipment, such as a T1 or ISDN PRI, probably includes a setting that affects the way telephone DNs are used on your network. Your trunk provider can configure the number of digits in the telephone numbers of incoming calls that get passed along to your voice gateway. The term for this type of setting is *transformations*, as in “called party transformations.” Some digits, such as the area code for local calls, are removed by the trunk before they reach the gateway. The gateway is then the source of the numbers for the call server.

And each gateway itself has a similar setting. These settings affect both inbound (PSTN-to-IP network) and outbound (IP network-to-PSTN) calls. They determine the number that is shown as the **Caller ID** at the receiving end of each call made from your IP phones, and within your network, they determine how the phone is identified in CallManager data records.

If a phone is identified solely by its extension in your dial plan—as 5678, for example—it may still be identified by its full, seven-digit number (such as 5445678) at the gateway. Similarly, the phone may be identified with or without its area code (such as 9895445678).

Be aware of the transformations being applied on your network as you use UC Monitor to monitor your system. You particularly need this information when identifying phones in Incident reports and when setting up Call Watch definitions for troubleshooting.

Bi-Directional Call Monitoring

As it travels across the network, a VoIP phone call consists of two call legs:

- Calling party (sender). Call setup metrics apply to this leg.
- Called party (receiver). Call Setup metrics are not applicable to this leg of the call.

From the perspective of a UC Monitor collection device, each VoIP call leg is viewed as unidirectional and consists of an endpoint (either another IP phone or a media device) receiving an RTP packet flow from its peer. But call data reporting varies per UC vendor, and in some cases, the endpoint that placed the call is not identified.

In a Cisco or Avaya deployment, the Collector can collect call quality data passively for each call leg because each endpoint returns a packet containing quality metrics. Calls made using Cisco call servers provide information to allow the Collector to identify the party that placed the call, but Avaya calls do not identify the caller and called party until the CDR is sent at the end of the call. In a Microsoft deployment, the endpoints provide the required information to identify the caller and the called party; however, Microsoft quality metrics do not include call setup performance data.

If a VoIP phone call originates or terminates at a telephone on the PSTN, the UC Monitor system also monitors a PSTN call leg. PSTN-to-IP network calls must traverse a voice gateway device, or another media server that performs the voice gateway function.

Call quality data is still available for PSTN call legs, but the Collector cannot collect this data passively in a Cisco environment. Instead, it must query the Cisco voice gateway (normally via SNMP polling), either while the call is in progress or shortly after its completion, to gather call quality statistics. For Avaya, the gateway reports these statistics to the Collector, just as the endpoints do. In a Microsoft Office Communications Server environment, the Mediation Server handles PSTN calls to or from the Microsoft endpoints and reports quality statistics to the UC Monitor Management Server.

NetQoS UC Monitor can usually correlate call legs belonging to the same end-to-end call. Audio-only call legs are correlated by the IP address/port combination of their two associated endpoints. For a VoIP call, the two call legs are the same, but reversed. But for PSTN call legs, the voice gateway creates a Global Call Identifier, which the Collector can correlate with the ID that appears in the call setup traffic for the call leg terminating on a gateway port. Avaya call-processing hardware does not provide information about call directionality until the call has completed. And this information is not available at all in UC Monitor reports unless the Avaya Communication Manager has been configured to send CDRs to the Collector.

Call legs that include a video stream are more complicated to correlate. To the Management Console, they appear, to all intents and purposes, to be pairs of separate calls as the call is routed and translated by various media devices in the path. To handle these cases, session-level correlation is available as a filtering option in the Calls Overview Report.

It’s important to understand call leg directionality when you’re analyzing UC Monitor Call Performance reports. Those reports express call quality as the mean opinion score (MOS) value **received by each listening party** in a call. The quality scores might differ, depending on the direction in which the data is traveling. See the following topics for more information about call legs and bi-directionality:

- “Call Legs and Bi-Directional Data” on page 64
- “Call Legs and Monitoring Reports” on page 65

Common Call Leg States

The following set of call leg states has been defined for the various multimedia protocols commonly in use. Not all states may be used for tracking each VoIP protocol, and transitions between states differ by protocol and by call setup scenario. These states are defined from the point of view of the calling party:

State	Description
OnHook	The initial call state.
OffHook	The phone has just been taken off hook.
DialTone	The phone is now receiving a dial tone.
Dialing	User is now dialing or has dialed a number.
ConnReq	Call Setup protocol has initiated a connection between a pair of call leg endpoints.
Connect	Call Setup protocol has completed a call leg connection.
Negotiate	Call Setup protocol is negotiating parameters of the media transmission for the call.
Ringing	The called party’s phone is now ringing.
NoAnswer	An event indication has been seen that the call was not answered.
Answer	An event indication has been seen that the call was answered.
OnHold	The call is on hold and RTP flow is not active.
Call Flow	Bi-directional RTP flow (voice traffic) is now active between the call leg endpoints.
DiscReq	Call Setup protocol has initiated teardown of the call leg connection.
QualityStat	Call Leg disconnect complete; waiting for transmission of call leg quality statistics.
Call Leg Completion States	
Complete	Normal call completion.
Aborted	A transient network error occurred that has (perhaps temporarily) aborted the call. An aborted call may manage to recover once the error condition clears.
Errored	A permanent error that occurred has ended the call.
Lost	The Collector has lost track of the call leg and has stopped attempting to track it. The call leg has ended, but one or more packets containing information necessary to classify and correlate the call leg were not seen.

In general, call setup metrics are calculated as follows:

- **Dial Tone Delay** — The time between entering the OffHook state and entering the DialTone state.
- **Post Dial Delay** — The time between entering the ConnReq state and entering the Ringing state.

However, in some scenarios these states might not occur; in such cases, the applicable metric is either reported as unavailable, or is calculated from related states.

CHAPTER 3

Using NetQoS UC Monitor

Your role as a UC Monitor operator enables you to view reports and receive notifications when Incident reports are created. A UC Monitor Administrator should have configured the system to optimize data collection and customize Incident reporting to suit your environment. This chapter provides some background information about the custom settings that are available to the Administrator. The information in this chapter will help you interpret the Incident reports you see and understand your role in troubleshooting any problems that NetQoS UC Monitor detects.

If your NetQoS reporting system includes the NetQoS Event Manager, you can view correlated event data from UC components and other devices, applications, and networks throughout your enterprise in the NetQoS Performance Center. See Appendix C, “Viewing Events in the Event Manager” on page 169 for more information about how UC Monitor events are displayed in the Event Manager and Map.

Some users also have the ability to set up and launch a traceroute investigation or a Call Watch, two investigative features that deliver real-time data about network paths and the call performance of selected phones. Instructions for using these features are provided in this chapter and in the “UC Monitor Reports” chapter.

This chapter contains the following topics:

Getting Started Using NetQoS UC Monitor

To start using the UC Monitor Management Console, access the server that hosts the console by entering a server name or IP address into the **Address** field of your Web browser. Use the following syntax:

```
http://<IPAddress>/UCMonitor/
```

The Management Console requires Microsoft Internet Explorer version 7 or later.

You are prompted to log in when you first access the Management Console. The UC Monitor Administrator at your organization can supply your login information, as well as the UC Monitor server name or IP address.

Configuration and Customization Options

The UC Monitor Administrator can configure the UC Monitor system to suit the performance monitoring needs of your environment. To learn more, see the sections of the *UC Monitor Administrator Guide* listed in the following table.

Note: Only users with the Administrator role can complete the tasks required for the configuration and customization options listed below.

Option	Description	Section of Administrator Guide
Data collection	Set up and push configuration information to the Collector(s); edit or delete Collectors.	“Configuring Collectors”
Reporting parameters	Create Location definitions, including subnets of IP phones and key phones. Supply information about media devices and call servers for more complete reporting. Create SNMP profiles so that voice gateways can be queried for performance data.	“Adding Locations” “Configuring Media Devices” “Working with Call Servers and Groups” “Working with SNMP Profiles”
Thresholds	Change the default thresholds to make UC Monitor more or less responsive to changes in performance.	“Understanding Performance Thresholds” “Understanding Call Server Thresholds”
Incident responses	Set up automatic responses to Incidents, including notifications and actions.	“Understanding Incidents and Incident Responses”
UC Monitor security settings	Determine which users can perform certain functions and view certain report pages.	“Working with Users and Roles”
Console settings	Update Management Console settings, including Console name and IP address.	“Management Console Settings”
Emailed reports	Edit the schedules for emailed reports.	“Scheduled Email Report Delivery”

Option	Description	Section of Administrator Guide
Database	• Perform database maintenance. • Monitor disk and database size and growth rate. • Purge data from the database.	"Changing Database Settings"

Using the UC Monitor System

No matter how well your network is performing today, tomorrow could be a whole different story. Use NetQoS UC Monitor to track VoIP and video performance and call-quality statistics daily and even hourly to make sure users can always initiate and complete calls with good quality. The UC Monitor system was designed with ongoing quality monitoring in mind and provides several features to help you keep tabs on your system:

- Performance thresholds, to continually track call setup and call quality performance
- Call server thresholds, to make sure you're alerted when phones fail to register successfully
- Call server group thresholds, to provide notifications when phones fail over to another call server or go missing
- Alerting mechanisms to let you know when performance falls below a threshold
- Automatic Incident response actions that can be initiated when a threshold is violated

The following sections in this chapter provide more information about each of these monitoring features.

UNDERSTANDING PERFORMANCETHRESHOLDS

For most metrics, UC Monitor provides a set of default **performance thresholds** that establish a foundation for VoIP performance monitoring and reporting. Performance thresholds define the boundaries of acceptable performance behavior. Thresholds are discussed in detail in the *UC Monitor Administrator Guide*.

Only a user with the Administrator role can change the default performance threshold settings. To ensure that a particular threshold does not create unnecessary Incidents each time it's crossed, an Administrator can edit thresholds specific to each Location, or even for pairs of Locations or voice gateways. The *Administrator Guide* contains instructions for changing them.

An Administrator has several options for customizing thresholds. He or she can assign different threshold settings to:

- each Location
- pairs of Locations, or pairs of voice gateways
- pairs of Locations and gateways

A recommended best practice is to enable call quality monitoring by codec. By default, codec thresholds apply codec-appropriate values for MOS and Network MOS as traffic using various standard codecs is detected. These values can be changed, however.

If a particular Location is known to have slightly higher network latency than the rest of the system, the Administrator may choose to set different thresholds for that Location to make sure network operators don't receive Incident notifications about known performance conditions.

The UC Monitor software uses performance thresholds to determine when Incidents are created and to rate collected data. For example, a call quality latency threshold of 150 milliseconds indicates a Degraded condition. If latency data crosses that threshold, UC Monitor rates the data as Degraded and displays it in yellow in the call quality bar charts in reports. Similarly, a measurement of 400-millisecond latency indicates an Excessive condition, displayed in orange in reports.

UC Monitor Performance Threshold Settings

UC Monitor default thresholds were selected according to well-defined industry standards for acceptable VoIP and video performance from the perspective of network users. UC Monitor offers two different sets of performance thresholds:

- **Call Setup thresholds** — Trigger Incidents in response to poor call setup performance metrics, such as an excessive delay to dial tone.
- **Call Quality thresholds** — Trigger Incidents in response to poor call quality performance metrics, such as low MOS values.

For any given metric that is monitored by UC Monitor, two thresholds are available:

- Degraded threshold— Indicates a decline in performance
- Excessive threshold— Indicates a severe decline in performance

The following table describes the UC Monitor **Call Setup** performance thresholds and their default settings:

Metric	Description	Threshold Defaults	Minimum Observations
Delay to Dial Tone	Time elapsed from when a user enters the last digit of a telephone number to when the user hears a ring or busy signal.	2000 ms (Degraded) 4000 ms (Excessive)	5 calls originated
Post-Dial Delay	Time elapsed between a user's punching in the last digit of a telephone number and receiving a ring or busy signal.	2000 ms (Degraded) 4000 ms (Excessive)	5 calls originated
Call Setup Failures	The rate at which calls are failing during the call setup phase.	2% (Degraded) 10% (Excessive)	5 calls originated

The following table describes the UC Monitor **Call Quality** performance thresholds and their default settings:

Metric	Description	Default Thresholds	Minimum Observations
Audio Metrics			
MOS	Mean Opinion Score: an industry standard for gauging call quality by estimating the impact of various impairments on the listener's likely perception of the call quality. Theoretically, highest score is 5.0. In practice, highest score is probably 4.5.	Codec. See the Notes below.	15 call minutes
Network MOS	Predictive MOS listening quality metrics based on network factors alone.	Codec. See the Notes below.	15 call minutes
Packet Loss	The rate at which VoIP packets are being lost—sent, but never received.	1% (Degraded) 5% (Excessive)	15 call minutes
Jitter Buffer Loss	The rate at which packets are being lost due to jitter buffer overruns.	1% (Degraded) 5% (Excessive)	15 call minutes
Latency	Delay, or the time taken for a VoIP packet to travel between the calling parties. Measured from end to end in a single direction.	150 ms 400 ms	15 call minutes
ACOM (ERL/ ERLE)	Sum of Echo Return Loss (ERL—echo reduction from the network without echo cancelling devices), echo reduction due to echo cancelling devices (ERLE, or Echo Return Loss Enhancement), and nonlinear processing loss for the call. The total reduction in echo seen by the network. This metric only applies to voice gateway devices.	15 decibels (dB) 6 decibels (dB)	15 call minutes
Video Metrics			
Video Latency	Delay, or the maximum time taken for a video packet to travel between the calling parties, measured from end to end in a single direction. Calculated by taking the average round-trip time for a call leg in a given video call and dividing it in half.	150 ms 400 ms	15 call minutes
Video Packet Loss	Average network packet loss for the entire stream.	1% (Degraded) 5% (Excessive)	15 call minutes

Metric	Description	Default Thresholds	Minimum Observations
Video Frame Loss	Average number of unique consecutive images, or video frames, lost due to corruption and error concealment for the entire stream. Video frames can span multiple packets, so this threshold is useful in conjunction with the video packet loss threshold.	1% (Degraded) 5% (Excessive)	15 call minutes
Frozen Video	The frequency of long and noticeable frozen video for the whole session.	1% (Degraded) 5% (Excessive)	15 call minutes

Notes

For the **MOS** and **Network MOS** audio metrics, the Administrator has two options for setting the Degraded and Excessive thresholds:

- Select **MOS** and supply a fixed MOS value.

  Defaults are: Degraded — 4.03; Excessive — 3.6.
- Select **Codec** to instruct NetQoS UC Monitor to use the codec threshold that applies to the codec being used for monitored calls.

More information about the two MOS metrics and what they measure is provided in Appendix A, "Calculating a Mean Opinion Score" on page 147.

The **Minimum Call Minutes** parameter lets you set a minimum number of observations—times that the monitored metrics can cross the performance threshold before an Incident is created. See "Observations in Call Performance Reports" for more information.

Threshold values are not treated as inclusive, which means that they must be actually crossed, not met, for an Incident to be created. For example, for phones using the default threshold settings, 4.03 is the lowest possible MOS value that can be rated as normal performance.

Understanding Call Server Thresholds

In a UC system, call server performance and status have a powerful impact on the user's quality of experience when making or receiving calls. IP phones and voice gateway devices must register with a call server and send it periodic keepalive messages to inform the rest of the system of their status. The call server handles all aspects of call setup, including sending dial tones and ringing or busy signals, routing calls, and cleaning up resources after a call has been completed.

To help you track call server and phone status, two types of call server thresholds are available in NetQoS UC Monitor:

- Call server thresholds: See "Call Server Threshold Settings" on page 35
- Call server group thresholds: See "Call Server Group Threshold Settings" on page 37

Important: The call server thresholds are designed for monitoring in Cisco environments. They cannot be applied to Avaya or Microsoft components.

While the call server thresholds must be applied to *individual* servers, the call server group thresholds must be applied to call server *groups* that you create to represent your server clusters. The two different threshold types provide more accurate Incident reporting when applied this way.

Each call server in a cluster is capable of playing several different roles to provide failover safeguards and load balancing. For example, in a Cisco Unified Communications Manager cluster, any server in the cluster can take on the call-processing role if the primary call server for a particular set of phones is taken offline for maintenance or becomes unavailable for another reason. The call server group thresholds could potentially apply to any call server in a cluster because they relate to this type of shared or redundant functionality.

See the following topics for more information about how call server Incidents are reported:

- "Incident Overview Report" on page 83
- "Call Server Incident Details" on page 86

Call Server Threshold Settings

Unlike the call server group thresholds, which are applied to call server clusters, the call server thresholds can only be applied to individual call servers.

The following table describes the call server group thresholds:

Metric	Description	Default Values
Registration Failures	Creates an Incident if the number of devices that are trying unsuccessfully to register with a call server exceeds the threshold. This Incident can indicate a configuration or security problem.	**15** failures per reporting interval Select **None** to disable this threshold. Severity is always Excessive.
Poor Call Quality QRT	Creates an Incident every time an IP phone user clicks the **QRT** soft key to report poor call quality. The QRT soft key activates the Cisco Quality Report Tool, an optional feature that the VoIP administrator can enable. See "More about the Poor Call Quality (QRT) Threshold" on page 36.	**Enabled** Severity is always Excessive.

Both of these thresholds are designed to create Call Server Incidents based on the information being reported in the the Phone Details Reports. For example, if a Registration Failures Incident is reported, multiple phones in the Phones List will have a status of **Registration Failed**.

More about the Registration Failures Threshold

The Registration Failures call server threshold was designed to notify an administrator if one or more devices are repeatedly, but unsuccessfully, trying to register with a call server. Excessive phone or voice gateway registration failures can indicate a configuration problem, a call server issue, or a network issue, such as a connectivity outage.

In some cases, excessive registration failures can also indicate a security problem that can impede server performance; if a phone or gateway is trying to register from an unauthorized address, the call server will try to resolve the address but will ultimately deny the registration request. Because the call server has to respond to every device registration request, excessive device registrations use up bandwidth and can tie up the call server as it attempts to resolve device addresses and process requests.

If you see a Registration Failures Incident report, check call setup performance statistics in the Performance Overview Report to see whether problems associated with an overburdened call server have caused other issues. Then check the Phones Report (a link in the **Related Reports** section on the Incident Details report page) to see whether the registration requests are coming from an unauthorized IP address.

More about the Poor Call Quality (QRT) Threshold

The Poor Call Quality (QRT) call server threshold is based on a feature of some Cisco IP phone models. The Quality Report Tool, or QRT, feature allows phone users to press a **QRT** softkey to report poor call quality. When the key is pressed, the Quality Report Tool collects information useful for troubleshooting the poor performance, such as jitter and packet counts, from various sources, formats the information in an IP Phone Problem report, and send it to its call server. The call server places the information in a CDR and also retains the report, which can be viewed using the QRT Viewer utility.

To enable this reporting feature, a Cisco Unified Communications administrator must define a softkey that an end-user can press to report a poor-quality call. The QRT softkey can be enabled for use while a call is in progress, after a call has completed, or both.

The UC Monitor Collector can detect whether the QRT softkey message has been sent. If this threshold is enabled, the Collector automatically generates an Incident when it detects a QRT event.

This feature is supported by phones using the SCCP and SIP protocols. If enabled, the threshold applies to individual call servers, not to call server groups or Locations.

When a Poor Call Quality call server Incident is reported, a Phone Details Report is available as a **Related Reports** link from the UC Monitor Call Server Incident Details report page. The Phone Details related report shows call legs for the 15 minutes just before the time the QRT key was pressed and provides information needed to identify the phone where it was pressed.

If the user presses the softkey while the call is still in progress, NetQoS UC Monitor initiates an automatic Call Watch for the phone where the key was pressed. Data views from the Call Watch Details Report are then included in the Incident Details Report.

Note: This Incident type is distinct from a call quality performance Incident in the sense that the call quality performance Incident is created in response to VoIP or video performance metrics that cross a threshold. By contrast, the Poor Call Quality call server Incident is triggered when a phone user presses a softkey. It's therefore possible that a user error is involved, and no actual performance issue exists.

Call Server Group Threshold Settings

Unlike the call server thresholds described in "Call Server Threshold Settings" on page 35, the call server group thresholds are designed to be applied to your call server clusters, or to other logical groupings of call servers. Each call server in a cluster is capable of playing several different roles to provide failover safeguards and load balancing. For example, in a Cisco Unified Communications Manager cluster, any server in the cluster can take on the call-processing role if the primary call server for a particular set of phones is taken offline for maintenance. The call server group thresholds could potentially apply to any call server in a cluster because they relate to this type of shared or redundant functionality.

The following table describes the events that could trigger a Phone Status Changes call server group Incident. The total number of all phone status changes for the group is used to trigger the Incident:

Status Changes	Description
Currently Missing Phones	The percentage of devices previously registered to this call server group that are no longer registered to (sending keepalive messages to) any of the call servers in the cluster. The missing phones total does not include any phones that had normal shutdowns (and accompanying deregistrations).
Recently Moved Phones	The percentage of devices previously registered to a call server in this call server group, but that are currently registered to a different call server in the same group.
New/Found Phones	The percentage of devices that are registered to this call server group, but that were not registered during the previous reporting interval (15 minutes ago). • A "new" phone has never registered to this call server group since monitoring with NetQoS UC Monitor began. • A "found" phone has lost contact with this call server group at some point in the past, but in the last reporting interval, it registered again with the same group.

As shown in the table, different types of status change can trigger the Phone Status Changes Incident as long as the threshold value is exceeded. The default value is **50%**, which refers to a percentage of all devices that are members of this call server group and that had status changes during the 15-minute reporting interval. A "member" of a call server group (commonly a cluster) is identified in a list that is maintained by a call server and shared among the servers in a cluster.

The total percentage of phones with applicable changes must exceed, and not meet, the threshold to trigger the Incident. A single Phone Status Changes Incident is then included in the summary list of Call Server Incidents; separate data views provide information about each type of status change when you drill down into the detailed Incident report. See "Phone Status Changes Incident Details" on page 88 for more information.

The Incident is not dependent on the similar information being reported in the Phones Report. For example, if a Currently Missing Phones status change is reported, multiple phones in the Phones List might show a status of **Unavailable** or **Lost Contact**, but keep in mind that the status of a device being reported at a given moment is actually the device status *at the end* of the reporting interval. When a change in phone status occurs, the Incident might be created before another status change occurs; the later status would then be reflected in the Phones Report and would be slightly out of synch with the Incident. It's a good idea to check the Phone Details Report, which includes each phone's **Previous Status**.

More about the Phone Status Changes Incident

The Phone Status Changes Incident was designed to detect failover events and branch office outages. It can also assist in improving the ability to identify call server performance issues and branch office connectivity failures that can be costly. Typically, the Incident itself provides enough information to help you identify the affected phones and call server group. However, planning Location definitions carefully makes it easier to identify the phones involved in the Incident.

In the most common scenarios, the Phone Status Changes Incident is used to report a bank of phones that have failed over to another call server, or that have gone missing from the network due to an outage. Often, call servers are shared among several remote sites, with banks of phones that may be in widely different geographical regions or that are using topologically distinct networks. Therefore, you need to be able to easily distinguish phones in branch offices that access call servers over a WAN link from other phones using a local cluster when a call server group Incident is reported.

As a best practice, the Administrator should place remote phones in a separate Location from phones local to the call server cluster. Then if the branch office phones undergo an outage or failover, the Incident notification will provide the Location name of the branch office, and the tables of information in the Incident report itself will also direct UC Monitor operators more quickly toward the phones and other equipment that need to be investigated.

The data views in the Phone Status Changes Incident Details can be sorted by Location to further reduce troubleshooting time. Click the column header to sort by Location. We also recommend that the Administrator configure a traceroute investigation to run automatically in response to this Incident. Check the **Related Reports** links for the Investigations Report.

Understanding Codec Thresholds

Codec-based thresholds supplement call quality performance thresholds to help you better understand and manage call quality. A basic component of any VoIP or video over IP component that includes a microphone, the codec encodes and decodes the audio from both ends of a telephone conversation, producing packets that can be sent and received across the network. Codec performance has a noticeable effect on VoIP and video performance.

A wide range of codecs are available to optimize VoIP or video performance, each with an accompanying set of drawbacks and benefits. In addition to the different bandwidth requirements associated with different codec types, codecs have other characteristics that can affect network performance. For example, some of the high-performance codecs do not compress the data they send and as a result, they use more bandwidth than codecs that use a compression scheme. Compression often degrades the audio signal and adds delay. See "Encoding Standards" on page 17 for more information.

For the most part, codecs are commonly understood to provide a certain level of audio quality, which is expressed as a theoretical maximum Mean Opinion Score (MOS). The newer codecs from Microsoft are unique, however, in receiving ratings for two types of theoretical maximum MOS, as well as in advertising different performance expectations in wideband and narrowband environments.

The UC Monitor codec thresholds feature adds flexibility and accuracy to two of the call quality performance thresholds, **MOS** and **Network MOS**. The ability to use a codec threshold allows the Administrator to set these thresholds either relative to codec performance or relative to absolute MOS value.

More about Codec Thresholds

To help you set accurate performance thresholds for your network and equipment, a substantial number of codec threshold settings have been pre-defined by NetQoS for the most common codecs. These values can also be modified by an Administrator to suit specific monitoring needs. They are documented in the online Help.

The Administrator can add new codec threshold settings based on a list of supported codecs. The settings consist of Degraded and Excessive values for each of two MOS metrics.

Pre-defined threshold settings are available for most popular codecs, but no “default” codec threshold is defined. Therefore, if codec thresholds are enabled, NetQoS UC Monitor applies the threshold settings associated with any codecs it detects during monitoring. The codec thresholds that may be applied include any pre-defined or custom thresholds that use the codec(s) that have been detected from monitored call traffic.

If a codec that is not in the list of pre-defined or custom codec threshold settings is detected, the associated MOS value is displayed as **Unrated** in reports.

Codec thresholds can be added, edited, deleted, or disabled by the UC Monitor Administrator.

Note: The proprietary Microsoft codecs, RTAudio and Siren, are the only codecs that offer a threshold for Network MOS, a metric that is only available from Microsoft VoIP and video endpoints in the Office Communications Server 2007 environment. Be aware that the MOS scale used in the Microsoft codec implementations is different from that used by other supported codecs. For example, the MOS value used for the default Degraded threshold for the RTAudio NB codec, 3.48, does not represent exactly equivalent performance to the same value if reported for the G.729 codec. See Appendix A, “Calculating a Mean Opinion Score” on page 147 for more information about the MOS and Network MOS calculations.

Understanding Incidents and Incident Responses

An Incident is a record of information that UC Monitor creates when a performance threshold is crossed. Thresholds are boundaries of acceptable performance behavior, and exist by default for each monitored call performance metric. Administrators can change thresholds to make them more or less sensitive to performance changes.

When thresholds are crossed, the UC Monitor software creates Incident reports with assigned sequential numbers, reports them on the Incident Overview Report page, and launches any associated responses. An Administrator can configure Incident responses for each type of Incident:

- Call setup Incidents
- Call quality Incidents
- Call server and call server group Incidents

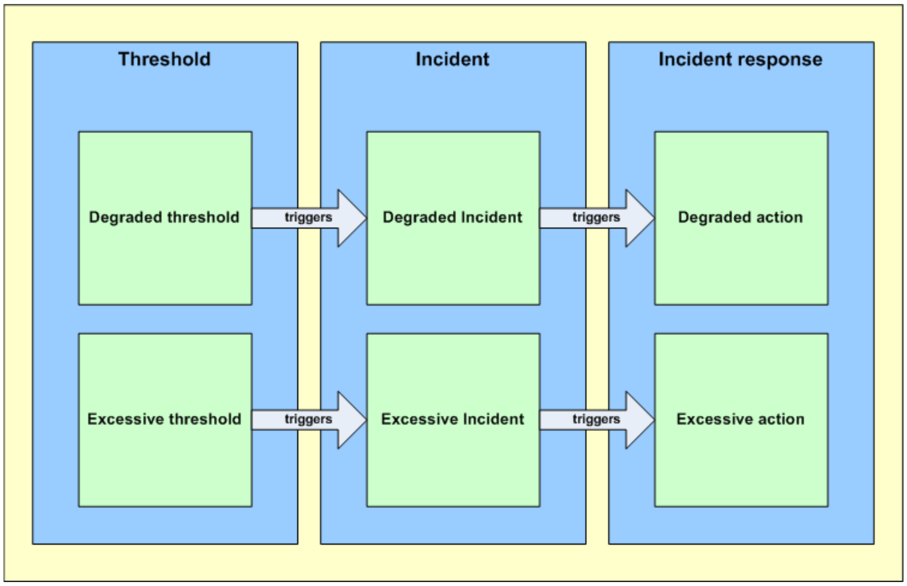
Collector Incidents are also applicable to UC Monitor Collector performance and are reported separately. The *Administrator Guide* contains more information about the Collector thresholds that trigger these Incidents. See "Collector Incidents" on page 96 for a description of the Collector Incident report.

By default, Incident responses do not launch any actions. A UC Monitor Administrator can set up actions and notifications to occur in response to a threshold violation. For a given Incident response, an Administrator can specify:

- An action or notification to occur when performance meets or exceeds the Degraded threshold
- An action or notification to occur when performance meets or exceeds the Excessive threshold

How Incidents Trigger Responses

UC Monitor creates an Incident anytime it detects a performance condition on the network that exceeds a threshold. If an action has been 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:

- The UC Monitor system creates an Incident the first time a threshold is crossed.
- Even if the threshold metric remains in violation of the threshold, a new Incident is not opened until the first one is automatically closed according to the rules of Incident closure. See "How Incidents Are Closed" on page 42 for more information.
- To trigger an Incident response, a violation must exceed minimum severity and duration criteria—either a minimum number of calls, or a minimum number of call minutes.
- A UC Monitor Administrator associates an Incident response with the Incident type (either call setup or call quality) while setting up thresholds. The threshold configuration page includes an option to select an Incident response.
- For a few types of Incidents, such as the Collector Abnormal Termination Incident, no applicable metrics can be monitored for improvement so that the Incident can be closed. Therefore, the Incident is briefly opened to trigger any automatic actions (such as creating a crash dump file), but it is immediately closed by the UC Monitor system. Any accompanying email or SNMP trap notification might indicate that the Incident is open, but in fact closure is pending.
- The traceroute investigation action is usually configured as an Incident response action for call setup or call server group Incidents only.

  If the Administrator assigns the Launch Traceroute Investigation action to other types of Incidents, such as call quality, the results are not very helpful, or the traceroute might not actually run at all. Traceroutes are run from the Collector, which is located so close to the call servers that little can be determined from the reported route taken by call traffic.

  For call server group Incidents, the Collector attempts to run a traceroute to the key phone at the affected Location, if a key phone has been defined.

  A traceroute investigation can also be launched independently of an Incident. See "Launching a Traceroute Investigation" on page 106 for more information about on-demand traceroute investigations.

How Incidents Are Closed

An Incident stays open until it is automatically closed. If the severity of the performance condition changes, but the metrics still violate either the Degraded or Excessive threshold, the Incident is updated to reflect the change in severity, but it is not closed.

Incidents are closed when:

- One full hour of clock time (measured from the top of one hour to the top of the next hour) has elapsed since the threshold violation occurred, and the violation has not been repeated.
- The performance condition that triggered the Incident has persisted for 24 hours. A new Incident is then opened.

Incident types (call setup or call quality) can change. A call quality threshold violation overrides a call setup violation if they affect the same pair of Locations or voice gateways. An Incident remains open for that pair, but the type of Incident changes to call quality if a call quality threshold violation has been detected.

Other Incident types do not have an applicable state. These are considered "closed" by default. For example, the abnormal termination Collector Incident type is never in an "open" state.

It's possible for a UC Monitor operator to 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 Excessive status while still appearing as acknowledged (indicated with gray shading in Incident reports). As a best practice, be careful only to acknowledge Incidents that you have taken steps to address.

When the NetQoS Event Manager is also running in your environment, NetQoS Performance Center operators might try to close UC Monitor events. Events from some NetQoS data sources can be closed manually. However, a NetQoS Performance Center operator's act of closing a UC Monitor event does not close the actual *Incident* that sent the event to the Event Manager. Such an Incident will have an Acknowledged status in the UC Monitor interface while appearing to have a Closed status in the Event Manager.

UC Monitor offers the following Incident responses:

Type of Incident	Actions Available	Description
Call Performance: Call Setup	Send Email	Notification: Send an email message to selected user(s).
	Send SNMP Trap	Notification: Send an SNMP trap to selected computer(s).
	Launch Traceroute Investigation	Action: Run a traceroute to the affected Location or gateway and report the results
Call Performance: Call Quality	Send Email	Notification: Send an email message to selected user(s).
	Send SNMP Trap	Notification: Send an SNMP trap to selected computer(s).
Call Server or Call Server Group	Send Email	Notification: Send an email message to selected user(s).

Type of Incident	Actions Available	Description
	Send SNMP Trap	Notification: Send an SNMP trap to selected computer(s).
Call Server Group	Launch Traceroute Investigation	Action: Run a traceroute to any key phones that have been defined at affected Locations. See the **Note**, below, for more information.
Collector	Send Email	Notification: Send an email message to selected user(s).
	Send SNMP Trap	Notification: Send an SNMP trap to selected computer(s).

Note: If the Administrator has set up a Launch Traceroute Investigation Incident response action for the Phone Status Changes Incident, the traceroute is only sent to key phones. Thus, if the percentage of phone status changes at a particular call server group crosses the threshold, the traceroute is only launched if key phones have been defined at any of the Locations whose phones had applicable status changes.

One other Incident response action is static. The Launch Call Watch Investigation action occurs automatically in response to a Poor Call Quality (QRT) call server Incident. This action cannot be disabled.

The following topics discuss Incident response actions and how to react to them.

Working with Incidents

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 help you troubleshoot a problem at the time that it occurs, reducing the mean time to repair (MTTR).

An email message you receive in response to a call setup or call quality Incident contains, in addition to a notification that a threshold has been crossed, 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 being reported in a given Incident response email message, one or more links to associated UC Monitor reports may be included.

Whenever you receive an email notification or SNMP trap in response to an Incident, you should take several steps, as appropriate, to troubleshoot the poor performance.

To respond to an Incident notification:

1. Click any hyperlinks provided in the notification to view the relevant Incident report.
2. Drill down, where appropriate, to find out more information about the Incident. For example, you'll want to find out exactly which VoIP components, such as call servers, were involved and their status. And you'll want to know which Locations or individual phones were affected.
3. Click the **Related Reports** link to any associated investigation report. Scan the Traceroute Investigation Details to see whether the path taken by the call setup traffic resembles the one shown in the Baseline Traceroute Details table.
4. If no investigation was launched automatically, launch one manually to find out more information about the route being taken between the affected phone and its call server or voice gateway. See "Launching a Traceroute Investigation" on page 106 for more information.
5. Initiate a Call Watch for the affected phones. For more information on setting up a Call Watch, see "Using the Call Watch Feature" on page 48.

If your system includes the NetQoS Performance Center and the NetQoS Event Manager, you should check the Event Source chart and table to see whether any infrastructure devices are showing open events. This information helps you isolate the UC performance problem to its root cause.

When you have found the source of the problem, you should acknowledge the Incident to reduce its priority and let other operators know that the issue is being worked on or has been resolved. For more information, see "Acknowledging Incidents" on page 46.

Viewing Incidents

Whenever call setup or call quality performance metrics exceed a threshold, UC Monitor creates and displays a list of sequentially numbered Incidents on the Incident Overview Report page. On this page, you can click the link associated with any Incident to view the full Incident report.

Incident reports show details of the related performance degradation. They have a maximum time window of 24 hours. You can select a time frame to include the time of interest and view Incidents that were active during that time frame.

Incidents open and close in conformity to a set of Incident creation rules. See "How Incidents Trigger Responses" on page 40 for a full discussion.

Historical Incident records are stored as long as interval data is stored. A UC Monitor Administrator can configure the retention period on the Database Administration page.

If your monitoring system includes the NetQoS Performance Center and the NetQoS Event Manager, you can see UC Monitor Incidents reported as events in the Event List. Correlated event data from multiple NetQoS data sources helps you isolate the UC performance problem to its root cause. See Appendix C, "Viewing Events in the Event Manager" on page 169 for a full discussion of UC Monitor integration with the Event Manager.

See "Incident Overview Report" on page 83 for more information about Incident reports.

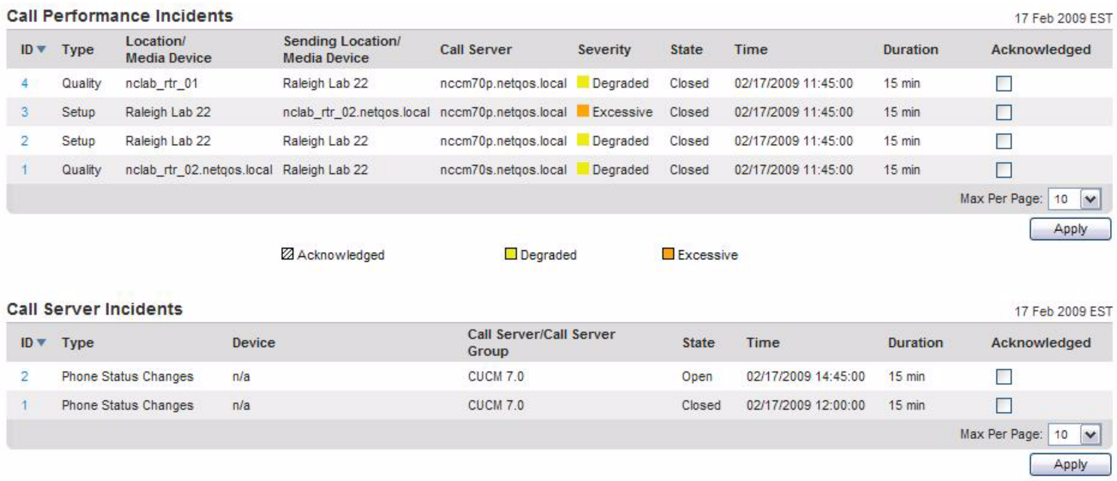
Viewing Incident Details

From the list of Incidents in the Incident Overview Report, you can drill into a specific Incident to see details for it. The drilldown view is called the Incident Details page.

To view details about an Incident:

1. Access the Incident Overview Report page by clicking any hyperlinks provided in the notification. Or click **Monitoring > Incidents** in the navigation links.

   The Incidents report page is displayed:



Call Performance Incidents — 17 Feb 2009 EST

ID ▼	Type	Location/ Media Device	Sending Location/ Media Device	Call Server	Severity	State	Time	Duration	Acknowledged
4	Quality	nclab_rtr_01	Raleigh Lab 22	nccm70p.netqos.local	🟨 Degraded	Closed	02/17/2009 11:45:00	15 min	☐
3	Setup	Raleigh Lab 22	nclab_rtr_02.netqos.local	nccm70p.netqos.local	🟧 Excessive	Closed	02/17/2009 11:45:00	15 min	☐
2	Setup	Raleigh Lab 22	Raleigh Lab 22	nccm70p.netqos.local	🟨 Degraded	Closed	02/17/2009 11:45:00	15 min	☐
1	Quality	nclab_rtr_02.netqos.local	Raleigh Lab 22	nccm70s.netqos.local	🟨 Degraded	Closed	02/17/2009 11:45:00	15 min	☐

Max Per Page: 10

Apply

▨ Acknowledged 🟨 Degraded 🟧 Excessive

Call Server Incidents — 17 Feb 2009 EST

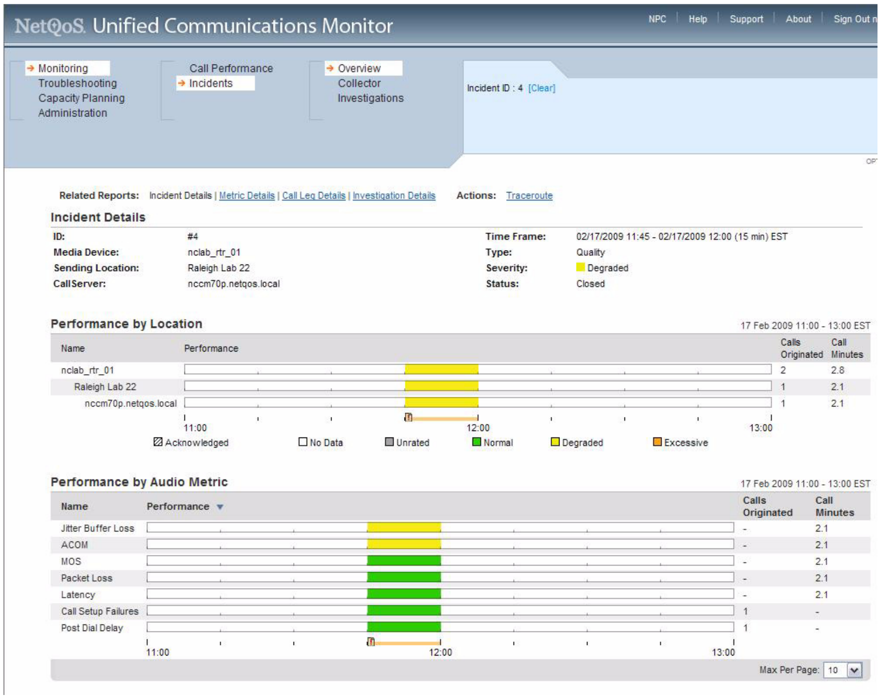
ID ▼	Type	Device	Call Server/Call Server Group	State	Time	Duration	Acknowledged
2	Phone Status Changes	n/a	CUCM 7.0	Open	02/17/2009 14:45:00	15 min	☐
1	Phone Status Changes	n/a	CUCM 7.0	Closed	02/17/2009 12:00:00	15 min	☐

Max Per Page: 10

Apply

2. Click the link for the Incident ID number whose details you want to view.

   The Incident Details page is displayed:



Incident ID : 4 [Clear]

Related Reports: Incident Details | Metric Details | Call Leg Details | Investigation Details Actions: Traceroute

Incident Details

ID:	#4	Time Frame:	02/17/2009 11:45 - 02/17/2009 12:00 (15 min) EST
Media Device:	nclab_rtr_01	Type:	Quality
Sending Location:	Raleigh Lab 22	Severity:	🟨 Degraded
CallServer:	nccm70p.netqos.local	Status:	Closed

Performance by Location — 17 Feb 2009 11:00 - 13:00 EST

Name	Performance	Calls Originated	Call Minutes
nclab_rtr_01		2	2.8
Raleigh Lab 22		1	2.1
nccm70p.netqos.local		1	2.1

▨ Acknowledged ☐ No Data ■ Unrated 🟩 Normal 🟨 Degraded 🟧 Excessive

Performance by Audio Metric — 17 Feb 2009 11:00 - 13:00 EST

Name	Performance ▼	Calls Originated	Call Minutes
Jitter Buffer Loss		-	2.1
ACOM		-	2.1
MOS		-	2.1
Packet Loss		-	2.1
Latency		-	2.1
Call Setup Failures		1	-
Post Dial Delay		1	-

Max Per Page: 10

The information included in the detailed report is already narrowed to show the affected Location or pair of Locations and a media device or call server. An alarm icon indicates the time period when the Incident was reported.

The following topics provide information about the fields you see in the Incident Details report views:

- "Incident Overview Report" on page 83
- "Incident Details" on page 86
- "Call Server Incident Details" on page 86

Acknowledging Incidents

Acknowledging an Incident reduces its priority in reports and indicates to others that the Incident has been reviewed.

If necessary, you can also unacknowledge an acknowledged Incident, to raise its priority in reports.

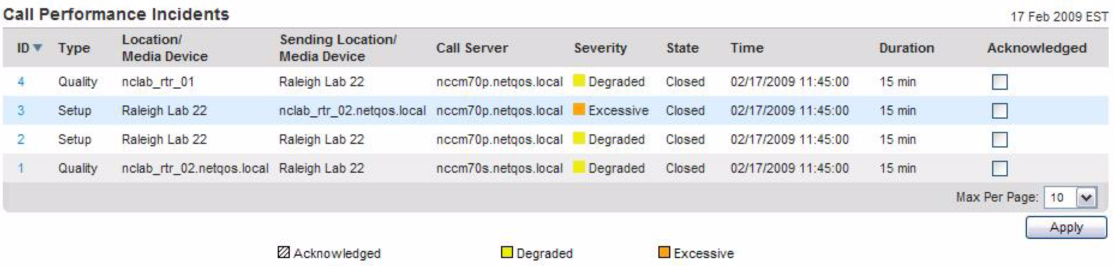
To acknowledge an Incident:

1. In the navigation links, click **Monitoring > Incidents**.

   The Incident Overview Report is displayed.

2. Find the Incident you want to acknowledge in the Incidents list.

3. Scroll to the right to find the **Acknowledged** column, which indicates the acknowledgement status of the Incident. Click to select the check box that corresponds to the selected Incident.



Call Performance Incidents

17 Feb 2009 EST

ID ▼	Type	Location/ Media Device	Sending Location/ Media Device	Call Server	Severity	State	Time	Duration	Acknowledged
4	Quality	nclab_rtr_01	Raleigh Lab 22	nccm70p.netqos.local	🟨 Degraded	Closed	02/17/2009 11:45:00	15 min	□
3	Setup	Raleigh Lab 22	nclab_rtr_02.netqos.local	nccm70p.netqos.local	🟧 Excessive	Closed	02/17/2009 11:45:00	15 min	□
2	Setup	Raleigh Lab 22	Raleigh Lab 22	nccm70p.netqos.local	🟨 Degraded	Closed	02/17/2009 11:45:00	15 min	□
1	Quality	nclab_rtr_02.netqos.local	Raleigh Lab 22	nccm70s.netqos.local	🟨 Degraded	Closed	02/17/2009 11:45:00	15 min	□

4. Click **Apply**.

The Severity status indicator now appears with gray shading to indicate that the Incident has been acknowledged.

Using UC Monitor for Troubleshooting and Diagnostics

NetQoS UC Monitor supports troubleshooting by collecting real-time diagnostic data based on precise network locations you can select. For example, if your user account and role allow it, you can launch a traceroute investigation to a selected network target and compare the resulting path information to baseline traceroute data collected from key phones and voice gateways. See "Launching a Traceroute Investigation" on page 106 for the steps.

The UC Monitor **Call Watch** feature also supports troubleshooting and diagnostics by collecting data from real-time monitoring of selected VoIP phone conversations for diagnostic purposes and presenting it in the Call Watch Overview Report. This feature is distinct from the core monitoring functionality that UC Monitor provides, which is largely passive monitoring of VoIP-related data. It is supported in Cisco and Avaya environments.

The **traceroute investigations** feature allows you to configure a traceroute test to run automatically as an Incident response or to launch a traceroute test on demand, to a selected target. For more information about Incident responses, see "Working with Incidents" on page 43. On-demand investigations are discussed in "Launching a Traceroute Investigation" on page 106.

In the Investigations report, the routine traceroute feature provides valuable information about the paths being taken by calls traveling through the system. By default, a traceroute test is run nightly to any Cisco voice gateway devices that have been discovered, collecting baseline path data that you can compare with the current path shown in the report.

Note: If you are monitoring Avaya call servers and endpoints, traceroute investigations have a few limitations. An Avaya-specific Call Path Report is often a better option. It also displays data about call paths, but this data is not linked to an investigation; rather, it is reported by the endpoints during each call.

To enable the Call Watch and investigations features, a UC Monitor user account must have an associated role with the appropriate privileges assigned by an Administrator.

More about the Call Watch Feature

The UC Monitor Call Watch feature provides an extra layer of call quality monitoring and can gather additional data from a potential problem area to use in troubleshooting. If a user complained of poor call quality, for example, you could initiate a Call Watch for her phone number to collect additional performance data. In the resulting Call Watch Overview Report, you would notice patterns in the measurements that would help you sort out the underlying problem.

Unlike the passive monitoring performed by the Collector at the core switch, a Call Watch is performed by means of active polling of the selected phone. When watching an IP phone, the Collector communicates with the phone via HTTP to collect in-progress call performance data from the phone's Web page. The HTTP query occurs every 15 seconds during the watch period if a call is active. An analog or PSTN phone can also be watched; NetQoS UC Monitor uses SNMP to query the MIB of the voice gateway that is routing the PSTN calls being watched every 15 seconds while a call is active.

Through active polling, the Collector can gather the following information from either the phone (if an IP phone number is watched) or from a voice gateway device (if a PSTN phone number is watched):

- Origination time
- Origination phone; destination phone
- Delay to dial tone; post-dial delay
- MOS
- Packet loss; jitter buffer loss
- Latency
- ACOM and ERL
- Signal in and signal out
- Concealed seconds; severely concealed seconds

See "Call Watch Overview Report" on page 112 and "Call Watch Details" on page 114 for more information about each of these metrics.

Note: Call Watch is not supported in a Microsoft Office Communications Server 2007 environment. In addition, a few older Cisco IP phone models do not support the collection of all Call Watch statistics. The Call Watch Reports will show no data for the statistics that are not supported.

Using the Call Watch Feature

The UC Monitor Call Watch feature performs extra, active monitoring tasks associated with all calls made to or from a selected phone. When you set up a Call Watch, you instruct UC Monitor to actively collect detailed, real-time call data for all calls traveling to or from a selected phone DN for a specific period of time. During the Call Watch time frame you specify, UC Monitor actively polls the associated device for information about call performance during active calls.

All calls made in an Avaya (Aura) Communication Manager environment are automatically watched. Data from these calls is displayed in the Call Watch Overview Report, with a **Type** of `Automatic`. Because this data accumulates rapidly, it is purged after two days. To retain Call Watch data for a longer time period, set up a Call Watch definition.

While you can set up Call Watch monitoring for multiple DNs, each Call Watch definition applies to a single phone DN. You can select either the DN of an IP phone inside your VoIP system or the DN of an analog phone in the PSTN for Call Watch monitoring.

Note: Call Watch is supported in Cisco and Avaya environments; it is not supported by the endpoints in a Microsoft Office Communications Server 2007 deployment.

Example of How to Use the Call Watch Feature

The Call Watch feature is specially designed for troubleshooting a reported problem with call setup or call quality. An example of when you would want to set up a Call Watch would be something like the following:

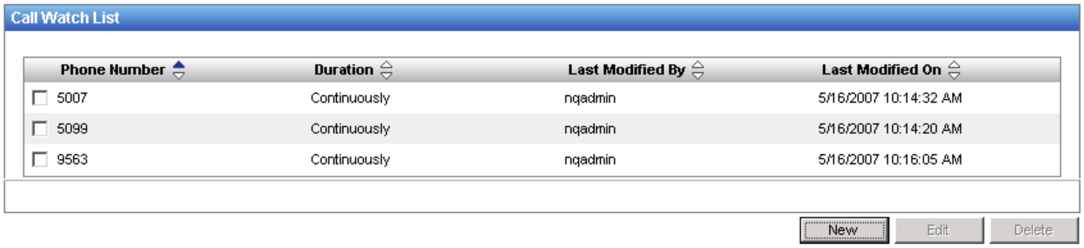
1. A coworker submits a Help Desk ticket claiming that the audio quality of the last call he made from his IP phone was very poor.
2. You set up a Call Watch, using the coworker's phone number and lasting two hours.
3. When you call the coworker at his desk, you ask him to make the call again to help you test the system.
4. When he makes the call again, the Call Watch feature performs extra polling to gather information about call performance.
5. You access the Call Watch Overview Report and watch the incoming data. Jitter and latency measurements are high, and the MOS value for the call is only 3.3.
6. You click the MOS bar chart to see which direction of the call was affected and note that the poor performance is occurring between the called party's phone (which is located in the PSTN) and the coworker's phone in the incoming direction only.

   This information indicates that the problem is most likely occurring at the voice gateway.
7. You switch to the Call Performance Overview Report and drill down into the data associated with the gateway at the user's Location.
8. You find that calls to and from this gateway have very low ACOM values, which could indicate a problem with excessive echo. As a next step, you will need to determine whether the echo canceller is functioning properly.

Viewing the Call Watch List

Each time you set up a Call Watch, a new Call Watch definition appears in the Call Watch List.

The Call Watch List is accessible from the navigation links. Click **Troubleshooting > Call Watch**, and then click **Definitions**:



Call Watch List

Phone Number	Duration	Last Modified By	Last Modified On
□ 5007	Continuously	nqadmin	5/16/2007 10:14:32 AM
□ 5099	Continuously	nqadmin	5/16/2007 10:14:20 AM
□ 9563	Continuously	nqadmin	5/16/2007 10:16:05 AM

The following information about each Call Watch definition is provided on the Call Watch List page:

Column Title	Definition
Phone Number	The phone number used to call this telephone or IP phone, in the format 8887675443.

Column Title	Definition
Duration	The length of time that the Call Watch will be performed. The date and time when UC Monitor will stop watching this phone are shown.
Last Modified by	The username of the user who set up or made changes to this Call Watch definition.
Last Modified on	The date and time the Call Watch definition was set up or modified; also the date and time when calls from and to this phone began to be actively monitored.

For information about how to set up a new Call Watch, see the following topic.

Setting Up a Call Watch

When you set up a Call Watch, you select a location on the network where you think performance issues are cropping up, and you instruct UC Monitor to gather extra data from a phone directory number (DN) in that location. You set up a Call Watch definition by selecting a DN to be "watched" and then setting the duration of the watch period.

Tips for Setting Up a Call Watch

As you select the DN to watch, keep the following guidelines in mind:

- All calls made by supported Avaya phones are automatically watched. No configuration is necessary in the Avaya (Aura) Communication Manager environment.
- Call Watch is not supported in a Microsoft Office Communications Server 2007 environment. In addition, a few older Cisco IP phone models do not support the collection of all Call Watch statistics. Select newer Cisco IP phones to watch.
- Call Watch works in both directions of the call.

  Unless there's a configuration issue in the Call Watch definition or in your network, Call Watch is bi-directional. Therefore, when you enter a DN to watch, all calls made by and to that phone number will be monitored for quality statistics.
- Do not include hyphens (-) or periods (.) to indicate the area code or exchange in the DN.
- Use an IP phone for the Call Watch.

  It's almost always best to select an IP phone from your VoIP network as the phone number to be watched. UC Monitor allows you to enter the directory numbers of analog phones located in the PSTN, but the complications of number transformations (see the next tip, below), area codes, and prefix digits make it difficult to enter them accurately. IP phones also provide extra information about call performance. To troubleshoot a voice gateway, select a DN that uses that gateway for the Call Watch.
- Supply enough digits to correctly identify the phone DN on your network.

  Depending on the "transformations" being applied on your network, the phone's extension may not be enough to identify it in CallManager and gateway records. See "Voice Gateways" on page 22 for more information.

  A phone's actual identity at the gateway matters because if you only enter a phone's extension as the Call Watch DN while the gateway is using more digits to identify phones, calls made to and from that phone *won't be watched* because UC Monitor won't be able to identify them.

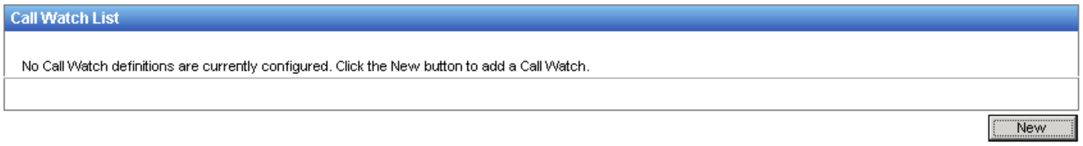
- Reload the Collectors each time you set up a new Call Watch or make changes to an existing one.
- Call the watched phone number. Or make a call from the watched phone.

  One good way to start gathering data from the Call Watch right away is to simply place a call to the selected phone number a few minutes after you schedule the watch to start and reload the Collector. Using this method, you can then check the Call Watch Real-Time report to make sure the number is being watched and update the Call Watch definition if necessary.
- Watch a gateway.

  If you're interested in watching a voice gateway, set up a Call Watch to a phone that uses that gateway, and then use a mobile phone to place a call to the watched number; or place a call from the watched phone. When the call is routed through the PSTN through the gateway, you'll see useful call performance statistics.

To add a Call Watch definition:

1. In the **navigation links**, click **Troubleshooting > Watch**, and then click **Definitions**.
2. The Call Watch List is displayed:



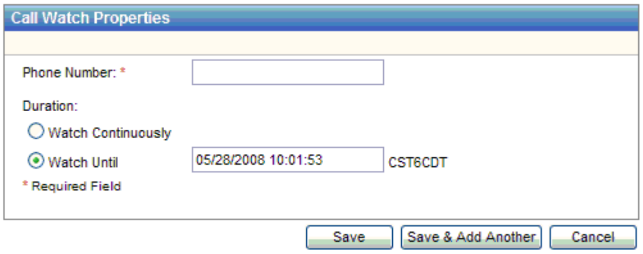
Call Watch List

No Call Watch definitions are currently configured. Click the New button to add a Call Watch.

   A message bar indicates that no Call Watch definitions have been set up yet.

3. Click **New** to add a new Call Watch definition.

   The Call Watch Properties dialog box is displayed:



Call Watch Properties

Phone Number: *

Duration:

○ Watch Continuously

● Watch Until 05/28/2008 10:01:53 CST6CDT

* Required Field

4. Supply information for the following properties:

Property	Description
Phone number	The phone number used to call this telephone or IP phone. Use the format 8887675443. Do not use hyphens (-) or periods (.) to separate the area code and number. Enter a direct-dial number.
Duration	

Property	Description
Watch Continuously	Continue to perform Call Watch functions until the Call Watch is manually canceled.
Watch Until	Perform Call Watch functions until a specified date and time. Enter the date when the Call Watch should end, using the format `MM/DD/YYYY`. The time is automatically set relative to the time zone of the currently logged-in user. You can edit it as a separate step. The default setting is to Watch Until 24 hours from the time the Call Watch definition is saved.

Note: After 8 hours of continuous polling—that is, in the unlikely event that a phone call is active at the watched phone for more than 8 hours—a Call Watch is automatically terminated for that call. Other calls to that phone are still watched.

5. Click **Save** to save this Call Watch definition.

   Or click **Save and Add Another** to save this definition and return to the Call Watch Properties page to set up another Call Watch.

CHAPTER 4

UC Monitor Reports

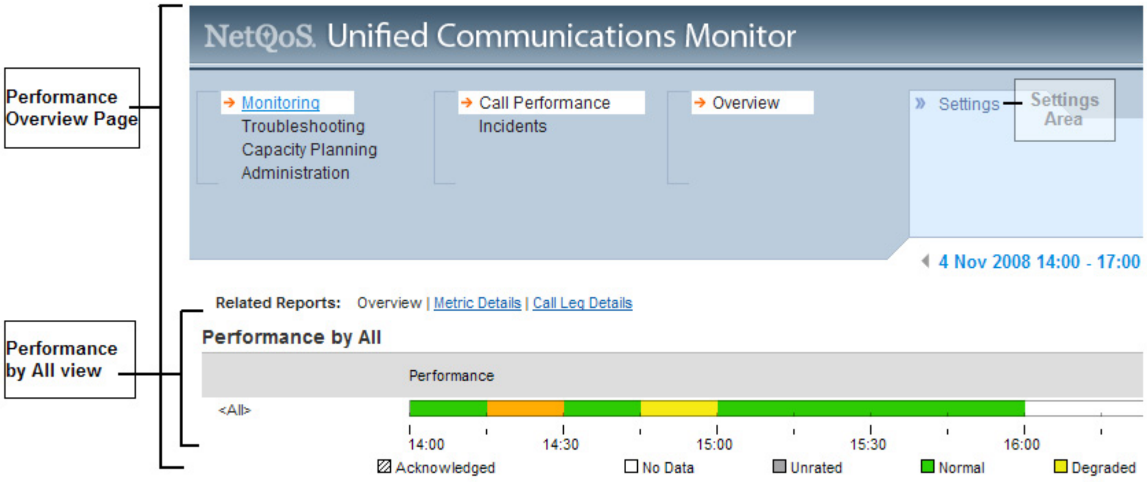
NetQoS UC Monitor offers a variety of reports that provide quick summaries of system health and call performance, detailed information about phones in the network and voice gateway utilization, and diagnostic data useful for troubleshooting performance issues. Reports provide summaries of performance data, with the worst-performing results shown first, as well as links to more detailed data that is narrowly focused on a single Location or component. Detailed information about endpoints active in the system is also available to help you with inventory and license tracking.

If an Administrator has defined any custom groups of Locations or devices in the NetQoS Performance Center, additional data views showing group-level metrics are included in the applicable reports. Drilldown is available from first-level groups into data from individual group members.

This chapter covers the following topics:

Report Pages, Views, and Navigation

On any report **page**, you can change the **views** that you see to gather more information about a particular performance condition. The term *page* describes the Web page you access by clicking items in the navigation links. For example, you can access the Call Performance Overview page by clicking **Monitoring** in the first set of navigation links, **Call Performance** in the second set of links, and **Overview** in the third set:



Each report page offers at least one *view* of the data, which has been collected and formatted as a chart. In the above illustration, the **Performance by All** view is shown first on the page. If an Administrator has defined custom groups for Locations and devices, the **Performance by Group** view is included just below the Performance by All view.

Within each view of the data, you can drill down into more detailed views by clicking hyperlinked items, such as individual call servers or media devices, such as voice gateways. Or you can use the navigation links to move between related reports and views.

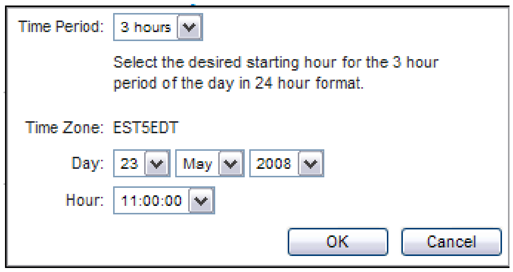
The following sections explain navigation among reports and views, the filtering settings that control which data is shown and the time frame, and how the metrics are calculated, rated, and presented.

Changing Report Views

Several filtering and drilldown options let you change the views on individual report pages to see different aspects of the data. Choose from the following options:

Report View Option	Description
Drill into the general overview reports to see more detailed information.	Click the hyperlinks within report pages to see more information about a particular item. See "Drilling down into Reports," below, for more information.
Narrow the data by selected criteria	Click any performance bar in the report to narrow the scope of data displayed. For example, in the Call Performance Overview Report, click the performance bar next to the first Location in the list to narrow, or restrict, the view of data shown in the report to calls measured to and from that Location.
Select a view in the lists of **navigation** links.	See "Navigation Links," below, for more information.
Change settings for a report page by clicking **Settings**.	See "Settings" on page 59 for more information.

You also have multiple options for selecting the time frame of the data you want to see. NetQoS UC Monitor stores data for up to 24 months; depending on your database maintenance settings, you can select any day from the stored data and view the data collected that day. The **Time Period** selector enables you to select the length of the segment of data that you want to see, such as a three-hour, one-day, or one-week segment. By default, data from the last three hours is shown for most reports. The Time Period selector is available just below the Settings area of the page. Access it by clicking the date-time link:



Time Period: 3 hours

Select the desired starting hour for the 3 hour period of the day in 24 hour format.

Time Zone: EST5EDT

Day: 23 May 2008

Hour: 11:00:00

The Call Performance reports offer a "custom" timeframe option to help you narrow the range of data being displayed and focus on a specific time of day. Select **custom** from the **Time Period** list. Then select a precise timeframe by selecting the day, the start time, and the duration of the custom timeframe. Available start times are based on the 15-minute reporting interval.

Drilling down into Reports

You can access detailed information from the general overview reports by clicking links in the reports themselves or by clicking the bar charts.

From overview reports, such as Incidents, Investigations, or Call Watch Real-Time, you can see detailed information about individual items by clicking the link corresponding to the item identification number.

Once you have clicked a link to drill down into a report, the term "Narrow by" is applied to the view to indicate the focus of the data being rated.

If an Administrator has defined custom groups for Locations and devices in the NetQoS Performance Center, drilldown from a view that lists group names and provides rollups of data for entire groups is available. The drilldown path takes you into data for each individual group member, such as a single Location, media device, or call server. Filtering by group is also available in the Settings dialog box.

The Call Leg Details reports (including the Performance Call Leg Details and Incident Incident Call Leg Details reports) provide an option to quickly access detailed, per-call information from a filtered view of data from individual call legs. An information icon ℹ next to table entries that have detailed call data also serves as a link to the Call Details Report for the selected calls.

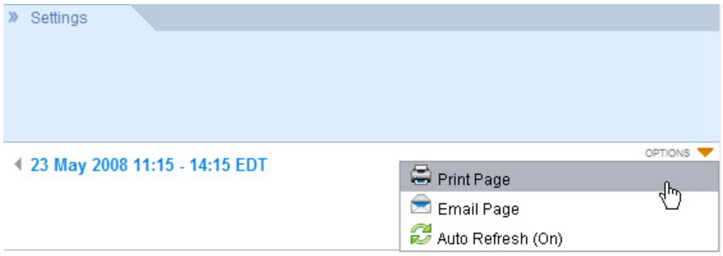
Navigation Links

On each report page, the sets of **navigation** links enable you to select a report or Administration page to view. Indicators light up next to the active links in the navigation list to help you move between reports.

The default report page places you in the Monitoring section of UC Monitor reports. The default page, the Call Performance Overview, provides an overview of call performance system-wide. From that page, you can easily access a report of detailed call setup and call quality metrics, or a report listing Incidents that occurred. Or you can click another link, such as **Capacity Planning** or **Troubleshooting**, from the first set of navigation links to see other reports.

Page Menu

The Page menu lets you perform export operations for the information contained on a report page. Click the orange arrow to see the menu items, as shown below:



The Page menu (labeled **OPTIONS**) is only available on report pages. The following options are available from this menu:

Menu Item	Description
Print Page	Prints the entire report page after converting it to Adobe PDF format. You are asked to select a vertical (Portrait) or horizontal (Landscape) orientation and page size. See "Print Properties" on page 57 for more information about the available options. Even after you select a longer page size, multiple pages might be needed to show all Locations. You may have to print multiple times to see all pages.
Email Page	Sends the report page in Adobe PDF format to specified recipients via email. If multiple pages are needed to show all Locations, multiple email messages are required. When you email a report page, you can send the report immediately, or **schedule** it to be sent at a later time. See "Selecting Properties for Emailed Reports" below for more information.
Auto Refresh (On or Off)	When set to **On**, enables an automatic refresh of the report in the browser to show any new data that has been sent from the Collector since the page was last accessed or refreshed. If enabled, refreshes the page automatically every 60 seconds. A global setting that affects all report pages.

Print Properties

When you select the **Print** option from the Page Menu, the Print Properties dialog box is displayed. Because some UC Monitor reports contain tables with many rows or many columns (or both), the Print Properties let you select formatting options for the report so that columns and table entries are printed appropriately. The following table describes the available properties:

Option	Description
Output Orientation	The directional orientation of the printed page. Select either: • **Portrait**: Standard printing on a page where the text is oriented vertically, or • **Landscape**: Text is oriented horizontally on the page. If the report contains a table with many columns, such as the Performance Call Leg Details Report, you should choose this option.
Page Size	Select a page size setting that will accommodate the amount of data that you want to print. For example, if you want to print the Call Leg Details Report or another report using the Landscape orientation, you can select the Legal paper size, which is longer than the Letter size. The following options are available: • **Letter**: 8.5 x 11" (the default) • **Legal**: 8.5 x 14" • **A3**: 11.7 x 16.54" (297 × 420 mm) • **A4**: 8.26 x 11.7" (210 × 297 mm) • **A5**: 5.83 x 8.26" (148 × 210 mm)

When you have made your selections, click **OK**. The page is exported to PDF format and displayed in your default PDF viewer. You can then either save it or verify the settings on the printer driver before printing it.

To verify settings and print from the PDF viewer:

1. If you are satisfied with the way the report looks in the PDF viewer, click the **Print** button in the viewer toolbar.

   Otherwise, close the PDF viewer. Return to the Print Properties dialog box to select different settings.

2. In the Print dialog box, take a look at the Preview area. A diagram shows the page size that will be used by default.

   If the default size is the same as the size you selected in the Print Properties, skip to Step 3.

3. If you selected a size other than the default page size, click to select the check box labeled **Choose Paper Source by PDF page size**.

   The Preview changes to show the size you selected.

4. Near the top of the Print dialog box, in the **Printer** area, verify that the printer where you want to send the printing job is selected in the **Name** list.

   If it isn't, click to select the desired printer.

5. Click **OK** to print the PDF on the default printer.

Printing Tips

If the report does not easily fit onto one of the available page orientation and size options, use the Settings dialog box to filter out some data. For example, you can remove some columns from the data tables in the Call Leg Details reports to make the tables narrower.

The default page size is determined by the printer driver settings on the computer where you are viewing the report. You may find that when you select a different paper size, the selected printer displays a message stating that the selected size cannot be found. Often you just need to select a new paper tray on the printer itself to complete the print job.

If you plan to print reports frequently using a paper size other than the default, you might want to change printer driver settings so that the new paper size is sent to the printer by default.

To change printer driver settings:

1. Click **Start > Settings > Control Panel > Printers and Faxes**.

2. Select the printer that you want to use. It should be the name of a network printer and not an internal driver, such as Adobe PDF.

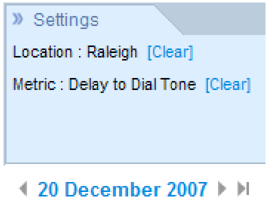
   If no external printer is shown in the list, click **Add Printer**, and use the **Browse for Printers** feature to search the domain for printers.

3. Right-click the printer, and select **Printing Preferences**.

The next steps to take depend on the type of printer driver you are configuring.

Settings

The Settings area appears at the top of each report page. The **Settings** heading is a link to a dialog box containing filtering and display options specific to the report currently being viewed. Beneath the heading, the current selections for the page are displayed. Each time you narrow the views that are shown by clicking a link, such as the link to a group or Location, the new selection is reflected here:



» Settings

Location : Raleigh [Clear]

Metric : Delay to Dial Tone [Clear]

20 December 2007

The image above shows settings after drilldown into the Call Performance Overview Report. The Time Period selector is also shown (a blue link below the Settings area).

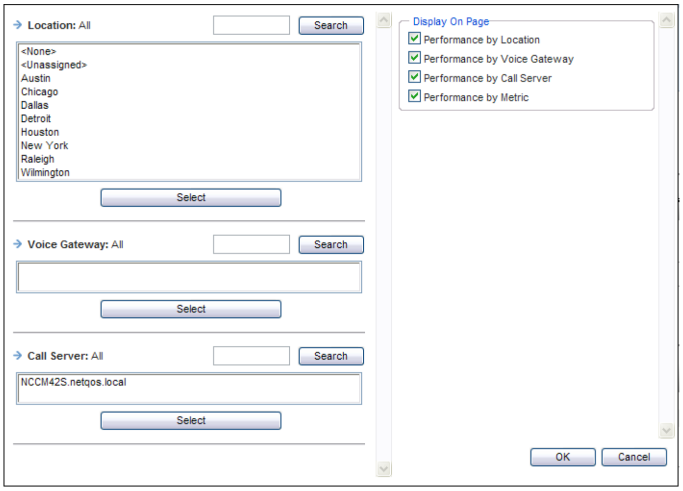
To change report settings:

1. On the selected report page, click **Settings**.

   The Settings dialog box displays the available filtering and display options for the report page.

   Each report page displays a set of options that are appropriate for the available data. Options on the left mimic the drilldown paths available from the report data. Options on the right (labeled **Display on Page**) affect the data views or tables that are included in the report.

   The example below shows settings for the Performance Overview Report:



Location: All

Search

<None>
<Unassigned>
Austin
Chicago
Dallas
Detroit
Houston
New York
Raleigh
Wilmington

Select

Voice Gateway: All

Search

Select

Call Server: All

Search

NCCM42S.netqos.local

Select

Display On Page

☑ Performance by Location

☑ Performance by Voice Gateway

☑ Performance by Call Server

☑ Performance by Metric

OK Cancel

2. Click to highlight an item by which you want to narrow the data that is shown on the report page. For example, to see only data views that are relevant to the Location named Raleigh, click the Raleigh Location in the list of Locations. Then click the **Select** button to select it.
3. If more drilldown or narrow by options are available, repeat the previous step, as desired.
4. After completing your selections, click **OK**. The report page displays, using the new settings.

As a general rule, each selection you make restricts the other settings available to you, showing you only the options that represent a valid drilldown path into the report data. But each Settings dialog box contains options that are specific to the selected report. The Settings dialog box also contains options to filter by group name and group member if custom groups have been defined.

Note: If you have defined a NetQoS SuperAgent data source in the NetQoS Performance Center where the UC Monitor data source is registered, the “All Servers” system group appears as a selection in the Group list. This group contains devices (specifically, call servers and other media devices) known to both data sources. The SuperAgent data source will also be included as a choice under the Data Sources group in this list.

Some of the settings you select are associated with your user account and persist for the relevant report across login sessions. These include settings that indicate a viewing preference, such as the **Display on Page** settings and **Additional Settings**. Drilldown settings only persist among related reports. For example, the filtering applied to the Call Performance Overview also applies to the Call Leg Details for that report. Otherwise, drilldown settings are automatically cleared as soon as you navigate away from the page.

Once you’ve made selections, you can clear them and start over from the default report views by clicking the **[Clear]** links in the Settings area at the top of the report page, or by clicking the **[Clear]** links that appear next to each selected item in the Settings dialog box itself. The [**Clear]** links in the Settings area clear out any choices you’ve made to a report view, whether by drilling down using links in the report views, or by making selections in the Settings dialog box.

Navigating between Reporting Interfaces

If you are also running NetQoS Performance Center version 4.0 or later in your environment, toggling between reports in the UC Monitor interface and the Unified Communications Dashboard Report page in the NetQoS Performance Center is supported. To access the Unified Communications Dashboard from NetQoS UC Monitor, click the **NPC** link in the upper right corner of the Management Console. If your user account allows you to access the NetQoS Performance Center, you can navigate between the two interfaces without having to supply authentication credentials.

Selecting Properties for Emailed Reports

Each UC Monitor report page offers multiple options for sharing report information with coworkers. From the Page Menu on each report page, you can access options to print and email the report pages to which you have access. For example, you can email Call Activity Utilization Report pages to coworkers in the IT department to provide detailed data for use in capacity planning. Or you can schedule Incident reports to be sent via email on a regular basis to help your team track the performance of the entire VoIP system.

Note: The UC Monitor Administrator must configure an email server to enable this feature.

On the Send Email Properties page, supply the following information to send a report page to a selected recipient (or to multiple recipients) in an email message:

Email Property	Description
Email Properties	
Send To:	Enter email addresses in the format: `<name>@<domain>` Separate multiple addresses with commas or semicolons. ***Note:*** You can enter an email alias that includes multiple recipients.
Subject	A descriptive subject for the emailed report. Include the report title and any Locations or components included in the report.
Message	A message to accompany the emailed report. Optional field.
Time Zone	The time zone of the data shown in the emailed report. Select the time zone of the intended recipient. The time zone of the message recipient is set by the Administrator during user account configuration.
Scheduling Options	
Send Now	Send the email message immediately.
Send on a Schedule	Schedule the email message containing a current version of the report to be sent on a regular basis. If enabled, reveals scheduling options (see below).
Send Daily	Schedule the email message to be sent once per day. If enabled, reveals check boxes where you can select the day of the week when the report should be sent. By default, the daily schedule sends the emailed report every weekday (Monday - 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	Schedule the email message to be sent once per week. If enabled, reveals a menu where you can select the day of the week when the report should be sent. By default, the weekly schedule sends the emailed report 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 - Saturday).
Send Monthly	An option to schedule the email message to be sent once per month. If enabled, the report is sent on the first Sunday 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.. ***Note:*** This scheduling option is only available for the Capacity Planning reports.

In addition, the Management Console can supply the email address of the user who is configuring the email schedule as the "**Reply to**" address. An Administrator must have configured an email address in the User Properties. Any recipient of the emailed report can then reply to this user.

Unsubscribing from an Email Schedule

Once you have received a scheduled report via email, you can unsubscribe yourself from the schedule.

To unsubscribe your user account from scheduled email reports:

1. Open the email message containing the report. By default, the Subject line is the same as the name of the attached report.
2. Scroll down and click the link labeled "**To unsubscribe from email**:"
3. The UC Monitor Management Console opens in a browser window.

   The Email Subscriptions page is displayed.
4. Click to select one of the following options:
   - Unsubscribe the designated recipient from this specific email schedule
   - Unsubscribe the designated recipient from every scheduled email sent from this SMTP server
5. Click **Unsubscribe**.

You can then choose to either close the browser window or log into the Management Console.

Interpreting Data in Reports

Each time a call is made or attempted on the network, the Collector gathers data from the flows that pass through the switch it shares with a call server or call server cluster. Only the data needed to calculate the call setup and call quality metrics that the UC Monitor system provides is retained and sent to the Management Console for evaluation.

Data evaluation takes place when the collected metrics are compared to the performance thresholds assigned to phone Locations and media devices. Incidents are only created if enough observations—either calls originated or call minutes—are collected.

The following topics provide more information about how data is evaluated and presented in UC Monitor reports:

- "Data Ratings" on page 63
- "Call Legs and Bi-Directional Data" on page 64
- "Call Legs and Monitoring Reports" on page 65
- "Call Attempts and Reporting Intervals" on page 63

Data Ratings

In most reports, for each assigned threshold, UC Monitor classifies the relevant data for call performance metrics by using one of the following ratings:

▨ Acknowledged □ No Data ■ Unrated 🟩 Normal 🟨 Degraded 🟧 Excessive

The following table describes each rating:

Rating	Description
Acknowledged	When you acknowledge an Incident, all the data the Incident covers is marked as acknowledged. Any future data covered by an Incident that has been acknowledged is also automatically marked as acknowledged.
No Data	No data is available.
Unrated	Either: • Sufficient data does not exist to establish a rating, or • The number of observations is less than the minimum observations threshold.
Normal	The metric value does not exceed a performance threshold. Performance may be considered good, or normal.
Degraded	The metric value exceeds the degraded threshold.
Excessive	The metric value exceeds the excessive (excessively degraded) threshold.

Call Attempts and Reporting Intervals

Every attempted call is logged in the database as a call attempt. However, to receive call setup measurements in the Call Performance report, a call must progress far enough to receive a response-time measurement.

UC Monitor measures call setup response time based on the time it takes for the call server to send setup information to a phone that is attempting to make a call. In a few rare cases, a call attempt may be logged with no data for the call setup metrics because no response time could be measured from the call server. Call server response time is used to calculate the post-dial delay and delay to dial tone metrics. The call server shares a switch with the Collector. In cases where a call is abandoned before a ringing signal is sent, the Collector's proximity to the call server may cause response-time measurements to be too negligible to be recorded. A call attempt would be logged in such a case, but no call setup metrics would be provided.

Call performance data is collected continuously and sent to the Management Console, but reports are updated every 15 minutes. Call quality metrics are collected as soon as a call completes, but they do not appear in reports until they are received at the Management Console and processed. A *reporting* interval is distinct from a *monitoring* interval: monitoring is continuous, while reporting occurs every 15 minutes. A call must end during a reporting interval for the call metrics to appear in reports, and it can take a few minutes for all data to be reported by the Collector.

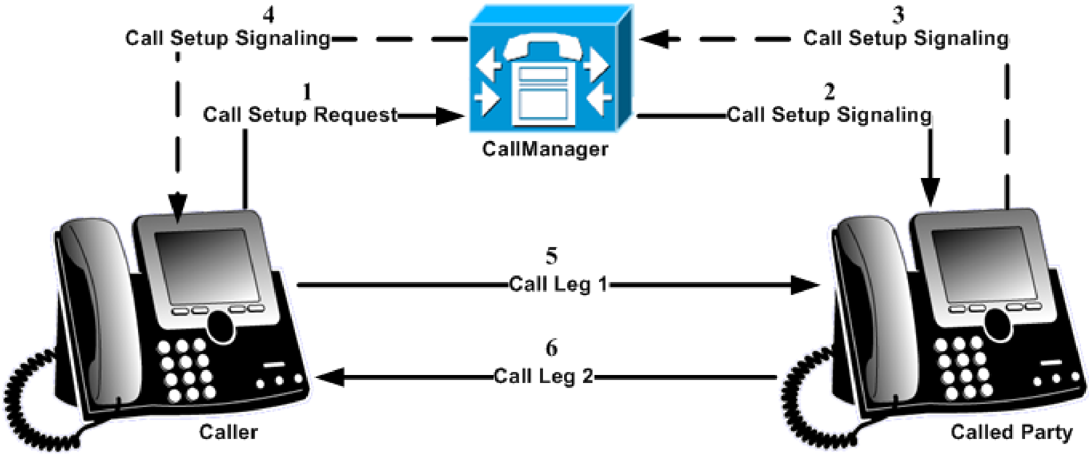
Note: Call Watch monitoring is performed differently. Data from watched calls is collected every 15 seconds and reported every minute.

A call that fails or is intentionally abandoned must actually reach the ringing phase for the UC Monitor product to be able to log both the calling and called party IP address or phone number.

Call Legs and Bi-Directional Data

When NetQoS Unified Communications Monitor collects the data it needs to rate call performance, it uses different methods to get call setup and call quality data. The basic unit of analysis for all metrics, however, is the "call leg," a unit expressing direction and applied to each of the bi-directional flows that carry VoIP and video conversations between the two conversing parties. The two parties may be referred to as the *caller* and the *called party*.

As a call is being set up by the call server, different types of setup data are exchanged between the server and the two parties' phones so that a ringing signal and other notifications may be sent. But after the call is in progress, two IP phones exchange bi-directional data streams directly (as shown in the image below of a call between Cisco IP phones):



The data for each leg represents a *direction* of data flow and not a single flow (such as a single sentence spoken by one call party to the other); thus, all the data taken from all discrete flows in the direction represented by a call leg is averaged and shown in reports for that call leg. The ways call legs are broken out in reports are discussed below in "Call Legs and Monitoring Reports" on page 65.

Note: A few limitations apply to the Collector's ability to correlate data from each call leg. For example, discrete call legs representing a single conversation may be reported as separate calls if a Media Termination Point (MTP) is used for the call (as when H.323 FastStart is used). See the Release Notes for details.

The Collector doesn't "listen in" on any conversations. Most data used in Cisco call performance measurements is collected from flows traveling to and from the Cisco call servers that are connected to the switch that the Collector is monitoring. For example, each Cisco IP phone reports quality metrics to its call server at the completion of every call. Avaya endpoints send packets containing call-quality data directly to the Collector. Or, in a Microsoft Office Communications Server deployment, the endpoints send end-of-call quality reports to a Microsoft server, which forwards them to the UC Monitor Management Console.

The UC Monitor software captures these metrics and uses them in calculating and reporting on call performance. For Cisco deployments, it gathers call setup data from call server flows and measures delay based on the timing of flows between the caller and call server. NetQoS UC Monitor can derive the delay to dial tone and post-dial delay call setup metrics based on these timings.

Without eavesdropping on calls, the Collector does monitor call legs in each direction. The Collector can also obtain call performance data from call legs that involve phones in the PSTN by polling the Cisco voice gateway that routed them, or by passively receiving call-quality reports from Avaya gateways. The Collector can gather data from all call legs that are processed by the call server(s) with which it shares a switch.

UC Monitor reports use the data from each call leg to evaluate the *listening quality* that UC system users experienced. For example, in Call Watch Reports, the call quality experienced by the listener is expressed as MOS values from call legs traveling *toward* each Location. The following topic explains how the listening aspect of call performance is presented in reports.

Call Legs and Monitoring Reports

The direction of a call leg matters when you are troubleshooting a performance issue. Reported performance may be different for each direction of a call, although in most cases the differences are slight. The route that a call is taking through your network may be asymmetric, for example, with a longer route—and thus, more delay—in one direction between the conversing parties.

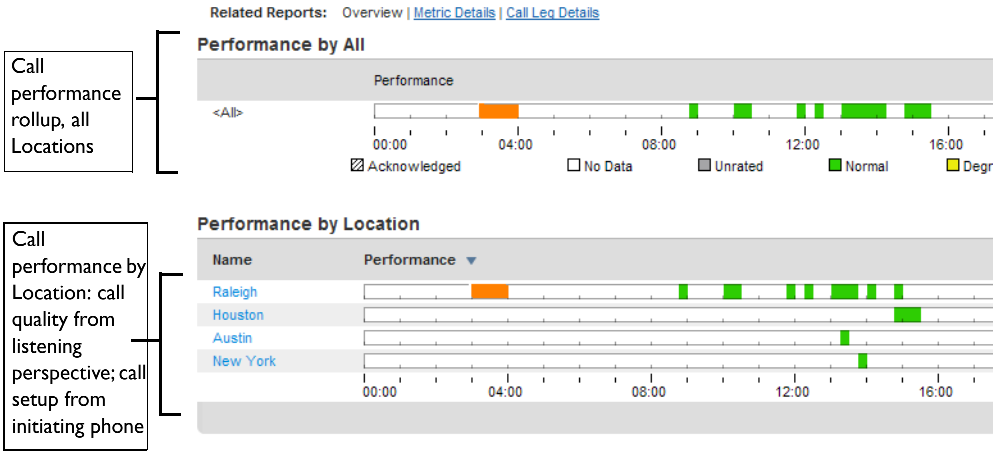
Therefore, you should keep the concept of bi-directional calls and call legs in mind as you interpret reports in the Monitoring section. And you should understand which directions are being presented in each view. (Call legs are discussed in detail in "Call Legs and Bi-Directional Data" on page 64.)

The top-level Call Performance Overview report first presents a view of performance data taken from, and averaged for, all Locations. In this view, call performance data is a rollup of Call Setup and Call Quality metrics. **<All>** indicates all Locations, including the "`<Unassigned>`" and "`<External>`" Locations. (See "Terminology: Locations" on page 67 for an explanation of these default Locations.)

Note: If you have defined some custom groups of UC devices and Locations, the first rollup view comprises data from all groups; subsequent views allow you to select individual groups and then drill down into data for specific Locations. The *UC Monitor Administrator Guide* includes an appendix that explains aspects of the grouping feature that are specific to NetQoS UC Monitor. This feature requires the NetQoS Performance Center.

The Call Performance Overview Performance by All view is a true rollup view, containing data from all observed call legs, traveling in both directions (inbound to the IP network and outbound to the PSTN; sending and receiving). But once you drill down to see metrics for selected Locations, media devices, or call servers, the Locations are divided into sending and receiving legs. An example will help to explain this concept.

With the default settings and no links selected, the first view in the Call Performance Overview Report shows all Locations (“Performance by All”). Then the next view down usually shows call performance data sorted by Location, with the worst-performing Locations listed first to help you detect problems quickly:

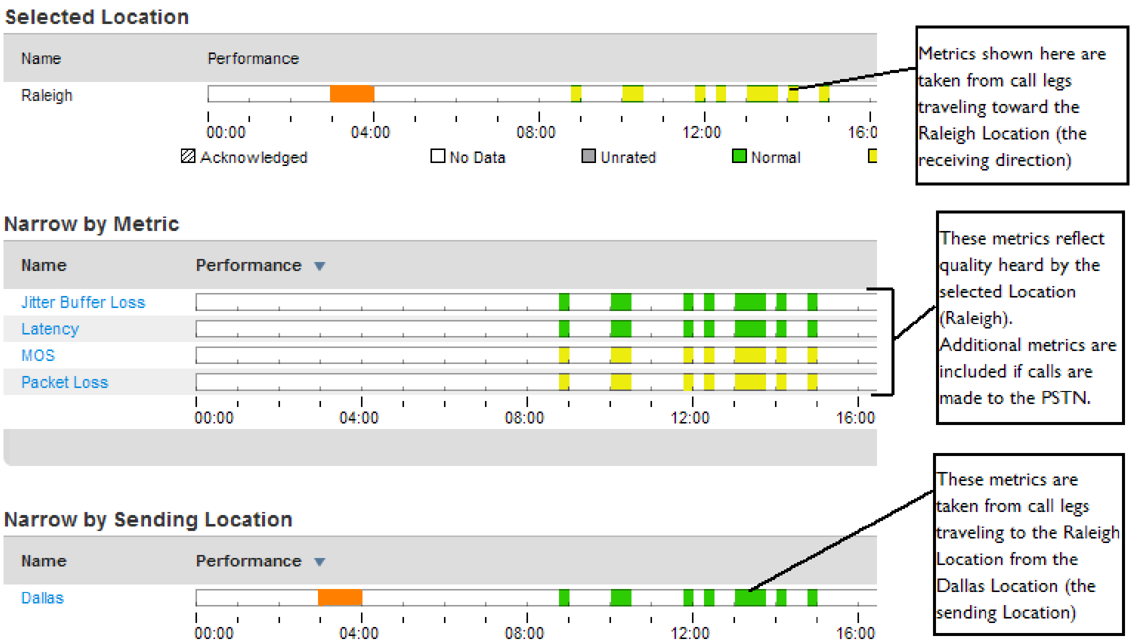


Call performance rollup, all Locations

Call performance by Location: call quality from listening perspective; call setup from initiating phone

The perspective on the data has changed with the Performance by Location view. Here, the call quality data being rated is only the data *observed by* that Location. That’s because measuring from the *listener’s perspective* is the most accurate way to judge a user’s experience with voice over IP. No matter which party initiated the call, in the views that show call performance broken out by Location, the call quality perspective is that of the listener, and the call-quality metrics are from the call legs traveling toward that listener. Call Setup metrics are taken only from the calls that originated at that Location.

If you clicked the first individual Location listed in the Performance by Location view shown above (in our case, the Raleigh Location), you would see a page similar to the following:



Metrics shown here are taken from call legs traveling toward the Raleigh Location (the receiving direction)

These metrics reflect quality heard by the selected Location (Raleigh). Additional metrics are included if calls are made to the PSTN.

These metrics are taken from call legs traveling to the Raleigh Location from the Dallas Location (the sending Location)

To show you the performance that users experienced when listening to VoIP and video calls on the monitored network, the Monitoring report views generally break out performance for a selected Location using data from the receiving direction. On drilldown by Location or by media device, the Sending Location is also shown in a separate view (shown in the image above). This allows you to easily distinguish the performance—by direction—of calls made between the pairs of Locations and/ or media devices.

Terminology: Locations

In Monitoring report views, the term **Location** refers to the metrics calculated from the call data streams that were *received by* phones in the applicable Locations. The term **Sending Location** is used to distinguish the views that show metrics for the *sending* direction. This allows you to quickly determine which sending Location is having a quality problem.

The `<Unassigned>` Location indicates IP phones that have been observed during monitoring but whose IP addresses don't fall into any subnets in the Locations you have defined. It is not the same as a Location of "`<None>`". If `<None>` is shown as the Location or Sending Location, it indicates that the IP address of the phone was not determined. This can happen when:

- A call setup failure occurred before the number could be determined.
- A phone number in the system has not been assigned to a phone.

By contrast, a phone may be `<Unassigned>` because:

- Locations have not been defined for IP address ranges of some phones in the network.
- There is a misconfigured device pool in a Cisco Unified Communications Manager (CallManager).
- The phone is misconfigured, placed in an unexpected VLAN or with an unexpected IP address.

The `<External>` Location only appears if Microsoft Office Communications Server 2007 is being monitored. This default Location indicates endpoints that are being reported to the QoE Monitoring Server or Front-End server as being "remote." Specifically, NetQoS UC Monitor uses this Location definition for endpoint addresses outside your network—that is, outside the firewall or behind a NAT device—that are making remote access connections through an edge server. Such endpoints have been assigned a temporary IP address (usually a private address) that potentially overlaps with internal IP addresses in use by other endpoints.

Monitoring Reports

The Monitoring report pages are intended to help IT staff track and monitor UC system performance and detect problems early. NetQoS UC Monitor “bubbles up” the worst-performing groups, Locations, call servers, and media devices so that you can detect problems at a glance. As you click any of these critical items, you can then select from the available variables to narrow the focus of the data you see. The topics that follow provide descriptions of the performance metrics contained in the Monitoring reports, as well as procedures for using the Monitoring report pages and examples of using these reports to understand and even avoid VoIP and video performance problems.

Navigating in the Monitoring Section

Access the following report pages and views from the **Monitoring** navigation link:

Report Page	Description
Call Performance Overview Report	Offers overview of call performance, including call quality and call setup. Displays performance by Location and then by component, categorized by performance level as compared to the thresholds: Normal, Degraded, Excessive. Provides a metric average based on the number of observations. Worst-performing Locations are “bubbled up” to the top. Provides an opportunity to drill down into: • Call Performance Metric Details • Call Leg Details
Incident Overview Report	Shows a list of Incidents that were raised in response to threshold violations. Provides some basic information about when Incidents were reported and where, and allows for quick drilldown into individual Incident reports. Provides an opportunity to drill down into: • Incident Details • Call Server Incident Details • Incident Metric Details • Incident Call Leg Details Also provides access to the Investigations area, where you can view the list of investigations that have been performed automatically.
Collector Incidents	Shows a list containing basic information about each Incident reported against Collector performance. Collector Incidents report problems that are local to a specific Collector. They do not apply to Microsoft deployments.
Investigations	Shows a list of investigations that were run in response to Incidents, on a scheduled basis for baseline data collection, or on demand. Provides basic information about when investigations were launched and where they ran. Allows for quick drilldown into individual Traceroute Investigation Details reports. Investigations may be launched manually from the Troubleshooting Reports area.

Report Page	Description
Quality Reports	The Quality navigation link provides access to the following two reports • Worst Locations Quality Report—Provides a quick overview of the worst-performing pairs of Locations or groups, based on their performance data and the associated performance thresholds. • Worst Phones Quality Report—Provides a quick overview of the worst-performing endpoints or phones, based on their MOS or Network MOS values and the associated performance thresholds.

Call Performance Overview Report

The Call Performance Overview provides a quick evaluation of the overall performance of your entire UC system. It also provides an easy point of entry when you need to drill down into specific data about a location, media device, or server you select for further analysis.

Call Performance comprises both **call quality** and **call setup** metrics. These two categories of metrics are combined in the Performance by Location, by Media Device, and by Call Server views to show call performance on the network. The call performance rating is a reflection of end-users' experience from the time they pick up the phone until they hang up at the end of the conversation.

Note: If you have defined custom groups of VoIP or other media devices and Locations in the NetQoS Performance Center, the first view is a rollup of data from all groups. Subsequent views allow you to narrow the report to a particular group or Location.

Data from both legs of a call is available in the **Related Reports**. Links to those reports are provided just above the first data view.

Before you drill down and filter the data that's shown in the Overview Report, the data that you see was taken from call legs *traveling toward* the indicated Locations. That data helps you understand the user experience while interacting with the system by emphasizing the call quality that the listener perceived. The term "sending" is used to label drilldown views that show data traveling toward a "selected Location" from a single Location or device.

Important: In drilldown reports, check the **Number** and **Sending Number** rows for data in the **Delay to Dial Tone**, **Post-Dial Delay**, or **Call Setup Failure** columns. Only the phone that placed the call has these Call Setup metrics.

For more information about the perspective from which data is rated and displayed, see "Call Legs and Monitoring Reports" on page 65.

Performance by All View

The first data view summarizes the performance of your entire UC system: data gathered from all monitored Locations and components is rolled up into a Performance bar chart labeled "Performance by All." If you have registered the UC Monitor data source with the NetQoS Performance Center, this top-level view is a rollup of data from all groups; otherwise, it is a rollup of data from all Locations.

This view is a good place to see, at a glance, the call volume of the system during the time period indicated: the **Calls Originated** column shows the number of calls that were placed by all phones in the monitored system.

Just below that section are several data views that break out call performance into Locations, then media devices, and then call servers.

Click the hyperlinks within each view to see more specific information about selected Locations or components or to narrow the report perspective to items of interest. The topic titled "Drilldown Views" on page 71 helps you understand what is shown after you click a link.

Performance by Location and Performance by Group

Unlike the Performance by All rollup, the Performance by Location data view begins to break out call performance by individual Location. This view lists all monitored Locations where phones had call activity.

Note: If you have defined any custom groups in the NetQoS Performance Center, the Performance by Group view precedes the Performance by Location view. You can drill down into individual group members and their data by clicking a group name. This view does not appear if you have not registered the UC Monitor data source with the NetQoS Performance Center.

The Performance by Location and Performance by Group views rate call performance in the incoming direction in order to gauge the listening quality that VoIP and video users in that Location experienced. To see ratings for performance metrics and for the components participating in calls to the Locations listed in this view, click a Location hyperlink.

For more information about how data is presented in the Call Performance Overview report, see "Call Legs and Monitoring Reports" on page 65.

Performance by Media Device View

In this view of media device performance, the perspective is of calls that the device handled: incoming from the PSTN, as well as outgoing from the IP network.

The *media device* category includes voice gateways and other devices that support call routing and processing. The metrics available for each device vary according to the device type and the environment. In a Microsoft Office Communications Server environment, SNMP polling of media devices is not possible, and as a result, fewer metrics are available for Microsoft media devices than for Cisco voice gateway devices. See "VoIP Hardware" on page 20 for more information.

The **Calls Originated** column provides the total number of calls that originated at points in the PSTN.

Performance by Call Server View

The call servers listed in the Performance by Call Server view are those that handled calls during the reporting interval. Their performance ratings are derived from the Locations they served, which can be seen by drilling down on a call server link.

The **Calls Originated** column provides the total number of calls that were set up by the call servers indicated. Calls not included in the Calls Originated total were routed by the call servers in this view but set up by another call server.

Drilldown Views

The UC Monitor report pages are designed to help you investigate performance degradation by "narrowing" the reports in ways that make it easy to compare the ratings among Locations, metrics, media devices, and call servers. You facilitate troubleshooting by drilling down into data, or *narrowing* report views, so that the charts of interest are presented in proximity.

Depending on how you drill down from a particular Performance by view, the additional views presented vary.

Narrow by Audio Metric

When you drill down into the performance data by clicking any component in the Performance by views of the Call Performance Overview Report, the Narrow by Audio Metric view becomes available. This view presents the performance ratings for the selected component, group, or Location.

The ACOM metric is a gateway-only metric. If no voice gateway was used for the calls whose performance is being reported in a particular view, no ACOM data is available. If you narrow the view to a Location that did not make or receive any PSTN calls during the selected timeframe, no ACOM metrics are shown.

See the following topics for more information about these metrics:

- "Call Quality Metrics" on page 78
- "Call Setup Metrics" on page 81

Narrow by Video Metric

When you drill down into the performance data by clicking any component in the Performance by views of the Call Performance Overview Report, the Narrow by Video Metric view becomes available beneath the Narrow by Audio Metric view. This view presents the video performance ratings for the selected component, group, or Location.

The video metrics are only reported if you are monitoring a Microsoft Enterprise VoIP system; they are not available in a Cisco-only deployment.

See "Video Metrics" on page 82 for more information about these metrics.

Narrow by Sending Location or Sending Media Device

When you drill down into a report by clicking the name of a Location, the Location you clicked is shown as the “Selected Location.” The Narrow by Audio Metric, Narrow by Video Metric, Narrow by Sending Location, Narrow by Sending Media Device, and Narrow by Call Server views become available. These views list the Locations or devices that communicated with the selected Location—that sent data to it.

To find the Location or device that placed the call, look for Call Setup metrics. Those metrics are only available from phones that placed calls.

Narrow by Location or Media Device

When you drill down into a report by clicking the name of a call server, the Narrow by Audio and/or Video Metric, Narrow by Location, and Narrow by Media Device views become available. If you then click one of the listed Locations or devices, that component receives the “Selected” designation. Only components that communicated with the selected call server during the selected time frame are then displayed.

Narrow by Call Server

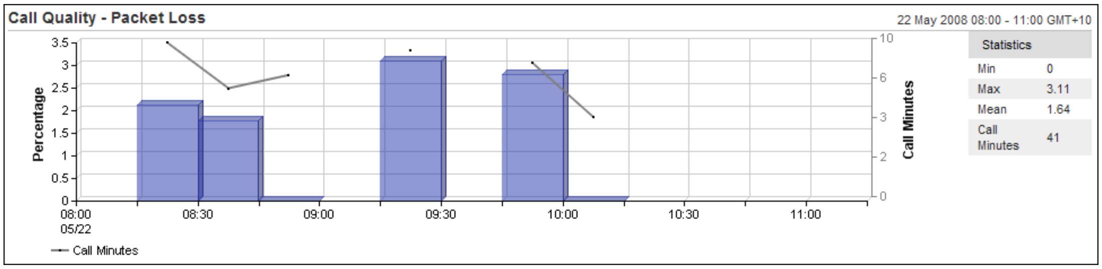
When you drill down into a report by clicking the name of a Location or media device, the Narrow by Call Server view becomes available. Only the call server used by phones in the selected Location is shown.

Call Performance Metric Details

The **Metric Details** link at the top of the Call Performance Overview Report enables you to see detailed charts of the collected data for each performance metric.

In the Metric Details data views, collected data is graphed over an X axis showing the time frame. A gray line graphs the number of applicable data observations that were used in the ratings: either **calls originated** or **call minutes**. The total number of observations is shown in the legend for each data view. See “Observations in Call Performance Reports” on page 76 for more information.

A logarithmic scale on the right Y axis shows the number of observations, while the Y axis on the left side of each view plots the metric itself. Here’s an example of Call Performance Metric Details, in which you can see from the Call Quality—Packet Loss data view that when call activity spiked at around 10 call minutes, data loss rose above 2%:



Refer to the legends for additional statistics that were calculated when analyzing data for each metric.

More information about each metric shown in the Call Performance Metric Details Report can be found in:

- "Call Quality Metrics" on page 78
- "Call Setup Metrics" on page 81
- "Video Metrics" on page 82

Note: In a few cases, older or lower-end IP phone models and "soft phones" do not support the collection of all performance statistics. For example, the Cisco Model 7902 phone only returns packets received and packets lost; therefore, the only metric NetQoS UC Monitor can report for this phone is Packet Loss.

Call Leg Details

The **Call Leg Details** link appears in the **Related Reports** area at the top of the Call Performance Overview Report. This report provides detailed data about calls that have completed. It is useful in conjunction with a drilldown view—of a Location and Sending Location, for example—to help you determine which specific calls, and which direction of each call, experienced performance problems.

While the Call Performance Overview Report rates call performance for each Location that had call activity, the Call Leg Details Report provides performance ratings per-call leg, per-metric and identifies the phone numbers of the phones within each Location. You can also use this report to find the IP address of any phone that appears as "`<Unassigned>`" in reports.

By default, the **IP Address** column and a few other columns of data are excluded from the report. Enable them in the Settings dialog box.

The following tables describe the detailed data that is available on the Call Leg Details report page. The first view is the **Performance Audio Call Leg Details** view. More information about each audio metric can be found in "Call Quality Metrics" on page 78 and "Call Setup Metrics" on page 81.

Note: If you are monitoring Microsoft Office Communications Server 2007, you will see an additional view, the Performance Video Call Leg Details view (see the separate table, below).

View	Description
Performance by All	Rollup view of call performance (call setup and call quality metrics) for all Locations or, if custom groups are defined, for all groups. Bar chart provides an indication of the times when calls were made and the quality of their performance. The Performance Call Leg Details table below then provides a per-metric, per-call breakdown of individual call performance. If you access the Call Leg Details Report from a drilldown view, a view of the selected items is shown here instead of "Performance by All".

View	Description
Performance Audio Call Leg Details	Detailed data about when calls were made, by which specific phones, identifies the Location to which each phone is assigned, and lists raw performance metrics for each call. Some columns in this view only appear if the data is not already included in the top-level view. For example, if you access the Call Leg Details Report from a drilldown view in which two Locations are selected, the **Location/Media Device** columns are only shown in the Selected Location view and are not included in the Performance Call Leg Details view.

Column	Description
Time	The time and date when the call was made.
Call IDs	The ID numbers assigned to the call by the Office Communications Server.
Number	The DN or SIP URI of the phone that received the call data. **Tip**: Check the **Number** and **Sending Number** rows for Delay to Dial Tone, Post-Dial Delay, or Call Setup Failure metrics. Only the phone that placed the call has these Call Setup metrics.
Location/Media Device	The assigned Location of the phone that received the call data. Or the hostname of the media device through which the call was sent. Could be `<Unassigned>` or another default Location. See "Call Legs and Monitoring Reports" on page 65 for an explanation.
Sending Number	The DN of the phone that sent the call data. See the **Tip** above for help with caller and called party identification.
Sending Location/Media Device	The assigned Location of the phone that sent the call data. Or the hostname of the media device that routed the call to the called party.
Duration	The length of the call, in minutes and seconds.
Call performance audio metrics: Delay to Dial Tone Post-Dial Delay MOS/Network MOS Packet Loss Jitter Buffer Loss Latency ACOM	Raw data for each metric that contributed to the call performance rating, shown in the Performance by All view (see above). A colored icon indicates the rating with respect to the relevant call setup or call quality threshold setting. Detailed information about each metric is available in: • "Call Setup Metrics" on page 81 • "Call Quality Metrics" on page 78
Call Setup Failure Code	If the call failed during the setup phase, the code that the call server returned, indicating the type of failure. See "Call Failure Cause Codes" on page 138 for more information.
Call Server	The hostname of the call server that handled the call.

Note: Some metrics are vendor-specific and are not available from all phones. Similarly, some older or lower-end IP phone models and "soft phones" do not support the collection of all performance statistics. For example, the Cisco Model 7902 phone only returns packets received and packets lost; therefore, the only metric NetQoS UC Monitor can report for this phone is Packet Loss.

Performance Video Call Leg Details

The **Performance Video Call Leg Details** view contains the following information:

Column	Description
Time	The time and date when the video call was made.
Number	The DN or SIP URI of the phone that received the call data.
Location/Media Device	The assigned Location of the phone that received the call data. Or the name of the media device through which the call was sent. Could be `<Unassigned>` or another default Location. See "Call Legs and Monitoring Reports" on page 65 for an explanation.
Sending Number	The DN or SIP URI of the phone that sent the call data.
Sending Location/Media Device	The assigned Location of the phone that sent the call data. Or the hostname of the media device that sent the call data.
Codec	The codec that was used to place the call.
Duration	The length of the call, in minutes and seconds.
Call performance video metrics: Frozen Video Video Frame Loss Video Packet Loss Video Latency	Raw data for each metric that contributed to the call performance rating, shown in the Performance by All view (see above). A colored icon indicates the rating with respect to the relevant threshold setting. For detailed information about each metric, see "Video Metrics" on page 82.
Call Server	The hostname of the call server that handled the call.

Call Types

Calls on the network may be classified according to their status at completion or according to their type. Cisco Unified Communications Manager supports many extra telephone features, such as hold, forward, and conference. When invoked by a user, each feature produces a call of a different type. The following table summarizes the call types that are monitored by UC Monitor:

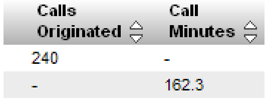
Call Type	Description
Abandoned call	Call attempt: a phone placed a call but then hung up before it was answered.
Failed call	Call attempt: a call that failed to connect during the setup phase. A call setup failure code should be reported. See "Call Failure Cause Codes" on page 138.
Call hold and resume	Calls placed on hold and then taken off hold while call conversation data resumes. ***Note:*** Placing a call on hold effectively ends a Call Watch for both phones.

Call Type	Description
Forwarded or redirected call	Calls may be forwarded automatically (that is, always), on busy, or on no answer. Calls may be forwarded to voice mail or to another phone number. An auto-attendant is often used. Cisco Unity and Unity Express provide this capability. The final destination, not the dialed destination, of the forwarded or redirected call is shown as the call leg in reports. Calls that are forwarded to voice mail can be watched using the Call Watch feature, if desired. Enter the computer telephony integration (CTI) route point port number of the auto-attendant or of the voice mail port for the DN when you set up the Call Watch. Then create a UC Monitor Location named “Voicemail” to see calls going to voice mail.
Conference call	Call that used a conference number; it appeared to be going into the conference bridge. As soon as the number of callers into the conference call is reduced to two calling parties, the call server connects them directly to each other and frees up the conference resource.
Pickup	The call is answered by a different extension than the one dialed. The extension that picks up the call receives a ringing signal based on membership in the pickup group. Similar to forwarded or redirected calls, above. The final destination, not the dialed destination, of the forwarded or redirected call is shown as the call leg in reports.
Transfer with consultation	A call is answered and then forwarded to another extension. Multiple call legs are logged: • Original call, from calling party to called party • Call from the transferring party to the transfer destination • Call from the transferred party to the transfer destination
Transfer without consultation	Also called a blind transfer. The call is not answered before it is forwarded.

UC Monitor reports show no quality statistics for call legs that terminate at a voice mail server or other device where these statistics are not available. For example, Cisco Unity and Unity Express do not report call quality statistics. In cases where calls are forwarded or transferred, reports should show the IP address or phone number of the call’s final destination, not the one originally dialed.

Observations in Call Performance Reports

UC Monitor reports provide indications of data validity by showing observation counts. As a general rule, the greater the number of observations, the higher the validity of the performance statistics being measured and rated. The observation units used for the metrics shown in Call Performance views correspond to those used in performance thresholds. The unit of observation depends on the type of metric:



Calls Originated	Call Minutes
240	-
-	162.3

Depending on whether the metric is a call setup or call quality metric, the size of the data pool is based either on the number of calls placed (calls originated) or the number of call minutes from which the performance data was taken.

The following table describes UC Monitor observation units:

Unit	Type of Metric	Description
Calls Originated	Call Setup	1 call = 1 call leg. The number of calls placed by phones at a given Location. The term **Originated** helps identify the direction of the call leg. Call setup metrics only apply to a single direction for a VoIP call. Only the applicable call legs are included in the "Calls Originated" count for call setup.
Call Minutes	Call Quality	1 call minute = 60 seconds of time that a phone was offhook and sending data. Call minutes are computed as follows: `(total seconds of all call data)/60` Normal rounding of seconds into minutes is then applied, but partial minutes are reported.

The observation units correspond to the units used in performance threshold configuration. UC Monitor Administrators can therefore set the minimum number of calls originated or call minutes that must be collected before an Incident is created by customizing threshold settings.

Observations are taken continuously and reported to the Management Console, but observed data is not immediately reflected in Call Performance reports. No data related to a given call is reported until the call ends. As soon as it ends, all data from that call is reported during the next 15-minute reporting interval. A call that lasts 40 minutes, for example, reports no data until the third reporting interval, at which point the updated Call Performance Overview Report adds the entire 40 call minutes to the total call minute observation count.

In addition to providing a gauge of statistical relevance, the number of observations can be a helpful means of judging whether relatively heavy utilization played any role in performance issues.

The topic "Call Attempts and Reporting Intervals" on page 63 contains more information about reporting intervals.

Call Setup Observations

Call setup observations are computed as **one per call** because only one call leg of the call contains the call setup data. Only calls that were originated by a Location are included in call setup measurements for that Location. The length of the call is not used to derive the value of the metric.

Note: The number of observations for the delay to dial tone metric and the post-dial delay metric may be different because calls originating from the PSTN (that is, from a voice gateway or other media device) only compute post-dial delay.

Call setup availability observations are also computed as one per call. The value for this metric is calculated as:

```
(# failed calls)/(total # of calls originated)
```

The number of call setup availability observations is equal to the total number of calls originated.

Call Quality Observations

To derive most call quality metrics, UC Monitor uses a **call minute** as the basic unit of observation. The value of each call quality metric is then calculated as a weighted average over the number of call minutes for each call that ends during the 15-minute monitoring interval. (This reporting behavior is discussed in "Call Attempts and Reporting Intervals" on page 63.) Normal rounding of seconds into minutes is also performed. For call quality metrics, each call leg contributes its metrics separately.

The following example should help to clarify the relationship between observation units and call quality metric calculation. Assume that two calls were made from A to B during a 15-minute monitoring interval: one call of nearly two minutes, and one approximately three-minute call. For the MOS metric, the following data was gathered:

Calls	MOS Value	Duration (Call Minutes)	Duration (seconds)
A -> B	3.1	2	118
A -> B	3.8	3	182

The UC Monitor calculation for MOS value is a weighted MOS for the 15-minute reporting interval that uses the actual total duration of calls in seconds. Totals for seconds are rounded to derive the totals for call minutes.

The MOS calculation would be:

```
(118*3.1) + (182*3.8) = 1057.4
 1057.4/300 seconds = 3.52
```

In this example, the MOS value would be 3.52 for the reporting interval and would be rated as Excessive (using the default threshold settings). The number of call minutes reported would be 5.

Call Quality Metrics

View call quality charts by drilling down on individual Locations, servers, or media devices shown in the Call Performance Overview report. The top-level **Performance by All** view shows ratings of the quality of call performance quality across all Locations and components. Both call quality and call setup metrics are included in this rating, as well as audio and video metrics. To see a breakdown of the various impairments that affected the quality ratings, click an individual Location. The **Narrow by Audio Metric** view provides an individual bar chart to rate each call quality and call setup metric separately.

The charts provided in the Call Performance Metric Details Report also provide separate views of the metrics relevant to call quality issues that occasionally arise in UC systems, such as packet loss.

Note: When you're monitoring voice over IP, you should try to understand the call quality data that's reported on the basis of paired network locations. Keep in mind that call quality is reported based on *listening quality*: the data used to calculate each metric is taken from the listening (incoming) direction of each bi-directional call.

The available call quality metrics are described in the following table:

Metric	Description
Mean Opinion Score (MOS)	Industry standard method for gauging call quality by estimating the impact of various impairments to the quality of the voice signal on the listener's likely perception of the call's quality. The **MOS average** is the average MOS listening quality (LQK) score observed for the entire voice stream. See Appendix A, "Calculating a Mean Opinion Score" on page 147 for more information.
Network MOS	Microsoft-only metric. MOS listening quality value based on network factors alone. See "Microsoft MOS Calculations" on page 148
Packet Loss	Expressed as a percentage of all packets in a discrete stream, describes the amount of data that is being lost—sent, but never received by the called party.
Jitter Buffer Loss	Jitter is the statistical term for variations in delay among the arrival times of packets in the same stream. Jitter buffers attempt to reduce or eliminate network jitter by caching packets. If jitter exceeds caching capacity, packets are lost; this loss is called jitter buffer loss. Each media device has a jitter buffer and reports jitter buffer loss statistics for each call based on early and late packet counts: • early packet loss: packets that arrived too quickly to be contained by the jitter buffer (also called jitter buffer underruns). • late packet loss: packets that arrived too slowly to be contained by the jitter buffer (also called jitter buffer overruns). Each IP phone or Microsoft endpoint also captures jitter buffer loss. For each phone, jitter buffer loss metrics are calculated based on the Conceal Ratio statistic and the total number of lost packets. The Conceal Ratio refers to the percentage of frames in the call data stream that were concealment frames, generated by the phones to conceal packet loss, and it includes both early and late packets.
Latency	One-way delay, calculated from the calling party to the called party. Includes: • propagation delay—delay produced by the physical distance traveled on the line • network delay—transport delay, produced by intervening network equipment, such as routers and switches • packetization delay—delay introduced by the codec Latency has a severe effect on VoIP call quality.

Metric	Description
ACOM	Sum of the following values recorded for a VoIP phone call: • Echo Return Loss (ERL) — The reduction in the echo level produced in the circuit without an echo canceller. • Cancellation loss, or Echo Return Loss Enhancement (ERLE) — An enhancement in the echo return loss, produced by an echo canceller. • Nonlinear processing loss Because it includes echo reduction that occurs without the activity of an echo cancellation device and also any echo reduction attributable to an echo cancellation device, ACOM is the total echo return loss seen by the network. Echo cancellation is the removal, by an echo canceller, of the echo portion of a VoIP call signal as it exits the tail circuit and heads into the WAN. This metric only applies to calls that pass through voice gateway devices.

See "Calculating a Mean Opinion Score" on page 147 for more information about the MOS metric. Where the MOS value includes the impact of the quality of the audio signal in addition to network impairments on the perceptual call quality, the Network MOS statistic only considers network factors. It therefore serves as a good means of isolating poor call performance to network conditions. Each codec has a maximum possible Network MOS that represents the best possible MOS value under ideal network conditions.

Depending on the equipment being monitored and the devices that handled the call, the Call Watch Details report may contain the following additional call quality metrics:

Metric	Description
Jitter	The average jitter (variation in delay times among packets in the same stream), measured for each call leg. Maximum jitter values are graphed as data points and indicated on the right Y axis.
Concealed seconds	Number of call seconds that had concealment events (due to lost frames) from the start of the voice stream. **IP phone calls only**.
Severely concealed seconds	Number of call seconds that had more than 5% concealment events from the start of the audio stream. **IP phone calls only**.
ERL	Echo Return Loss (ERL) — Reduction in the echo level produced in the circuit without an echo canceller. The degree or amount of loss reflects the volume of the echo that remains. Like ACOM, a measurement of how significantly echo was reduced. **PSTN calls only**.
Signal In	Signal level of the data flow traveling into the echo canceller. **PSTN calls only**.
Signal Out	Signal level of the data flow traveling out of the echo canceller toward the IP network. **PSTN calls only**.

Call Setup Metrics

View call setup performance statistics by drilling down on individual Locations, call servers, or media devices shown in the Call Performance Overview Report. The top-level **Performance by All** view shows ratings of overall call performance, which includes both call setup and call quality metrics and audio as well as video. Drill down into an individual Location, call server, or media device to see the individual call setup and call quality metrics. The **Narrow by Audio Metric** view provides an individual bar chart to rate each call quality and call setup metric separately.

The charts provided in the Metric Details Report also provide separate views of call setup delay and other metrics relevant to call setup issues that occasionally arise in VoIP or UC systems, such as failed calls.

The available call setup metrics are described in the following table:

Metric	Description
Call Failures	Calls that failed to connect during the setup phase; failed calls. Expressed as a percentage of all calls attempted during the monitoring interval.
Call Setup Failure Code	If the call failed during the setup phase, the code that the call server returned, indicating the type of failure. See "Call Failure Cause Codes" on page 138 for more information.
Delay to Dial Tone	For a user, the amount of time it takes to hear a dial tone after picking up the receiver of an IP phone. For the IP phone itself, the amount of time (or delay) measured between the following: • off-hook event sent from the IP phone to its call server • dial tone indication received from the call server A measurement of call server (or network) response time, or of how long it takes to receive a response from the call server for the phone to provide a dial tone.
Post-Dial Delay	The time between entering the last digit of a telephone number and receiving a ring tone or call connect.

The term *call setup* refers to a series of connections that occur between a phone trying to place a VoIP call and the active call server. The call server is responsible for certain signaling to the phone that allows it to play a dial tone and place the call; it also establishes a connection to the called IP phone or voice gateway device (if the called party is in the PSTN). The call setup protocol (either SIP, H.323, MGCP, or SCCP) defines the messages that are passed among the call server, gateway, and phones.

VoIP technology experts recognize the "call setup delay" metric as one of the call setup metrics most relevant to user quality of experience. It is commonly defined as the time interval measured from the moment the user initiates a connection request until the calling party receives the message indicating the call status.

Within the call setup delay time interval, the time measured between the phone's being taken offhook and the start of the dial tone is called the *delay to dial tone*. During the call setup phase of a VoIP phone call, the phone receives certain messages from the call server to play a dial tone. If these messages are delayed, the user may think that the phone system is not working because the dial tone is slow to sound. This delay should be minimized to prevent the user from assuming that the call has failed and redialing or hanging up.

The next key event in the call setup phase occurs when the number is dialed. The dialing of the phone number initiates an exchange of messages to locate the called party and ring the correct phone. The time between dialing the number and the start of the phone's ringing is known as *post-dial delay*.

Video Metrics

Ensuring user Quality of Experience is immensely challenging for video applications. For one thing, it's hard to measure your success in delivering high-quality video. There's not a widely accepted video quality standard equivalent to the MOS for audio. Video quality is even more subjective than audio quality, and it's also a lot more complicated to implement.

You can view video metric data in charts by drilling down on individual Locations, call servers, or media devices shown in the Call Performance Overview report. The top-level **Performance by All** view shows ratings of overall VoIP and video quality across all Locations and components. All the monitored audio and video metrics are included in this rating. To see a breakdown of the various impairments that affected the quality ratings, click an individual Location. The **Narrow by Video Metric** view provides an individual bar chart to rate each video quality metric.

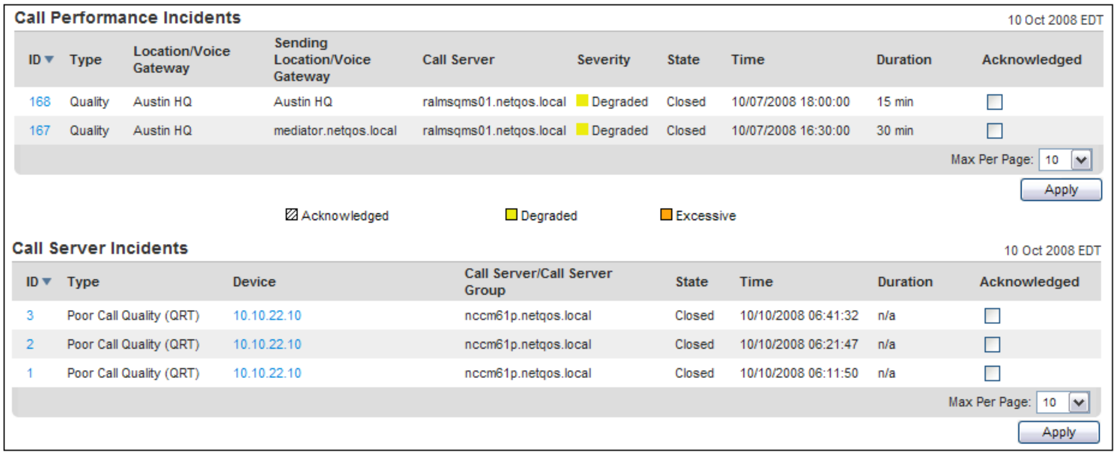
Note: Video metrics are only available if you are monitoring Microsoft Enterprise Voice.

The available video metrics are described in the following table:

Metric	Description
Video Latency	Delay, or the maximum time taken for a video packet to travel between the calling parties, measured from end to end in a single direction by dividing the Microsoft `RoundTrip` delay metric in half. The `RoundTrip` delay is the average round-trip time for a call leg in a given video call.
Video Packet Loss	Average network packet loss for the entire stream.
Video Frame Loss	Average number of unique consecutive images, or video frames, lost due to corruption and error concealment for the entire stream. Video frames can span multiple packets, so this threshold is useful in conjunction with the video packet loss threshold.
Frozen Video	The frequency of long and noticeable frozen video for the whole session.

Incident Overview Report

The Incident Overview Report shows information about Incidents that were raised in response to threshold violations. The overview provides a list of recent Incidents, with some basic information about when the Incident was reported and which network locations were affected.



Call Performance Incidents 10 Oct 2008 EDT

ID ▼	Type	Location/Voice Gateway	Sending Location/Voice Gateway	Call Server	Severity	State	Time	Duration	Acknowledged
168	Quality	Austin HQ	Austin HQ	ralmsqms01.netqos.local	🟨 Degraded	Closed	10/07/2008 18:00:00	15 min	□
167	Quality	Austin HQ	mediator.netqos.local	ralmsqms01.netqos.local	🟨 Degraded	Closed	10/07/2008 16:30:00	30 min	□

Max Per Page: 10

Apply

▨ Acknowledged 🟨 Degraded 🟧 Excessive

Call Server Incidents 10 Oct 2008 EDT

ID ▼	Type	Device	Call Server/Call Server Group	State	Time	Duration	Acknowledged
3	Poor Call Quality (QRT)	10.10.22.10	nccm61p.netqos.local	Closed	10/10/2008 06:41:32	n/a	□
2	Poor Call Quality (QRT)	10.10.22.10	nccm61p.netqos.local	Closed	10/10/2008 06:21:47	n/a	□
1	Poor Call Quality (QRT)	10.10.22.10	nccm61p.netqos.local	Closed	10/10/2008 06:11:50	n/a	□

Max Per Page: 10

Apply

The Incident Overview Report is useful for network operators and engineers who need to know whether troublesome network conditions exist, whether call servers have experienced a failover, or whether unauthorized devices have accessed the network. Network personnel can also use this report to quickly gain access to more information about a recent Incident. Details about any particular Incident are available from the tables in the Incident Overview Report by clicking the Incident **ID** number link.

The Incident Overview report provides a filtering feature to help you sift through multiple Incident reports. Filtering options are available next to the Settings section at the top of the report page. If you have defined custom groups, filtering is available by group.

The report provides two Incident list views:

- "Call Performance Incidents Table"
- "Call Server Incidents Table"

The two types of Incident are handled slightly differently. For example, the call performance Incidents receive a severity rating, while the call server Incidents do not.

Note: Call server Incidents are only reported for Cisco call servers.

Call Performance Incidents Table

The Call Performance Incidents table provides the following basic information about each Call Setup and Call Quality Incident. Detailed information is available when you click the hyperlinked Incident IDs:

Column	Description
ID	The sequential number assigned to this Incident, and a link to more information about it. See "Incident Details" on page 86.
Type	The type of Incident: either **Quality** (call quality) or **Setup** (call setup).

Column	Description
Location/Media Device	The Location of the phone that reported the Incident, or the hostname of the voice gateway or other media device that sent the call from the PSTN, if applicable. The metrics were taken from the call leg that was traveling toward it.
Sending Location/Media Device	The Location of the phone that sent the call leg that triggered the Incident, or if the call involved the PSTN, the hostname of the gateway media device.
Call Server	The call server that handled the call that triggered the Incident.
Severity	The severity of the Incident: either **Degraded** or **Excessive**.
State	The status of the Incident: **Open** or **Closed**.
Time	The date and time of day when the Incident was reported.
Duration	The length of time that the performance condition persisted.

Call Server Incidents Table

The Call Server Incidents table provides basic information about each of the call server Incident types. The different types of call server Incident apply either to individual call servers or to call server groups:

- **Call Server**—Registration Failures; Poor Call Quality
- **Call Server Group**—Phone Status Changes

The following information is provided in the Call Server Incidents table. Detailed information is available when you click the hyperlinked Incident IDs:

Column	Description
ID	The sequential number assigned to this call server Incident. A link to more information about this Incident. See "Call Server Incident Details" on page 86 for more information.
Type	The type of Incident: either **Registration Failures**, **Poor Call Quality (QRT)**, or **Phone Status Changes**. ***Note:*** The Phone Status Changes type includes information about **Currently Missing Phones**, **Recently Moved Phones**, and **New or Found Phones**.
Device	The IP address of the phone or media device that reported the Incident to the call server. For IP phones, a hyperlink to the phone Web page. For a call server group Incident, shows the ID of the call server group, or "n/a".
Call Server/Call Server Group	The hostname or IP address of the call server, or the name of the call server group (usually representing a call server cluster) that reported the metrics that triggered the Incident.
State	The status of the Incident: **Open** or **Closed**.
Time	The date and time of day when the Incident was reported.
Duration	The length of time that the performance condition persisted. Not applicable for some Incident types (shows "n/a").

The final columns in each Incidents table provides **acknowledgment** check boxes; click to select the check box next to any Incident that you want to acknowledge and click **Apply**. If an Incident has already been acknowledged, the box is checked. The severity icon for an acknowledged Incident, if applicable, appears shaded, both in the Incident Overview Report and in Call Performance views of the affected Locations and metrics.

Note: Acknowledging an Incident is a way to let other UC Monitor operators know that you are aware of the performance condition associated with it.

For more information about how Incidents are reported and how they automatically open and close, see "More about UC Monitor Incident Reporting" on page 95.

Incident Report Settings

The Incident Overview Report offers two methods for narrowing the scope of the data that's displayed. To help you quickly find a particular Incident report, three filtering options are available just above the Incidents list. These options let you filter the Incidents in the list:

Setting	Description
Incident State	The state, or status, of the Incidents you want to see: either **Open**, **Closed**, or **Open and Closed** (all Incidents). Filters out all Incidents that are not of the selected state.
Minimum Severity	The minimum severity of the Incidents you want to see, either: • **Degraded** — Shows all Incidents, Degraded and Excessive, or • **Severe —** Shows only Excessive Incidents.
Minimum Duration	The minimum amount of time that the Incident remained open. Duration does not apply to some Poor Call Quality call server Incidents. If the QRT softkey was pressed while the call was in progress, the Incident is considered to be instantaneous. Select the **All** option for the duration to see these Incidents.

In addition to these quick filtering options, the Settings dialog box provides more filtering and display options. Click the **Settings** link. To change any report settings, or to set filters to change the data views, click to select or clear the check box next to each option. Options on the left side of the dialog box mimic the drilldown paths available from the report data.

Quick filtering options are associated with your user account and persist across login sessions.

Incident Details

The detailed reports for individual Incidents show details of the related performance degradation, with bar charts that break out the performance listeners experienced in each direction of the degraded calls. The information included in the detailed report is already narrowed to show the affected Location or pair of Locations and a media device or call server.

Three views are provided on the Incident Details page:

Incident Details

Provides Incident summary information, which is described in "Incident Overview Report" on page 83.

Performance by Location

Provides bar charts that illustrate call performance broken out by the Locations of the calling and called parties and that of the call server or media device involved in the poorly performing calls. The Call Performance category includes averages of all the call setup and call quality data that contributed to this Incident. Bar charts are aligned over a single time frame indicator to help you compare performance ratings. The actual time that the Incident report was created is shown below the bar charts, where an Incident icon marks the time in question.

If you have defined custom groups in the NetQoS Performance Center, the applicable group and any subgroups for the selected Incident are indicated, with indentation to indicate group hierarchy. The final nested item is the call server.

Performance by Metric

Provides bar charts that illustrate how data was rated for each call performance metric, where applicable. For example, if no PSTN calls contributed to the Incident, no ACOM metric is applicable.

Details for each metric are available if you click the **Metric Details** link in the Related Reports section at the top of the report page.

See "Viewing Incident Details" on page 45 for more information about this page.

Call Server Incident Details

The following tables describe the detailed information provided in the Call Server Incident Details Report:

Call Server Incident Details Table

Note: This is a comprehensive list; not all fields apply to every type of call server or call server group Incident.

Item	Description
ID	The identifier, assigned by NetQoS UC Monitor, for the selected call server Incident. Matches the ID in the Incident Details Overview summary table.
Device	The phone that is being reported as missing, moved, or new.
Phone Number	The phone number of the phone involved in the Incident. For Poor Call Quality (QRT) Incidents, the phone where the QRT softkey was pressed.

Item	Description
Name	The name of the affected phone.
IP Address	The IP address of the affected phone.
Location/Current Location	The Location definition associated with the phone's current subnet.
Call Server/Call Server Group	The hostname of the call server, or the name of the call server group (usually representing a call server cluster) that reported the metrics that triggered the Incident.
Protocol	The protocol being used by the call server for call setup signaling.
Trigger	The type of the trigger for this Incident. For Poor Call Quality (QRT), either: • In Progress—The QRT softkey was pressed while the call was active, or • On Hook—The QRT softkey was pressed while the phone was on hook (usually after the call had been completed).
Time or Time Frame	The specific time when, or the range of times within which, the Incident was reported. For Poort Call Quality (QRT), the time when a user pressed the **QRT** button.
Type	The type of call server Incident, one of the following: • Registration Failures • Poor Call Quality (QRT) • Phone Status Changes (includes Currently Missing Phones, Recently Moved Phones, or New/Found Phones)
QRT Count Registration Failures	The number of times the applicable behavior occurred to trigger the Incident. ***Note:*** Does not affect the number of Incident reports for the same phone - call server combination. For example, even if the phone in question had 15 registration failures, the Incident is only reported once.
Acknowledged	Whether the Incident has been acknowledged (Yes or No).
Duration	The length of time that the condition persisted, in minutes and seconds.
Status	The status of the Incident: Open or Closed.

See the following topics for specific information about the detailed report for each call server Incident type:

- "Phone Status Changes Incident Details" on page 88
- "Poor Call Quality (QRT) Incident Details" on page 91
- "Registration Failures Incident Details" on page 92

Phone Status Changes Incident Details

The detailed information provided for a call server Incident of the type **Phone Status Changes** describes changes to the devices registered to call servers in the call server group where the Incident was reported. This type of Incident can indicate a failover situation, where a call server within a call server group has become unreachable.

The detailed report includes the following tables:

- Currently Missing Phones Table—Contains information about phones whose call server registration status is unknown and that are considered missing
- Recently Moved Phones Table—Contains information about any phones that registered to different call servers during this reporting interval.
- New/Found Phones Table—Contains information about any phones that are currently registered with the call server group but that weren't registered during the last reporting interval.
- Phone Status Changes Table—Summarizes changes from the other tables and provides totals.

The reporting interval is 15 minutes; however, a device is considered "missing" if the Collector has not observed any keepalive traffic from it for any period of five minutes. If the five-minute period falls within the reporting interval, the phone appears in the "New/Found Phones" table.

Refer to "Call Server Incident Details" on page 86 for descriptions of the items in the Call Server Incident Details table.

Currently Missing Phones Table

The **Currently Missing Phones** table lists all IP phones that were previously known to the servers in the call server group that reported the Incident, but that, during the last 15-minute reporting interval, were no longer sending keepalive messages to these servers. Any phones that had normal shutdowns (and accompanying deregistrations) are excluded from this list; they are not considered "missing."

The following table describes the information provided in the Currently Missing Phones table:

Item	Description
Device	The IP address of the phone that is being reported as missing.
Phone Number	The phone number of the phone that is being reported as missing.
Name	The name of the missing phone.
Location	The Location definition associated with the phone's last known subnet.
Previous Call Server	The hostname and IP address of the call server where the phone was previously registered.
Time	The 15-minute reporting interval (date and time range) when the phone lost contact.

Recently Moved Phones Table

The **Recently Moved Phones** table lists all IP phones that registered to a different call server within the indicated call server group during the specified 15-minute reporting interval.

Item	Description
Device	The IP address of the phone that is being reported as moved.
Phone Number	The phone number (DN) of a phone that has moved to a different call server.
Name	The name of the phone that has moved.
Location	The Location definition associated with the phone's current subnet.
Previous Call Server	The hostname and IP address of the call server where the phone was previously registered.
Current Call Server	The hostname and IP address of the call server where the indicated phone was registered during the specified 15-minute reporting interval.
Time	The 15-minute reporting interval (date and time range) when the phone changed call servers.

New/Found Phones Table

The **New/Found Phones** table lists all IP phones that appeared to be newly registered or re-registered to a monitored call server group during the specified 15-minute reporting interval.

- A "new" phone has never registered to this call server group since monitoring with NetQoS UC Monitor began.
- A "found" phone has lost contact with this call server group at some point in the past, but in the specified reporting interval, it registered again with the same group.

Item	Description
Device	The IP address of the phone that is being reported as new or as found.
Phone Number	The phone number (DN) of a phone that registered to the call server during the specified reporting interval.
Name	The name of the new or found phone.
Location	The Location definition associated with the phone's current subnet.
Previous Call Server	If applicable, the hostname and IP address of the call server where the phone was registered in previous reporting intervals.
Current Call Server	The hostname and IP address of the call server where the new (or found) phone was registered during the specified interval.
Time	The 15-minute reporting interval (date and time range).

Phone Status Changes Table

The **Phone Status Changes** table summarizes the per-interval totals of changes to IP phone registration status for the call server group where the Incident was reported over the entire duration of the Incident (open to close).

Each row in the table shows the status changes that were reported for a specified reporting interval, which is shown in the last column. As you read the data in each row from left to right, the resulting statement is something like the following:

“During the specified reporting interval, there were X active phones for this call server group. Y of these phones were new, or were found during the interval. Z of these phones lost contact with all call servers in the group during the interval. And U of these devices moved from one call server to another during the interval. Therefore, the percentage of device status changes for that interval is calculated as (Y + Z + U)/X”.

Note: If you compare the Incident duration shown in the **Time Frame** field in the Call Server Incident Details view, you can see that the table includes rows for short time periods before and after the Incident was opened and closed. These are included to help you see any changes that might have been occurring before the threshold was crossed and after the Incident was closed.

The following call server group totals are included in the Phone Status Changes table:

Item	Description
Active Phones	The total number of phones that were either “active” (that is, in an active contact status with any of the call servers in the call server group) at the beginning of the specified reporting interval or that were new or found during the interval.
New/Found Phones	The total number of phones that were registered to the servers in the call server group during the specified reporting interval, but that either: • had never registered to this call server group before (new); or • lost contact with this call server group at some point in the past, and registered to this group again during this interval (found).
Missing Phones	The total number of phones that were previously registered to the servers in the call server group but that, during the specified reporting interval, were no longer sending keepalive messages to these servers. Does not include phones that had normal shutdowns.
Moved Phones	The total number of phones that appeared to be registered to a different call server in this group during the specified reporting interval.
Time	The 15-minute reporting interval (date and time range).

Poor Call Quality (QRT) Incident Details

The detailed information provided for a call server Incident of the type **Poor Call Quality (QRT)** includes information about the Incident itself, about the phones involved in the call where the Incident was reported, and about the data used in calculating actual quality metrics.

Refer to "Call Server Incident Details" on page 86 for descriptions of the items in the Call Server Incident Details table.

Origination and Destination Phone Information Tables

Tables of information about the two phones involed in the call where a poor call quality (QRT) call server Incident was reported are included in the Incident Details report. The phone where the QRT softkey was pressed is indicated in the **Call Leg Details** table described below. The following information is included in the tables of information about the origination and destination phones:

Table	Description
Origination Phone Information	If available, detailed information about the phone or endpoint that placed the call for which the poor quality was reported, including the phone number, IP address, the phone port through which the data passed, the phone make and model, call server, codec, firmware version, serial number, and connection information. Where provided, the **IP address** is a hyperlink to the phone's Web page. If the call involved a phone in the PSTN, provides information about the gateway media device that handled the call, including the interface and voice channel through which the data passed. Availability of this information depends on the type of phone, endpoint, or gateway.
Destination Phone Information	If available, detailed information about the phone that placed the call for which the poor quality was reported, including the phone number, IP address, the phone port through which the data passed, the phone make and model, call server, codec, firmware version, serial number, and connection information. Where provided, the **IP address** is a hyperlink to the phone's Web page. If the call involved a phone in the PSTN, provides information about the gateway media device that handled the call, including the interface and voice channel through which the data passed. Availability of this information depends on the type of phone, endpoint, or gateway.

Call Leg Details Table

The following table of information is also included in the report for a poor call quality (QRT) call server Incident:

Column	Description
Call ID	The call identifier, assigned by NetQoS UC Monitor, for the selected call. Matches the ID in the Calls Overview Report summary table.
Origination Time	The time the call began.
Receiving Phone	The phone number where the call data being rated was received. (Call quality is rated from the listener's perspective.)
Sending Phone	The phone number of the phone that sent the call data.

Column	Description
QRT	Whether this phone was the source of the QRT report (yes or no).
Delay to Dial Tone	For a user, the amount of time it takes to hear a dial tone after picking up the receiver of an IP phone, in milliseconds. For more information, see "Call Setup Metrics" on page 81.
Post Dial Delay	The time between entering the last digit of a telephone number and receiving a ring tone or call connect, in milliseconds.
MOS	The average MOS listening quality (LQK) score observed for the entire voice stream. See "Calculating a Mean Opinion Score" on page 147 for more information.

Below the **Call Leg Details** table on the Poor Call Quality (QRT) Incident Details page are call quality **metric details** data views. It's a good idea to examine the actual reported quality metrics provided here to help determine why the user initiated the QRT poor-quality reporting action.

- For an explanation of how the metric details views are presented in UC Monitor reports, see "Incident Metric Details" on page 93.
- For an explanation of the types of data graphed in each view, see "Call Quality Metrics" on page 78.

Registration Failures Incident Details

The detailed information provided for a call server Incident of the type **Registration Failures** includes information about the devices that attempted to register with the call servers where the Incident was reported and the times when the registration failures occurred.

A registration failures call server Incident is triggered if the number of times that a device attempts unsuccessfully to register with a call server exceeds the configured threshold. By default, the threshold is 15 registration failures per device, per reporting interval.

This type of Incident can indicate a configuration or security problem. Check the Call Performance Incidents table in this report for call setup failure Incidents. This step may help you locate a call server issue.

Refer to "Call Server Incident Details" on page 86 for descriptions of the items in the Call Server Incident Details table.

The Call Server Incident Details table for the **Registration Failures** call server Incident type contains the following information:

Item	Description
ID	The identifier, assigned by NetQoS UC Monitor, for the selected call server Incident. Matches the ID in the Incident Details Overview summary table.
Phone Number	The phone number of a phone that has registration failures on the call server.
Name	The name of the phone.
IP Address	The IP address of the phone that is reporting registration failures.
Current Location	The Location definition associated with the phone's current subnet.

Item	Description
Call Server	The hostname and IP address of the call server where the indicated phone is trying to register.
Protocol	The protocol that the call server is using for call setup.
Time Frame	The date and time frame when the Incident was reported.
Type	The type of call server Incident (Registration Failures).
Registration Failures	The number of times the indicated phone attempted unsuccessfully to register with the call server during the interval when the Incident was reported.
Acknowledged	Whether the Incident has been acknowledged (Yes or No).
Status	The status of the Incident: Open or Closed.

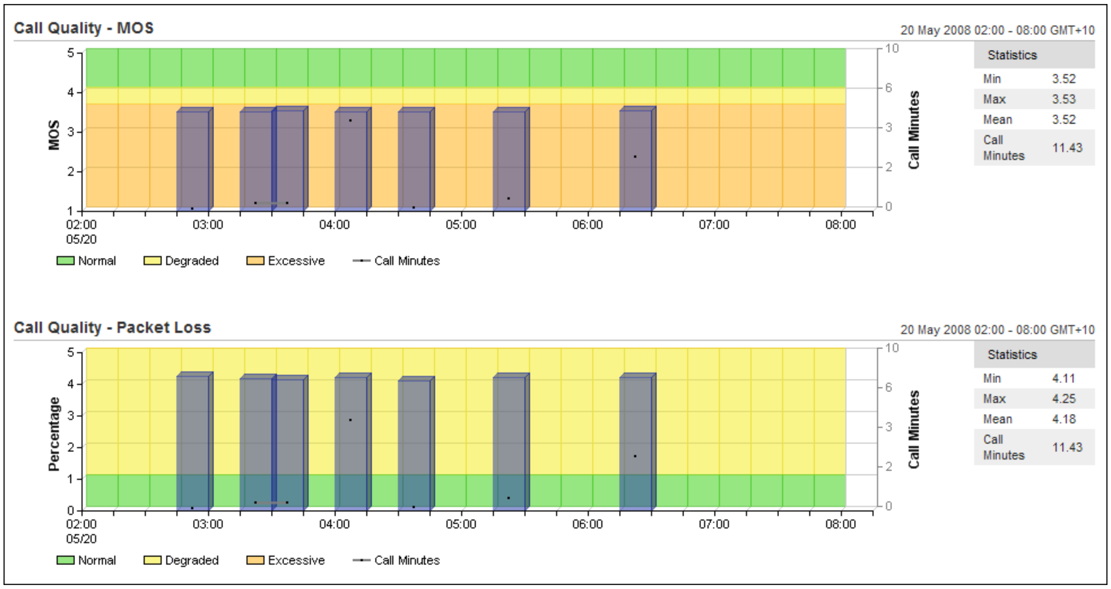
Incident Metric Details

The **Metric Details** link at the top of the Incident Details Report enables you to see detailed charts of the collected data for each performance metric that contributed to the selected Incident.

In the Incident Metric Details data views, collected data is graphed over an X axis showing the time frame and a background that uses green, yellow, and orange to show how the data compared to the thresholds for expected normal, Degraded, and Excessive (excessively degraded) performance.

A gray line graphs the number of observations that were used in the ratings: either calls (originated calls) or call minutes. The total number of observations is shown in the legend for each data view. See "Observations in Call Performance Reports" on page 76 for more information. A logarithmic scale on the right Y axis shows the number of observations, while the Y axis on the left side of each view plots the metric itself. The legends also report other statistics calculated for each rated metric.

Here's an example in which packet loss that crossed the Degraded threshold contributed to MOS values that reached the Excessive threshold:



Statistics	
Min	3.52
Max	3.53
Mean	3.52
Call Minutes	11.43

Statistics	
Min	4.11
Max	4.25
Mean	4.18
Call Minutes	11.43

More information about each metric shown in the Incident Metric Details Report can be found in the following topics:

- "Call Quality Metrics" on page 78
- "Call Setup Metrics" on page 81
- "Video Metrics" on page 82

Incident Call Leg Details

The **Call Leg Details** link appears in the **Related Reports** area when you select an Incident report for viewing. This report provides detailed data about poorly performing calls. It is useful for helping you determine which specific calls, and which direction of each call, experienced performance problems. Incident-specific information from the Incident Details Report is included.

Where the Incident Overview Report rates call performance for each *Location* or *media device* that had degraded or excessively degraded performance, the Incident Call Leg Details Report provides performance ratings *per-call*, *per-metric*, and identifies the phone numbers of the phones within each Location.

Note: For a report that provides the IP address that corresponds to a given DN, access the Call Leg Details Report from the main Call Performance Overview. You can use this report to find the IP address of any phone that appears as "`<Unassigned>`" in reports.

The following table describes the detailed data that is available in the Incident Call Leg Details report. The top view, Incident Details, contains fields that are fully described in "Incident Details" on page 86. More information about each performance metric can be found in "Call Quality Metrics" on page 78 and "Call Setup Metrics" on page 81.

Column Title	Description
Time	The time and date when the call was made.
Number	The DN of the phone that received the poorly performing call data. **Tip**: The presence of Call Setup metrics for a number indicates the phone that placed the call. Call Setup metrics apply to the calling party only.
Sending Number	The DN of the phone that sent the poorly performing call data.
Duration	The length of the degraded or excessive performance, in minutes and seconds.
Call performance metrics: Delay to Dial Tone Post-Dial Delay MOS Packet Loss Jitter Buffer Loss Latency ACOM	Raw data for each metric that contributed to the call performance rating. Metrics with the worst ratings are listed first. A colored icon indicates the rating with respect to the relevant call setup or call quality threshold setting. Detailed information about each metric is available in: • Call Quality Metrics • Call Setup Metrics

Column Title	Description
Call Setup Failure Code	If the call failed during the setup phase, the code that the call server returned, indicating the type of failure. See "Call Failure Cause Codes" on page 138 for more information.

From the Incident Call Leg Details Report, you can then view the Incident Metric Details, with more detailed information about the data that triggered the Incident. And if any associated Investigations were triggered by the selected Incident, you can quickly access the Traceroute Investigation Details Report.

More about UC Monitor Incident Reporting

UC Monitor creates an Incident when it detects a performance condition on the network that exceeds a threshold. Thresholds include a component that limits Incident creation by specifying a minimum number of observations that must be reported before the threshold is considered to have been breached. Therefore, in most cases, an Incident represents multiple instances of poor or extremely poor call performance. For more information about thresholds, see "Understanding PerformanceThresholds" on page 31.

An Incident remains available in the Incident Overview report until it is closed. Incidents are closed as soon as:

- they have been open for 24 hours.

  At the 24-hour time limit, if the problem is still occurring, 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; it starts at the beginning of an hour and ends at the beginning of the next hour.

The reports for individual Incidents show details of the related performance degradation, and have a maximum time window of 24 hours. You can shift that window forward or backward in time, using the Time Period selector. You can also view Incident reports within any time frame where they were active. Historical Incident records are stored as long as interval data is stored. An Administrator can configure the retention period in the Database Administration pages.

Incidents are reported for pairs of reporting components. Because the call quality experienced by a user occurs between pairs of network endpoints, call quality thresholds are assigned to pairs that consist of two Locations, two media devices, or a Location and a media device. Call setup thresholds are assigned to single network entities, but call setup Incidents are reported for pairs of affected Locations and call servers or media devices. See the chapter of the *UC Monitor Administrator Guide* that explains data management for a full discussion.

A set of consecutive Incidents might represent a single extended degraded state. Depending on the type of metrics, excessive or degraded statistics will trigger either a call quality Incident or a call setup Incident. There will never be more than one Incident open at a time for any unique call quality or call setup pair. If an Incident is already open for a pair, the Incident is updated with the time of the new observation, which allows it to be closed according to the logic described above.

It's possible to 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 (indicated with gray shading in Incident reports). Configure an SNMP trap notification with Severity Updates enabled to be notified when this occurs. See the *UC Monitor Administrator Guide* for more information.

Collector Incidents

The Collector Incidents table provides basic information about each of the Collector Incident types. Collector Incidents report problems that are local to a specific Collector. They are useful for detecting and troubleshooting problems with SPAN port configuration that can impede monitoring of your UC system and for alerting you to any Collector performance issues.

Note: Collector Incidents are not reported for OCS Collectors that monitor Microsoft UC deployments.

During the early phase of NetQoS UC Monitor deployment, you should plan to check the Collector Incidents page regularly to ensure that SPAN ports are configured correctly and that the Collectors in your system are performing as expected.

To help you quickly find a particular Collector Incident report, two "quick-filtering" options are available just above the Collector Incidents list. These options let you filter the list:

Setting	Description
Incident State	The state, or status, of the Collector Incidents you want to see: either **Open**, **Closed**, or **Open and Closed** (all Collector Incidents). Filters out all Incidents that are not of the selected state.
Minimum Duration	The minimum amount of time that the Collector Incident remained open. Duration does not apply to Abnormal Termination Incidents, which are instantaneous. Select either **15 minutes** or **Any** to see these Incidents in the list.

The following information is provided in the Collector Incidents table. Detailed information is available when you click the hyperlinked Incident IDs:

Column	Description
Incident ID	The sequential number assigned to this Collector Incident. A link to more information about this Incident. See "Collector Incident Details" on page 97 for more information.

Column	Description
Type	The type of Collector Incident. Corresponds to the Collector threshold that was exceeded. One of the following: • **Abnormal Termination**—Indicates that a service on the Collector has logged a fatal exception. The path to the Collector "crash dump" log file is provided. • **Discarded Packets**—The threshold for the maximum percentage of packets passing through the SPAN port that can be intentionally discarded by the Collector was exceeded. Usually caused by traffic bursts. See the UC Monitor Release Notes for information about scalability and hardware requirements. • **Duplicate Packets**—The threshold for the maximum percentage of traffic observed by the Collector that can be composed of duplicate packets was exceeded. Usually indicates a SPAN port issue. • **Lost Bytes**—The threshold for the maximum percentage of traffic that can be lost by the Collector was exceeded. Usually caused by traffic bursts. See the UC Monitor Release Notes for information about scalability and hardware requirements. See the online Help for information about the Collector Threshold settings.
Collector	The Collector where the Collector Incident was reported.
State	The status of the Incident: Open or Closed.
Time	The date and time of day when the Incident was reported.
Duration	The length of time that the performance condition persisted.

The final column in the Collector Incidents table provides acknowledgment check boxes; click to select the check box next to any Incident that you want to acknowledge and click **Apply**. If a Collector Incident has already been acknowledged, the box is checked.

Note: Acknowledging a Collector Incident is a way to let other UC Monitor operators know that you are aware of the condition associated with it.

Collector Incident Details

The following tables describe the detailed information provided in the Collector Incident Details Report. A summary table provides basic information about the Incident. Each type of Collector Incident also includes a separate Metric Details view with Incident-specific information.

Item	Description
ID	The identifier, assigned by NetQoS UC Monitor, for the selected Collector Incident. Matches the ID in the Collector Incidents summary table.
Collector	The IP address of the Collector where the Incident was reported.
Time Frame	The specific time when, or the range of times within which, the Incident was reported.

Item	Description
Type	The type of Collector Incident. One of the following: • Abnormal Termination • Discarded Packets • Duplicate Packets • Lost Bytes
Acknowledged	Whether the Incident has been acknowledged (Yes or No).
State	The status of the Incident: Open or Closed.

Abnormal Termination Metric Details

The following additional information is included in the Detailed report for an Abnormal Termination Collector Incident:

Item	Description
Dump file on Collector	The filename and path to a crash dump file that was created automatically in response to the Collector service fatal exception event.
Packet capture on Collector	If available, the filename and path to a packet capture file that was created automatically in response to the Collector service fatal exception event.

Discarded Packets Metric Details

The following additional information is included in the Detailed report for a Discarded Packets Collector Incident:

Item	Description
Total Number of Packets	The total number of packets processed by the Collector during the reporting interval when the Incident was triggered.
Discarded Packets (%)	The amount of data that the Collector discarded, expressed as a percentage of all packets processed during the reporting interval. Packets are usually discarded due to traffic bursts that exceed UC Monitor capacity for analysis given the current configuration. Packets are dropped when they arrive for processing but the Collector is too busy to receive them.

Duplicate Packets Metric Details

The following additional information is included in the detailed report for a Duplicate Packets Collector Incident:

Item	Description
Total Number of Packets	The total number of packets processed by the Collector during the reporting interval when the Incident was triggered.

Item	Description
Duplicate Packets (%)	The amount of data that the Collector treated as duplicated, expressed as a percentage of all packets processed during the reporting interval. Packet duplication is generally caused by a problem at the monitored switch SPAN port. Duplication can occur due to a SPAN misconfiguration that causes packets to be sent to the Collector twice. Duplicate packets may also indicate network problems. They may have been retransmitted when a response to a previous transmission was not received in time.

Lost Bytes Metric Details

The following additional information is included in the detailed report for a Lost Bytes Collector Incident:

Item	Description
Total Number of Bytes	The total number of bytes processed by the Collector during the reporting interval when the Incident was triggered.
Lost Bytes (%)	The amount of data that the Collector recorded as lost, expressed as a percentage of all bytes processed during the reporting interval. Bytes of data are usually lost due to traffic bursts that exceed UC Monitor capacity for analysis given the current configuration. Some messages are too big to fit in one packet and must be split into separate packets. Packets can also arrive out of order. To handle these situations, the Collector contains a re-assembly engine that re-orders and re-assembles packets using their sequence numbers. During this processing, if the sequence numbers indicate that expected data has not been received, the bytes not received are counted as lost. A high number of lost bytes usually indicates a "one-way" spanning problem. Because the Collector is only seeing the packets from one side of a conversation, it will count the data flowing in the other direction as being lost because it cannot see it.

Collector Incident Report Settings

The Collector Incident Report offers two parameters for narrowing the scope of the data that's displayed. To help you quickly find a particular Collector Incident report, two quick-filtering options are available just above the Incidents list. These options let you filter the Incidents in the list:

Setting	Description
Incident State	The state, or status, of the Collector Incidents you want to see in the list: either **Open**, **Closed**, or **Open and Closed** (all Incidents). Filters out all Incidents that are not of the selected state. Default is **Open and Closed**.
Minimum Duration	The minimum amount of time that the Incident remained open. Default is **Any**.

Quick filtering options are associated with your user account and persist across login sessions.

Investigations

The Investigations Report provides a list with a basic description of all traceroute investigations that were completed during the selected time period.

Investigations are linked to the Incident Overview Report because many investigations are launched automatically, in response to an Incident report of a call setup threshold violation. However, investigations can also be launched:

- According to a schedule to establish a baseline of data, such as the route most frequently taken by call setup flows between certain Locations and call servers.
- On demand by users with the appropriate permissions to launch investigations manually. See "Launching a Traceroute Investigation" on page 106 for more information.

The **Trigger** column of the Investigations Report indicates what type of situation caused the investigation to be launched. For example, the Trigger indicates **Incident** if the investigation was launched as a call setup Incident response action.

Details about any particular investigation are available from the Investigations Report by clicking the investigation **ID** link. Filtering by group is also available if you have defined custom groups in the NetQoS Performance Center. Click the **Settings** link for filtering options.

The Investigations Report contains the following information about each investigation that was launched during the selected time period:

Column	Description
ID	The sequential number assigned to this investigation. Click it to see detailed information about the selected investigation.
Trigger	The reason why the traceroute was performed. Either: • **Incident**—A traceroute action was launched in response to a threshold violation (a call setup or call server group Incident). ***Note:*** In some cases, traceroute investigations can be launched in response to other types of Incidents, but the results are usually not very helpful. See "How Incidents Trigger Responses" on page 40 for more information. • **Manual**—A UC Monitor user launched the investigation from the Launch Traceroute page. • **Scheduled**—The traceroute was performed as part of UC Monitor baseline threshold monitoring.
Target Type	The type of target for the investigation. Either Location, Media Device, or Device. **Device** indicates that the target type selected for an on-demand traceroute investigation was an IP address.
Target Name	The hostname of the target for the investigation; the destination host for the traceroute.
Target Address	The IP address of the target for the investigation; the destination address of the traceroute.

Column	Description
Collector	The name assigned to the Collector that performed the traceroute. Under certain conditions, more than one Collector might send traceroutes to the same target device. The baseline path results are less accurate in such a case because different Collectors are likely to get different results.
Completed On	The date and time when the traceroute was completed. ***Note:*** Depending on the settings used for the number of retries and timeout length, this time may be different from the time the investigation was first attempted.

Traceroute Investigation Details

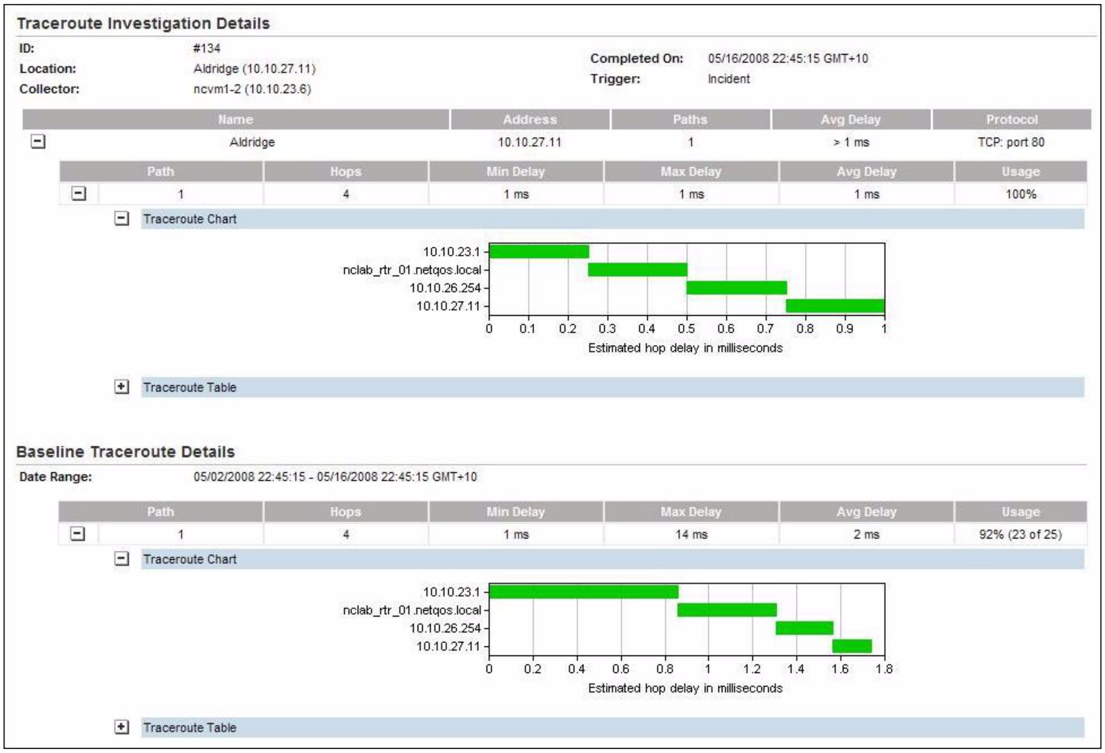
The Traceroute Investigation Details Report page provides more information about a selected traceroute investigation.

Investigation Details are available for individual investigations by drilling down from the Investigations Report page. Access Investigation Details by clicking the link to the ID number of an investigation in the Investigations List. Or click **Investigation Details** from the **Related Reports** links in an Incident Details Report.

The detailed reports for individual investigations show more information about the route, router hops, and delay data collected from the traceroutes that were performed, whether on demand, scheduled, or in response to an Incident. The baseline traceroute data provided allows you to compare the routes through the network that are being taken by call traffic.

Expand the Traceroute Chart or Traceroute Table areas (highlighted in blue) to see the data in the format you prefer, either graphical or tabular.

Here’s an example of traceroute data, including baseline information:



Traceroute Investigation Details

ID: #134

Location: Aldridge (10.10.27.11)

Collector: ncvm1-2 (10.10.23.6)

Completed On: 05/16/2008 22:45:15 GMT+10

Trigger: Incident

	Name	Address	Paths	Avg Delay	Protocol
⊟	Aldridge	10.10.27.11	1	> 1 ms	TCP: port 80

	Path	Hops	Min Delay	Max Delay	Avg Delay	Usage
⊟	1	4	1 ms	1 ms	1 ms	100%

⊟ Traceroute Chart

⊞ Traceroute Table

Baseline Traceroute Details

Date Range: 05/02/2008 22:45:15 - 05/16/2008 22:45:15 GMT+10

	Path	Hops	Min Delay	Max Delay	Avg Delay	Usage
⊟	1	4	1 ms	14 ms	2 ms	92% (23 of 25)

⊟ Traceroute Chart

10.10.23.1
nclab_rtr_01.netqos.local
10.10.26.254
10.10.27.11
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
Estimated hop delay in milliseconds

⊞ Traceroute Table

The following information is displayed for an investigation on the Traceroute Investigation Details Report page:

Metric	Description
ID	Unique number that identifies the traceroute investigation that was performed.
Device, Location, or Media Device	The device (an IP phone, voice gateway, or other device), the Location, or the media device that was the target of the traceroute.
Collector	The Collector that launched the traceroute.
Completed On	The date and time when the investigation was completed.
Trigger	The reason why the investigation was launched, either: • **Incident**—A traceroute action was launched in response to a threshold violation (a call setup or call server group Incident). ***Note:*** Traceroute investigations can also be assigned as responses to other types of Incident, but the results are usually not very helpful. See "How Incidents Trigger Responses" on page 40 for more information. • **Manual**—A UC Monitor user launched the investigation from the Launch Traceroute page. • **Scheduled**—The traceroute was performed as part of UC Monitor baseline threshold monitoring.
Name	The hostname of the target device.
Address	The IP address of the target device.

Metric	Description
Paths	The number of unique network paths found during this investigation. ***Note:*** This value also depends on the setting configured for the **Route Searches** parameter. For example, if you selected 0 for that parameter during a manual traceroute, this value must be 1 because no other attempts to find a route were attempted. The default setting is 0.
Avg Delay	The average amount of time, in milliseconds, that it took for the traceroute to complete.
Protocol	The protocol used for the traceroute.
Individual Path Details	
Path	The sequential number assigned to this network path. See **Paths**, above.
Hops	The number of hops found in the network path.
Min. Delay	The smallest amount of path delay of all path samples for this unique path.
Max. Delay	The greatest amount of path delay of all path samples for this unique path.
Avg. Delay	The average amount of path delay of all path samples for this unique path.
Usage	The percentage of time that this particular path was taken during the baseline date range (see below). Varies based on the number of different paths found.
Baseline Traceroute Details	
Date Range	Indicates the time period during which the baseline traceroute data represented here was collected for the indicated device or Location. By default, the 14 days prior to (and including) the **Completed On** date. Baseline traceroute data is collected from every voice gateway (by default) and every key phone at four-hour intervals. See "Baseline Traceroute Parameters," below, for more information.
Hops Delay (Min, Max, Avg) Usage	See above for definitions of these metrics. Of all unique paths found during baseline testing, the path with the highest Usage percentage is the one whose data is shown in this section of the report.

Baseline Traceroute Parameters

NetQoS UC Monitor calculates baseline routes by running regular traceroutes to selected Cisco IP phones and voice gateways. The route information is included as a basis for route comparison in the Traceroute Investigation Details Report for all gateways and all Locations where you have defined a key phone. The key phone serves as the target device for the traceroutes.

"Routine" traceroutes to find a baseline are a Cisco-only feature. Routine traceroute monitoring to derive a baseline route is performed on a regular schedule by default on all Cisco voice gateways, including those newly discovered by the system and those that you add. A UC Monitor Administrator can disable the option to **Perform routine traceroutes for baseline** when adding or editing a voice gateway definition. See the *UC Monitor Administrator Guide* for more information.

Note: To diagnose network routing issues in an Avaya environment, either consult the Avaya-specific Call Path Report or launch a traceroute investigation. Some limitations apply in an Avaya deployment. See "Launching a Traceroute Investigation" on page 106 for more information.

Routine traceroute tests are launched every four hours, starting at 2:00 AM (02:00). The schedule is determined by the time zone of the Collector, but the times that appear in reports reflect the Management Console time zone.

Note: In general, only one Collector will run a routine traceroute to a target, but under certain circumstances, multiple Collectors might run traceroutes to the same target. In such a case, baseline path results are less accurate: different Collectors are likely to get different results, and baselines are calculated based on the frequency of path results. The main Investigations Report page lists the Collector that performed the traceroute.

Each traceroute uses the following parameters:

Parameter	Description
Packet size	The size of the data payload that is sent to find the route through the network. 0 bytes. DiffServ ToS bits in the header are set for CS3 handling, the standard for call setup traffic.
Retries	The number of times the traceroute probe is repeated per router hop if no response is received from the target device. Two times. Counting the initial attempt, the traceroute is attempted up to three times per hop.
Route searches	The number of additional times the traceroute is run. 0 additional times.
Timeout	The number of seconds to wait for a response to a traceroute probe before timing out. 2 seconds.
Port	The port and protocol to use for the traceroute. If the traceroute target is a Cisco key phone, the Collector uses **TCP** over port **80**. If the target is a voice gateway media device, the Collector selects the appropriate protocol and port based on the call setup protocol: • ICMP • TCP over port 80 • TCP for **SIP** (port 5060) • TCP for **MGCP** (port 2428) • TCP for **H.323** (port 1720)

These are default settings. You can configure these parameters to use different values when launching a traceroute investigation on demand. See "Launching a Traceroute Investigation" on page 106 for more information.

Baseline traceroute data can be viewed in the Traceroute Investigation Details report. Tables of data from baseline testing can then be compared with any data taken from traceroutes that were launched automatically, in response to an Incident, or that were launched on demand.

Launching a Traceroute Investigation

To help you collect extra information about the sources of poor call performance, NetQoS UC Monitor offers traceroute investigations.

Traceroute investigations are available for Cisco devices, and also for Avaya with some limitations. Avaya IP phones do not support traceroute investigations using protocols other than ICMP. However, Avaya voice gateways and Communication Managers support traceroute investigations that use either TCP or ICMP. Be aware that the baseline route shown in the report for an Avaya phone's call path is calculated differently from the baseline that is available from Cisco baseline traceroute testing.

A UC Monitor Administrator can configure a traceroute investigation to run automatically in response to a call setup threshold violation, or any UC Monitor operator with the necessary user account permissions can launch an investigation on demand. To instruct NetQoS UC Monitor to launch a traceroute automatically, the Administrator enables a traceroute investigation as an Incident response action. See the *UC Monitor Administrator Guide* for more information about actions.

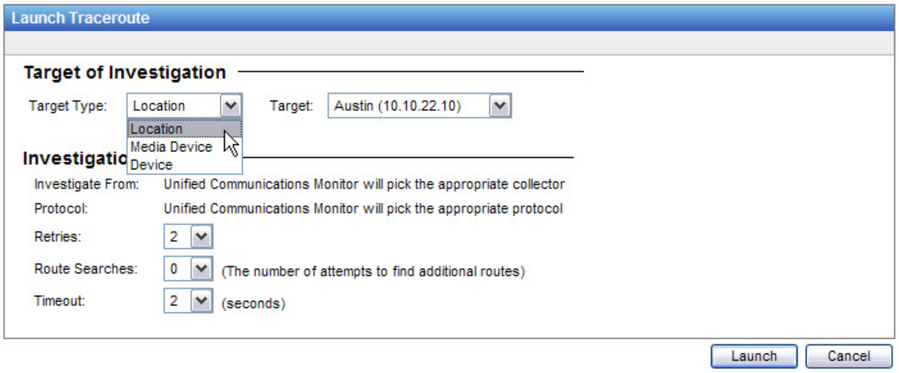
Whether the traceroute was launched as an Incident response or on demand, the results of a traceroute investigation are displayed in a Traceroute Investigation Details report.

Note: If broader access to this feature is desired, the Administrator must grant the role for each user account permission to launch an investigation; this ability is not enabled by default for new user accounts unless they have the Network Manager role. Any user accounts with other roles will lack the necessary area access.

To launch a traceroute investigation manually:

1. In the navigation links, click **Troubleshooting > Launch Investigation**.

   The Launch Traceroute page provides options to determine the target for the traceroute and other parameters, such as a timeout and number of retries to attempt:



Launch Traceroute

Target of Investigation

Target Type: Location

Target: Austin (10.10.22.10)

Investigatio

Investigate From: Unified Communications Monitor will pick the appropriate collector

Protocol: Unified Communications Monitor will pick the appropriate protocol

Retries: 2

Route Searches: 0 (The number of attempts to find additional routes)

Timeout: 2 (seconds)

2. Supply the following information in the fields provided:

Property	Description
Target of Investigation	
Target Type	The type of target for the investigation. Select either **Location**, **Media Device**, or **Device**. Your selection determines the options that are available in the **Target** menu. The **Device** option lets you enter an IP address as the target. Select the **Media Device** option for a voice gateway.
Target	The target device for the investigation; the destination of the traceroute. The available targets depend on the Target Type you selected. If you selected **Location** as the Target Type, the target must be a Cisco key phone. Typically, a key phone is designated at each Location you have defined. If the Administrator has not designated any key phones, edit the Locations under investigation to designate a key phone and then return to this page to launch a traceroute. Or select **Device** as the Target Type and enter its IP address. If you select an Avaya IP phone as the target, use ICMP for the protocol.
Investigation Options	
Investigate From	The Collector that will launch the traceroute. The Management Console selects the appropriate Collector based on the Target unless you selected **Device** as the Target Type.
Protocol	The protocol to use for the traceroute. If you selected either **Location** or **Media Device** as the Target Type, the Collector uses TCP over Port 80. If you selected **Device** as the Target Type, select the appropriate protocol and port, based on the call setup protocol used by the call server or gateway device: • ICMP • TCP over port 80 • TCP for **SIP** (port 5060) • TCP for **MGCP** (port 2428) • TCP for **H.323** (port 1720) ICMP is the only supported protocol for Avaya IP phone targets. For all traceroutes, including baseline traceroutes, the DiffServ ToS bits in the header are set for CS3 handling, the standard for call setup traffic.
Retries	The number of probes, from 0 to 10, to send to each component in the route in the event that a target endpoint does not respond. Default is 2 retries.
Route Searches	The number of times, from 0 to 20, to attempt to find additional routes for the selected target. Multiple traceroutes are attempted to see whether any alternate routes are being used between the Collector and the target device. Default is 0. ***Note:*** All unique routes attempted are included in the Investigation Report.
Timeout	The number of seconds, from 1 to 10, that must elapse for a traceroute to be considered timed out (target unreachable). Default is 2 seconds.

3. Click **Launch** to launch the traceroute immediately. Results are displayed as soon as they become available. For more information about the results, see "Traceroute Investigation Details" on page 102.

Troubleshooting Traceroutes

No **baseline traceroute** information is collected from your network if:

- an Administrator has not defined any key phones at your Locations.
- the Administrator has used phones or endpoints made by vendors other than Cisco for the key phones. Other endpoints do not support this feature.
- an Administrator has disabled routine traceroutes on your voice gateways.
- the key phones you have defined have not sent or received any call traffic.

To enable traceroutes to Locations, an Administrator must define key phones when adding or editing Location definitions. The **Key Phone Address** parameter is available on the Location Properties Administration page.

A parameter that enables the collection of baseline traceroute data, **Perform routine traceroutes for baseline**, is enabled by default for all voice gateways. An Administrator can disable it. The *UC Monitor Administrator Guide* contains more information.

Similarly, if you attempt to launch a **traceroute investigation** to a Location whose key phone has not yet sent or received any call traffic, the investigation will fail. You'll see an error message stating that a traceroute could not be initiated because a Collector could not be found for that Location. The Collector must have observed that key phone in collected traffic before it can run a traceroute to it. But as a workaround, you can select **Device** as the Target Type and enter the IP address of that key phone.

A traceroute investigation is only launched in response to a call setup Incident if:

- a Cisco key phone is defined for the affected Location
- the key phone has seen some traffic since it was configured and is therefore known to the Collector
- routine traceroutes are enabled for the affected voice gateway
- an Incident response action to run a traceroute is configured

Traceroute investigations can be launched in response to call quality Incidents, but the results are usually not very helpful. The Collector, which is co-located with the call servers, launches the traceroute and can gather accurate data about the routing of call setup traffic between phones and call servers. But call quality Incidents are reported between Locations. The routing data found will not be as accurate if the Collector is located in North Carolina (along with the call servers) and it launches a traceroute in response to a call quality issue that was reported in Texas.

Worst Locations Quality Report

Monitoring reports in the Quality section provide a quick overview of the worst-performing pairs of Locations, based on their performance data and the associated performance thresholds.

The Worst Locations Report provides a useful perspective on performance. Where other Monitoring reports provide quality statistics for the data received by the listening Location, as in the Performance by Location and Performance by Group data views, the Worst Locations Report shows the *pairs* of talkers (Locations) that had the lowest-quality metrics for the data traveling between them. The "**Severity Breakdown**" bar chart shows a comparison of data ratings by severity, based on the performance thresholds that were applied to the collected quality metrics. Each bar represents 100% of rated quality data (depending on the filter applied), with colored portions indicating the relative percentages of data that received each severity rating (Normal, Degraded, Excessive, or Unrated).

Click a bar to see a view of the pair of Locations in question with the call traffic filtered by the selected metric. From this filtered view, a helpful next step to take would be to check the Call Leg Details report. Click the link from the **Related Reports** section.

A quick-filtering option allows you to select the **Metric Type** whose severity is reflected in the bar chart. All the available Call Setup and Call Quality performance metrics are included in the list. See the following topics for more information about these metrics:

- "Call Setup Metrics" on page 81
- "Call Quality Metrics" on page 78
- "Video Metrics" on page 82

Depending on the metric selected in the quick-filtering list, the "worst" Locations might show excellent performance; they are not showing degraded performance for that particular metric. Select different metrics from the **Metric Type** list to see which ones had the worst severity for the same pairs of Locations.

The following information is provided in the **Worst Locations** table:

Column	Description
Name	The name of the Location or media device that received the data stream with poor performance metrics. If the data view is filtered by one of the Call Setup metrics, it refers to the Location that placed the call.
Sending Name	The name of the Location or media device that sent the low-performing call data to the other Location in the pair.
Call Server	The call server that handled the calls whose severity breakdown is shown.
Call Minutes	The number of minutes that calls were active between this pair of Locations.

Column	Description
Calls	The number of distinct calls that ran between this pair of Locations and that also contributed to the "worst" performance metric being displayed. A hyperlink to the **Calls Overview** table, filtered to show all calls that ran between the selected pair of Locations or media devices. ***Note:*** This total might not exactly match the number of calls shown in the Calls Overview. The Worst Locations report defines a call as a unique combination of Origination Location, Destination Location, and originating call server. Phones in the same Location that are registered to different call servers will have their calls counted separately in the Worst Locations report, but will all appear in the Calls table. See "Calls Overview Report" on page 118 for more information.
Severity Breakdown	A stacked bar chart that adds up to 100%. Each applicable severity rating is shown as a portion of that 100% and color-coded to match the severity indicators in other reports. Click a bar to see a view of the pair of Locations in question with the call traffic filtered by the selected metric.
• Unrated (%) • Normal (%) • Degraded (%) • Excessive (%)	The actual severity percentages for the selected quality metric type. Percentages always total 100%. An "Unrated" metric may indicate that a threshold has been disabled, but in most cases, it indicates that the threshold for minimum observations is set too high for the typical levels of call traffic. The UC Monitor Administrator can set a lower minimum for observations to allow all metrics to be rated or assign a different set of thresholds to the Location pairs in question.

To see the severity breakdown for another quality metric, select another metric from the **Metric Type** list in the Settings area.

Worst Phones Quality Report

Monitoring reports in the Quality section provide a quick overview of the worst-performing endpoints or phones, based on their MOS values and the associated performance thresholds.

The Worst Phones Report provides a list of phones with the lowest MOS values for the selected timeframe. Phones are identified by phone number or SIP URI and by their IP address. A stacked bar chart shows the percentages of MOS values that fell into the various severity ratings categories.

The following information is provided in the **Worst Phones** table:

Column	Description
Phone Number	The phone number (directory number, or DN) of the phone, or the SIP URI of the endpoint. A hyperlink to the **Phone Details** and **Phone Call Details** tables for the selected phone or endpoint. See "Phones Report" on page 131 for a description of the available data.
Name	The name of the phone or endpoint.
IP Address	The IP address of the phone or endpoint.

Column	Description
Call Minutes	The total number of minutes that calls were active on this phone or endpoint during the selected timeframe.
Calls	The number of distinct calls that this phone placed or received. A hyperlink to the **Calls Overview** table, filtered by the selected phone or endpoint. All calls from the selected timeframe of the Worst Phones Quality Report that you were viewing are included in the Calls Overview table if the phone or endpoint was either the **Origination Number** or the **Destination Number**. See "Calls Overview Report" on page 118 for more information.
Average MOS	The average MOS value for all calls to and from this phone or endpoint during the selected time frame. Unlike the MOS severity reflected in the bar chart, this average is not weighted by the duration of the calls.
MOS Severity Breakdown	A stacked bar chart that adds up to 100%. Each applicable severity rating is shown as a portion of that 100% and color-coded to match the severity indicators in other reports.
• Unrated (%) • Normal (%) • Degraded (%) • Excessive (%)	The actual severity percentages for the MOS metric. Percentages always total 100%. An "Unrated" metric may indicate that a threshold has been disabled. The UC Monitor Administrator can assign a different set of thresholds to the Location pairs in question so that all metrics are rated.

Troubleshooting Reports

The Troubleshooting report pages are intended to help network engineers explore in-depth performance metrics, plan for upgrades or other network changes, and identify performance issues at a particular VoIP endpoint. Detailed metrics gleaned from records kept by the call server and from frequent polling of IP phones while calls are in progress help you track statistics on when calls are being made, where calls are coming from, how they are being routed, and how they are performing.

The Troubleshooting section of the UC Monitor Management Console provides the following reports:

Report	Description
"Call Watch Overview Report" on page 112	Real-time views of metrics collected from calls that are being actively monitored while still in progress. Provides a drilldown path to charts of detailed metrics in the Call Watch Details report.
"Calls Overview Report" on page 118	Summary data about recent call activity. Provides a drilldown path to detailed call data in the Call Details Report.
"Calls Export" on page 128	Data from UC Monitor database exported to a file in `.csv` format. Filtering and column selection available.
"Phones Report" on page 131	Detailed information about the phones and endpoints known to all monitored call servers. Provides a drilldown path to detailed call data for each phone in the Phone Details Report.

You also have the option to launch a manual traceroute investigation from the Troubleshooting section. See "Launching a Traceroute Investigation" on page 106 for more information.

Navigating in the Troubleshooting Section

Access the following report pages and views by clicking the **Troubleshooting** navigation link:

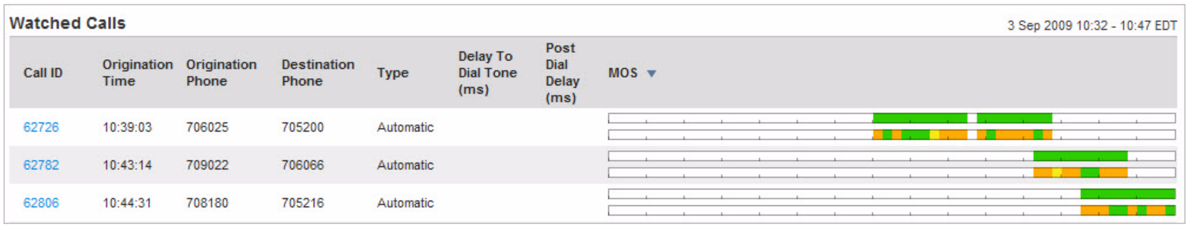
Report Page or View	Navigation and Description
Call Watch Overview Report	Click **Troubleshooting > Call Watch > Overview**. Lets you view Call Watch data as it comes in from 15-second polling of active calls. Call Watch data is shown in real time. You can also use the Time Frame selector to view the data from calls watched previously. Provides an opportunity to drill down into: • Call Watch Details • Call Path Report (*Avaya only*)
Calls Overview Report	Click **Troubleshooting > Calls > Overview**. Provides summary data about recent call activity. Also provides drilldown into the Call Details Report.
Calls Export	Click **Troubleshooting > Calls > Export**. Lets you export data from the UC Monitor database to a `.csv` file. Provides filtering options.
Launch Investigation	Click **Troubleshooting > Launch Investigation**. Lets you manually configure and launch a traceroute investigation. An "Traceroute Investigation Details" report becomes available within a few seconds. See "Launching a Traceroute Investigation" on page 106 for more information.
Phones Report	Click **Troubleshooting > Phones**. Provides information to identify all monitored phones and endpoints. Provides drilldown into the Phone Details Report.

Call Watch Overview Report

The UC Monitor Call Watch feature allows you to monitor, or "watch," all call activity of a phone DN within a Location. If you are monitoring Avaya IP phones, Call Watch data is automatically collected from all active calls. In Cisco environments, Call Watch data is only collected from the phones you specify when you create a Call Watch definition.

The Call Watch Overview Report presents views of metrics collected from calls that are currently being watched (that is, VoIP phone calls that are being monitored while in progress). This report also provides a time period navigation feature that lets you view data from calls that were watched previously. A fifteen-minute or one-hour time frame can be selected.

Filtering of report data is available. Click the **Settings** link to access the Settings dialog box.



Watched Calls

3 Sep 2009 10:32 - 10:47 EDT

Call ID	Origination Time	Origination Phone	Destination Phone	Type	Delay To Dial Tone (ms)	Post Dial Delay (ms)	MOS ▼
62726	10:39:03	706025	705200	Automatic			
62782	10:43:14	709022	706066	Automatic			
62806	10:44:31	708180	705216	Automatic			

See “Using the Call Watch Feature” on page 48for more information about Call Watch capabilities.

Note: Call Watch is not supported in a Microsoft Office Communications Server 2007 environment.

The following information about watched phone calls is available in the Call Watch Overview Report. Note that for each call, two MOS bar charts are shown, one for each call leg:

Call Watch Metric	Description
Call ID	The call identifier, assigned by NetQoS UC Monitor, for each call that was made or received by a watched phone during the call watch period. A link to detailed information about a watched call. See “Call Watch Details” on page 114 for more information. An asterisk (*) is displayed next to the call ID if the party that placed the call cannot be determined from collected data. Applies to Avaya only. Usually indicates that CDR collection is not enabled on an Avaya system.
Origination Time	The time the call began.
Origination Phone	The number of the phone that placed the call. When Avaya endpoints are watched, the calling and called parties are not identified until after the call completes. An asterisk next to the Call ID indicates that the direction of the call (that is, which endpoint placed the call) could not be reliably determined from the collected data. This usually occurs when CDR collection is not enabled.
Destination Phone	The number of the called party. See the previous description for more information about call direction.
Type	The type of Call Watch, either: • **Automatic**—Applies to all Avaya calls, which are automatically “watched” • **Defined**—Applies to any Call Watch you set up manually, or to any Call Watch that was launched in response to a user QRT softkey event. Call Watch definitions are created in the **Troubleshooting > Call Watch > Definitions** area. See “Setting Up a Call Watch” on page 50 for more information. QRT events are Cisco-only. They are discussed in “More about the Poor Call Quality (QRT) Threshold” on page 140. If desired, you can filter the report by Call Watch type. Click the **Settings** link.
Delay to Dial Tone	(*Cisco Only*) The time it took, in milliseconds, for the calling phone to receive a dial tone from the call server or voice gateway.
Post-Dial Delay	(*Cisco Only*) The time between entering the last digit of a telephone number and receiving a ring or call connect.

Call Watch Metric	Description
MOS	The mean opinion score measured for this call by the IP phone, endpoint, or voice gateway. Appendix A, “Calculating a Mean Opinion Score” on page 147 contains a full discussion of MOS values and how they are derived.

Note: In a few cases, older or lower-end IP phone models and “soft phones” do not support the collection of all Call Watch statistics. The Call Watch reports will show no data for the statistics that are not supported. For example, the Cisco Model 7902 phone only returns packets received and packets lost; therefore, the only metric NetQoS UC Monitor can calculate when this phone is watched is Packet Loss.

Placing a call on hold effectively ends a Call Watch for both phones involved in a watched call.

Call Watch Details

Click the link for the Call ID to view detailed information about a watched call.

See the “Notes” section below for help with the charts if phone number masking is being applied.

The following details are available, depending on the equipment being monitored (that is, some metrics are specific to a single hardware vendor, and some types of endpoint or phone can provide different metrics):

Item	Description
Origination Phone Information	If available, detailed information about the phone that placed the call, including the phone number, make and model, its call server, voice gateway, codec, firmware version, serial number, and switch connection type. Availability of this information depends on the type of phone or voice gateway. ***Note:*** If you’re monitoring Avaya, information about the phone that placed the call requires CDR data from the Communication Manager and is not available until the call has completed. While the call is in progress, either endpoint might therefore be the origination or destination phone. If CDRs are not enabled, the Call ID and phone numbers show an asterisk (*) on the main Call Watch Overview page to indicate that the caller and called party could not be reliably identified. Also see below for the **Trunk Group** parameter.
Destination Phone Information	If available, detailed information about the phone that received the call, including the phone number, make and model, its call server, voice gateway, codec, firmware version, serial number, and switch connection type. Both the availability and reliability of this information depends on the type of phone or voice gateway, and your configuration; see the **Note** above if you are monitoring Avaya.
Trunk Group	Trunk group number for a voice gateway call. While the call is still in progress, the phone number of the endpoint sending data through the gateway cannot be identified. The Trunk Group ID is substituted for the phone number (and displayed in the **Phone Number** field) until this information is received.
Conference ID	Avaya identifier for a voice gateway call.

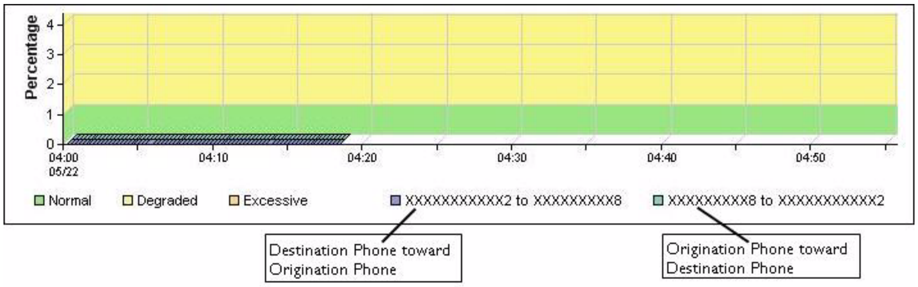
Item	Description
Switch	The name, IP address, and port of the switch to which the phone is connected. This information comes from the Web page of the IP phone, which uses Cisco Discovery Protocol (CDP) to collect the information. If the phone is connected to a switch that does not support CDP, the next CDP-enabled device in the path of the watched call is shown for the **Switch** value.
Call Leg Details	Summarizes the metrics shown in the Call Watch Overview Report with the MOS rating broken out per call leg (directional flow of the conversation).
MOS	The Mean Opinion Score (MOS) Listening Quality (LQK) average. For some types of phones, this score is updated every second during a call. Appendix A, "Calculating a Mean Opinion Score" on page 147 contains a full discussion of MOS values and how they are derived.
Packet Loss	Number of packets lost in transit, expressed as a percentage of all packets in the stream and broken out per call leg.
Latency	One-way delay, calculated from the calling party to the called party. Includes: • propagation delay—delay produced by the physical distance traveled on the line • network delay—transport delay, produced by intervening network equipment, such as routers and switches • packetization delay—delay introduced by the codec Latency of 150 ms and higher has a noticeable effect on call quality.
Jitter Buffer Loss	Percentage of packets lost due to jitter buffer overruns or underruns.
Jitter Buffer Delay	The delay introduced by the receiver while it holds one or more packets to reduce variations in packet arrival times.
Jitter Buffer Over Runs	The number of times that the actual jitter (variation among packet delay values) exceeded the maximum size setting of the jitter buffer. Usually packet loss is a result. ***Note:*** Avaya endpoints have a limitation that affects the way this metric and the following one, **Jitter Buffer Under Runs**, are reported. The maximum value is 255. If you see this cumulative value for one of these performance metrics, it usually means that the value was greater than 255, and the actual maximum value cannot be reported. Also note that these values, reported every 15 seconds during a Call Watch, are additive: once the 255 threshold has been reached, the Jitter Buffer Over Runs or Jitter Buffer Under Runs chart will show 0 values for each successive interval until the call is completed.
Jitter Buffer Under Runs	The number of times that the jitter buffer became empty. Usually indicates that delays are too lengthy for the buffer setting.
Sequence Jumps	The number of times that at least one consecutive packet was lost.
Max Sequence Jump	The maximum number of consecutive packets that were lost during any reporting interval.
Sequence Falls	The number of times times that at least one packet arrived out of order.
Max Sequence Fall	The maximum number of packets that arrived out of order for any reporting interval.

Item	Description
Jitter	The average jitter (variation in delay times among packets in the same stream, in milliseconds), measured for each call leg. ***Note:*** When calls that travel through an Avaya voice gateway are watched, the Average Jitter reported by the gateway very often exceeds the **Max Jitter** reported (the following metric). We have reported this issue to Avaya.
Max Jitter	The maximum jitter (delay variation in milliseconds) for any reporting interval.
Concealed Seconds	Number of call seconds that had concealment events (due to lost frames) from the start of the voice stream. **IP phone calls only**.
Severely Concealed Seconds	Number of call seconds that had more than 5% concealment events from the start of the audio stream. **IP phone calls only**.
ACOM	Sum of the following values recorded for a phone call involving the PSTN: • Echo Return Loss (ERL) — The reduction in the echo level produced in the circuit without an echo canceller. • Cancellation loss, or Echo Return Loss Enhancement (ERLE) — An enhancement in the echo return loss, produced by an echo canceller. • Nonlinear processing loss—Reduction in echo resulting from NLP echo cancellation algorithms, which attempt to remove residual echo. **PSTN calls only**. For this metric, lower values are rated as worse (closer to crossing the Degraded or Severe threshold) because ACOM is a measurement of how significantly echo was reduced.
ERL	Echo Return Loss (ERL) — Reduction in the echo level produced in the circuit without an echo canceller. The degree or amount of loss reflects the volume of the echo that remains. Like ACOM, a measurement of how significantly echo was reduced. **PSTN calls only**.
Signal In	Signal level of the data flow traveling into the echo canceller. **PSTN calls only**.
Signal Out	Signal level of the data flow traveling out of the echo canceller toward the IP network. **PSTN calls only**.

Notes

If phone number masking is used, the charts in this report may become difficult to interpret. Chart legends are used to indicate the colors that are used to graph each call leg so that quality metrics can be broken out for each direction of call data flow. If the UC Monitor Administrator sets up a mask so that, for example, only the first digit of each phone DN is displayed, these legends become virtually useless because often the first digits in a dial plan are identical.

To decipher the Call Watch Details charts where masking is being applied, keep the following in mind: the legend entries are positional. If ordered from left to right, the first pair of masked phone numbers (shown as “XXXX to XXXX” in each chart legend) indicates Destination phone to Origination phone; the second pair indicates Origination phone to Destination phone, as shown in the following example:



Destination Phone toward
Origination Phone

Origination Phone toward
Destination Phone

Call Path Report

The Call Path detailed report is only available in Avaya Communication Manager environments. This report uses the call path data that is included in the RTCP packets collected from Avaya endpoints during a call. In addition to a chart showing each hop that the call data took, the Call Path Report compares path data from the present call with any historical data collected and stored from the same endpoints to provide a baseline call path.

Access the Call Path Report from the **Related Reports** section of the Call Watch Details report.

The Call Path Report shows both current and baseline path information for each direction of call data flow. Additional information is also provided about the route, router hops, and per-hop delay.

By default, baseline path data is available if calls that ran between the same endpoints have been observed in the past. This information is kept in the UC Monitor database for up to 14 days and is used to determine a base path. This information allows you to compare the routes through the network that are being taken by call traffic and gauge whether calls are being routed normally.

Expand the **Path Chart** or **Path Table** areas (highlighted in blue) to see the data in the format you prefer, either graphical or tabular. Click the **Settings** link if you want to remove the **Baseline Call Path Details** chart and table from the report.

The following information is displayed on the Call Path Report page:

Metric	Description
ID	Unique number that identifies the call that was watched.
Completed On	The date and time when the call was completed.
Name	The hostname of the destination endpoint.
Address	The IP address of the destination endpoint.
Paths	The number of unique paths that have been detected between these endpoints. Includes any paths reported in the Baseline Call Path chart and table.
Avg Delay	The average delay for all hops in all paths detected between these endpoints.
Individual Path Details	
Path	The sequential number assigned to this network path. See **Paths**, above.
Hops	The number of hops found in the network path.
Min. Delay	The smallest amount of path delay of all path samples for this unique path.

Metric	Description
Max. Delay	The greatest amount of path delay of all path samples for this unique path.
Avg. Delay	The average amount of path delay of all path samples for this unique path.
Usage	The percentage of time that this particular path was taken during the baseline date range (see below). Varies based on the number of different paths found.
Baseline Call Path Details	
Date Range	Indicates the time period during which the baseline path data represented here was collected. The data comes from calls made between the Locations of the indicated endpoints during the 14 days prior to (and including) the **Completed On** date. If this is the first call observed between these two Locations, the **Date Range** shows a blank.
Path Hops Delay (Min, Max, Avg) Usage	See above for definitions of these metrics. Of all unique paths found during baseline testing, the path with the highest Usage percentage is the one whose data is shown in this section of the report.

Calls Overview Report

The Calls Overview Report provides summary data about recent call activity. Call IDs in the summary table provide links to more detailed information about the source and destination endpoints or phones and to granular metrics used in calculating MOS values and deriving averages.

If you are monitoring Microsoft Office Communications Server 2007 and later, a “quick-filtering” option is available. The **Media Type** list appears in the Settings area to allow you to filter the list of calls. The default filter is **All**, which means that all calls placed during the selected time frame are included in the list. The **Audio** option excludes all video call streams from the list. Selecting the **Audio/Video** filtering option from the list allows you to see calls with separate video and audio streams as correlated “sessions.” See “Session Details” on page 124 for more information.

The following information about phone calls from the selected time period (by default, the last three hours) is available in the **Calls Overview** table. Note that for each call, two MOS scores are shown, one for each directional call leg:

Metric	Description
Call ID	The call identifier, assigned by NetQoS UC Monitor, for each call that was made or received during the selected time period. A hyperlink to detailed data about each call. See “Call Details Report” on page 119 for more information.
Session ID	(*Microsoft Only*) The session identifier, assigned by NetQoS UC Monitor to identify call legs for separate audio and video data streams that the Collector recognizes as part of a single UC call. A hyperlink to detailed data about each separate leg in the correlated “session.” See “Session Details” on page 124 for more information.
Origination Time	The date and time the call began.

Metric	Description
Origination Number	The phone number or SIP URI of the phone or endpoint that placed the call.
Origination Location/ Media Device	The Location of the phone or endpoint that placed the call, or the gateway device that forwarded the call from a point in the PSTN.
Destination Number	The phone number or SIP URI of the phone or endpoint that received the call.
Destination Location/ Media Device	The Location of the phone or endpoint that received the call, or the gateway device that forwarded the call to a point in the PSTN.
Duration	The length of the call, in minutes and seconds.
Media Type	The type of data stream in the call, either **Audio**, **Video**, or **Audio/Video**. By default, **All** types are included in the data view. (*Microsoft Only*) If you selected the **Audio/Video** option from the **Media Type** quick-filtering list, the Audio/Video media type refers to calls with correlated call leg data, which can be viewed in a Session Details view.
Origination MOS	The Mean Opinion Score (MOS) value of the data stream perceived at the origination endpoint or phone. See Appendix A, "Calculating a Mean Opinion Score" on page 147 for more information.
Destination MOS	The MOS value of the data stream as perceived at the destination endpoint or phone.
Call Setup Failure Code	If the call failed during the setup phase, the code that the call server returned, indicating the type of failure. See "Call Failure Cause Codes" on page 138 for more information.

Call Details Report

The Call Details Report provides a deeper set of metrics reported for the calls in the Calls Overview Report. The Overview report is a summary that provides preliminary details about recent calls. You can use it as an entry point for troubleshooting a call quality issue or a call server Incident.

When you click a hyperlinked call ID number in the **Calls Overview** list, you access the Call Details Report.

Note: If you are monitoring Microsoft, you can also access Session Details by clicking a hyperlinked session ID number. See "Session Details" on page 124 for more information.

This report contains several data views that provide information about the selected call and the phones or endpoints involved in that call, plus call quality metrics for each side of a bi-directional call. The raw metrics presented in these views are useful for understanding how other quality metrics, such as the MOS value, were derived; for looking more closely at individual metrics, such as jitter; and for tracking metrics that are not used in calculating the MOS, such as echo, noise, video metrics, and burst statistics.

The following tables describe the detailed information provided in the Call Details Report:

Call Information Table

Item	Description
ID	The call identifier, assigned by NetQoS UC Monitor, for the selected call. Matches the ID in the Calls Overview summary table.
Origination Number	The phone number or SIP URI of the phone or endpoint that placed the call. The URI is a link that opens the Microsoft Office Communicator application, if it is loaded on the local computer.
Origination Called Number	The phone number or SIP URI that was dialed.
Destination Number	The phone number or SIP URI where the call was received.
Origination Time	The date and time the call began.
Duration	The length of the call, in minutes and seconds.
Media Type	The type of data stream in the call, either Audio or Video. (*Microsoft-Only*) The Audio/Video media type refers to calls with correlated call leg data, which can be viewed in a Session Details view.

Origination and Destination Information Tables

Metric	Description
Origination Information	If available, detailed information about the phone or endpoint that placed the call, including the phone number or SIP URI, IP address, the phone or endpoint port through which the data passed, the phone make and model, call server, codec, firmware version, serial number, and connection information. Where provided, the **IP address** is a hyperlink to the phone's Web page. If the call involved a phone in the PSTN, provides information about the voice gateway that handled the call, including the interface and voice channel through which the data passed. Availability of this information depends on the type of phone, endpoint, or media device.
Destination Information	If available, detailed information about the phone or endpoint that placed the call, including the phone number or SIP URI, IP address, the phone or endpoint port through which the data passed, the phone make and model, call server, codec, firmware version, serial number, and connection information. Where provided, the **IP address** is a hyperlink to the phone's Web page. If the call involved a phone in the PSTN, provides information about the voice gateway that handled the call, including the interface and voice channel through which the data passed. Availability of this information depends on the type of phone, endpoint, or media device.

Origination or Destination Call Quality Metrics Tables—Audio

Metric	Description
MOS MOS (Min) Conversational MOS Listening MOS Listening MOS (Min)	The MOS, or Mean Opinion Score, is a call quality score based on a standard method of gauging the impact of impairments on the signal. **MOS** is the average MOS listening quality (LQK) score observed for the bi-directional voice stream. **MOS (Min)** is the lowest LQK score observed. (*Microsoft Only*) **Conversational** MOS is based on MOS values from both directions of data flow. **Listening** MOS is based on call legs traveling toward the phone or endpoint to reflect the quality perceived by the listener. Appendix A, "Calculating a Mean Opinion Score" on page 147 contains a full discussion of MOS values and how they are derived.
Network MOS Network MOS (Min)	(*Microsoft Only*) A MOS calculation that predicts the quality of the audio received by the listener while only considering the network impairments, such as codec, and packet errors. The average and minimum network MOS values are provided. See "Microsoft MOS Calculations" on page 148 for more information.
Network MOS Degradation Network MOS Degradation (Max) Network MOS Degradation: - Jitter - Packet Loss	(*Microsoft Only*) A breakdown of the metrics used in calculating the Network MOS. "Degradation" refers to an impairment factor that decreased the MOS value. The **Network MOS Degradation** is the average network MOS degradation for the data stream. The **Max** degradation is the highest degradation observed for the stream. **Jitter** and **Packet Loss** degradations represent the percentage of the overall Network MOS Degradation metric that was caused by levels of those individual metrics.
Latency	Delay in a single direction between the calling and called parties. See "Call Quality Metrics" on page 78 for more information.
Jitter Buffer Loss	(*Cisco Only*) Percentage of packets lost due to jitter buffer overruns or underruns. See "Call Quality Metrics" on page 78 for more information.
Jitter Buffer Delay	(*Avaya Only*) The delay introduced by the receiver while it holds one or more packets to reduce variations in packet arrival times.
Jitter Buffer Over Runs	(*Avaya Only*) The number of times that the actual jitter exceeded the maximum size setting of the jitter buffer.
Jitter Buffer Under Runs	(*Avaya Only*) The number of times that the jitter buffer became empty.
Jitter Jitter (Max)	The average amount of variance in packet inter-arrival times, in milliseconds. **Jitter (Max)** is the highest observed jitter level for the call.
Packet Loss Packet Loss (Max) Packets Received Packets Lost	Number of data packets lost in transit, expressed as a rate (the percentage of all packets in the stream that were lost). See "Call Quality Metrics" on page 78 for more information. **Packet Loss** is an average loss rate; the **maximum** rate is also provided for Avaya. **Packets Received** provides a means of gauging the size of the data stream. **Packets Lost** is the difference between Packets Sent and Packets Received.
Sequence Jumps Maximum Sequence Jump	(*Avaya Only*) The number of times that at least one consecutive packet was lost; the maximum reported is per reporting interval.

Metric	Description
Sequence Falls Maximum Sequence Fall	(*Avaya Only*) The number of times times that at least one packet arrived out of order; the maximum reported is per reporting interval.
Minimum Time-To-Live Maximum Time-To-Live	(*Avaya Only*) The TTL value in the IP header instructs network routers whether a packet has been forwarded towards its destination too many times and should be discarded.
Echo Tail Length	(*Avaya Only*) The "length" of echo cancellation processing determined by the distance between a voice gateway and the endpoint, and represented in milliseconds. Typical values range from 8 ms to 32 ms.
Differentiated Services Code Point	(*Avaya Only*) The DiffServ quality of service setting of the incoming RTP packets carrying voice data. A value in the range of 0 - 63, used to specify the level of service a packet should receive on the network.
802.1p Tag	(*Avaya Only*) The QoS priority setting for voice packets at Layer 2.
VLAN ID	(*Avaya Only*) The VLAN that carried the RTP packets.
Cumulative Concealment Ratio Maximum Concealment Ratio Severely Concealed Seconds	(*Cisco Only*) The **Cumulative Concealment Ratio** is the percentage of all call seconds that had concealment events (due to lost data). The **Maximum Concealment Ratio** is the highest concealment ratio value during the call. **Severely Concealed Seconds** reflects call seconds that had more than 5% concealment events from the start of the data stream.
Burst Density Burst Duration	(*Microsoft Only*) "Burst" refers to points in the data stream when a high percentage of packets are either lost or discarded due to late arrival. The **Burst Density** is the percentage of packets within burst periods that were either lost or discarded. The **Burst Duration** is the average duration of all high-loss periods in the data stream.
Gap Density Gap Duration	(*Microsoft Only*) The **Gap Density** is the percentage of packets in the gaps between bursts in the data stream that were either lost or discarded. The **Gap Duration** is the average duration of all periods of good performance (low loss) between periods of data loss in the data stream. ***Note:*** Occasionally, we have seen reported Gap Duration values that exceeded the call duration.
ACOM	(*Cisco Only*) The total echo return loss for the call, or the total amount that echo cancellation was able to reduce echo. **PSTN calls only**. See "Call Quality Metrics" on page 78 for more information.
Signal Level	The average audio signal level in decibels. The **dBm0** abbreviation specifically refers to dBm (decibels relative to a power level of one milliwatt, a standard reference point) as measured at a zero transmission level.
Noise Level	The average portion of the audio signal that is noise and not actual voice data, in decibels (dBm0; see above for explanation).

Origination Call Setup Metrics Table (Audio Only)

For audio-only calls that used Cisco Unified Communications Manager for call setup, call setup metrics are provided. The Call Setup Failure metric is also available from Microsoft.

Cisco call setup metrics are only collected from the originating IP phone (the phone that placed the call). If applicable, the following call setup metrics are provided:

Metric	Description
Delay to Dial Tone	For a user, the amount of time it takes to hear a dial tone after picking up the receiver of an IP phone. For the IP phone itself, the amount of time (or delay) measured between the following: off-hook event sent from the IP phone to its call server dial tone indication received from the call server A measurement of call server (or network) response time, or of how long it takes to receive a response from the call server for the phone to provide a dial tone.
Post Dial Delay	The time between entering the last digit of a telephone number and receiving a ring tone or call connect.
Call Setup Failure Code	If the call failed during the setup phase, the code that the call server returned, indicating the type of failure. See "Call Failure Cause Codes" on page 138 for more information.

Origination or Destination Call Quality Metrics Tables—Video

Note: Video metrics are only reported when monitoring a video over IP deployment using Microsoft Office Communications Server 2007 and later.

Metric	Description
Frozen Video Frequency	The frequency of long and noticeable frozen video for the whole session, expressed as a percentage of session time.
Frozen Period	Average length of frozen video instances.
Video Latency	Delay in a single direction between the calling and called parties. See "Video Metrics" on page 82 for more information.
Video Frame Loss Video Frame Rate	Average percentage of video frames lost. Based on the number of unique consecutive images (frames) lost due to corruption and error concealment for the entire stream. Video frames can span multiple packets; this metric is useful in conjunction with the video packet loss metrics (see below). **Frame Loss**: Average frames lost due to corruption and error concealment for the entire stream. **Frame Rate**: Average frames per second sent for the entire stream. See "Video Metrics" on page 82 for more information.

Metric	Description
Video Packet Loss (Max) Video Packets Received Video Packets Lost Video Consecutive Packet Loss	Number of data packets lost in transit, expressed as a rate (the percentage of packets in the video stream that were lost). See "Video Metrics" on page 82 for more information. **Packet Loss** is an average loss rate; the **maximum** rate is also provided. **Packets Received** provides a means of gauging the size of the data stream. **Packets Lost** is the difference between Packets Sent and Packets Received. **Consecutive Packet Loss** is the percentage of all lost packets that were lost consecutively to provide a gauge of loss burstiness.
Video Jitter Video Jitter (Max)	The average amount of variance in packet inter-arrival times, in milliseconds. **Jitter (Max)** is the highest observed jitter level for the call.
Resolution	The width and height of the video image, in pixels. Higher resolutions require more bandwidth and more CPU resources. Some resolution settings are not supported by all endpoints.
Video Bit Rate Video Bit Rate (Max	Average number of bits per second sent for the entire stream. The **Bit Rate Max** is the maximum number of bits per second sent for the entire stream. Bit rates provide a gauge of codec performance.
Video Frame Decoding Time	The average time spent for frame decoding for the entire stream. A slower decoding rate may be caused by a condition on the endpoint, such as lack of CPU resources, and can affect call quality.

Session Details

Calls that are processed by the Microsoft Office Communications Server may consist of simultaneous audio and video data streams. Depending on how the audio/video call was placed, the call might consist of several distinct call legs, including legs that traveled between a user and a conferencing server, those that carried the audio stream, and those that carried video data.

NetQoS UC Monitor can provide correlated call data for such calls, based on an identifying **session ID** that is assigned by the Collector when it detects similarities in endpoint identities and timestamps among audio and video data streams.

To view call data with correlated session information, first select one of the quick-filtering options. The following options are available in the **Media Type** list of quick filters:

- **All**—All calls are displayed. Those without video streams have the Audio media type; those with accompanying video streams usually have the Audio/Video media type and provide correlated call leg statistics in the Session Details view.
- **Audio**—Audio-only calls are displayed, and for calls with an accompanying video stream, only metrics from the audio stream are displayed.
- **Video**—All calls that include a video component are displayed, but only the metrics from the video stream are displayed.
- **Audio/Video**—All calls that include a video component are displayed, and their audio and video components are correlated: the separate audio and video streams are represented together in a

Session Details data view. Calls correlated in this way are represented by a Session ID instead of a Call ID. See the table below for more information about the Session ID.

If session information is available for a call, a link to correlated Session Details is available in the **Session ID** column. The following tables summarize the data that is provided on the Session Information page.

Session Information

Item	Description
ID	The session identifier, assigned by NetQoS UC Monitor, for the selected session. A "session" consists of correlated call legs that the Collector has identified as belonging to the same call. Matches the Session ID in the **Calls Overview** summary table.
Origination Number	The phone number or SIP URI of the phone or endpoint that placed the call.
Origination Called Number	The phone number or SIP URI that was dialed.
Destination Number	The phone number or SIP URI where the call was received.
Origination Time	The date and time the call began.
Duration	The length of the call, in minutes and seconds.
Media Type	The type of data stream in the call, either audio or video.

Origination and Destination Information

Detailed information about the phones or endpoints that participated in the call is provided in separate tables. For the **Origination** (the phone or endpoint that placed the call) and **Destination** side (the phone or endpoint that received the call), the following information is provided, if available.

Item	Description
Endpoint Name	The hostname of the endpoint, or the name associated with the device.
User Agent	The firmware version and build of the software that the phone or endpoint is reporting.
URI	The SIP universal resource identifier (URI) of the logged-in user associated with this endpoint.

Other Information

This section is usually included to provide information to identify conference calls.

If available, the **Conference URI** is provided. This URI is generated by the Conferencing Server and usually includes the URI of the user who set up the conference call.

Session Details Table

If call data is available from a set of call legs that the Collector has identified as being from the same call, a separate data view is displayed to show statistics for each of the correlated data streams. The correlated streams are identified by a shared **session ID**.

The following table summarizes the data that is provided in the **Session Details** view:

Item	Description
Call ID	The call identifier, assigned by NetQoS UC Monitor, for the selected call. Matches the ID in the **Calls Overview** summary table. Provides a drilldown path to the Call Details Report.
Origination Time	The date and time the call began.
Origination Number	The phone number or SIP URI of the phone or endpoint that placed the call.
Origination Location/ Media Device	The Location of the phone or endpoint that placed the call, or the media device that forwarded the call from a point in the PSTN.
Destination Number	The phone number or SIP URI of the phone or endpoint that received the call.
Destination Location/ Media Device	The Location of the phone or endpoint that received the call, or the media device that forwarded the call to a point in the PSTN.
Duration	The length of the call, in minutes and seconds.
Media Type	The type of data stream, either audio or video.
Origination MOS	The Mean Opinion Score (MOS) value of the data stream perceived at the origination endpoint or phone. See Appendix A, “Calculating a Mean Opinion Score” on page 147 for more information. Only applicable to audio streams.
Destination MOS	The MOS value of the data stream as perceived at the destination endpoint or phone. Only applicable to audio streams.
Call Setup Failure Code	If the call failed during the setup phase, the code that the call server returned, indicating the type of failure. See “Call Failure Cause Codes” on page 138 for more information.

Tips for Viewing the Calls Reports

For various reasons, such as high call volume or a long time frame, the Calls Overview might contain many calls. Like other reports, it provides multiple sorting, paging, and filtering options, and if you are monitoring Microsoft, it provides additional quick-filtering options to filter the data by Media Type. If you’re not seeing the data you are looking for, it helps to be aware of the various filtering and sorting options.

Filters, Paging, and Sorting

Pay close attention to the filters being applied. Until you become accustomed to accessing and viewing correlated call data and Session Details, try viewing the same time frame using different quick-filtering options, and sort the data in the resulting table by **Media Type** or by **Session ID**.

When sorting through a long list of calls, be aware that you might also need to select from the page options available at the bottom of the **Calls Overview** table to see all call data. For example, you can increase the **Max Per Page** setting and see more calls without paging forward. Or you can decrease the time frame to see fewer calls.

Typically, an easy way to find an audio/video conference call might be to sort the Calls Overview table by **Session ID**, but you might still need to page forward or back to see every table entry that has a session ID.

Conference Calls

Conference calls are not specifically designated as such in the Calls Overview table, but you can find them by drilling to Session Details. Conference calls receive a Session ID, which is a link to more information. When you click the Session ID for a conference call, a **Conference URI** is provided under the section labeled **Other Information** on the page of Session Information.

Reporting of Uncorrelated Call Legs

If one or more intermediate devices handled a given call, that single call is displayed in the Calls Overview table as multiple call legs. Here's an example:

Call ID 6381; **Origination Time**: 06/12/2009 18:23:18; **Origination Number**: 15225678910; **Origination Location/Media Device**: 172.12.3.45; **Destination Number**: 1718; **Destination Location/Media Device**: mediator01.netqos; **Duration**: 37 secs; **Media Type**: Audio

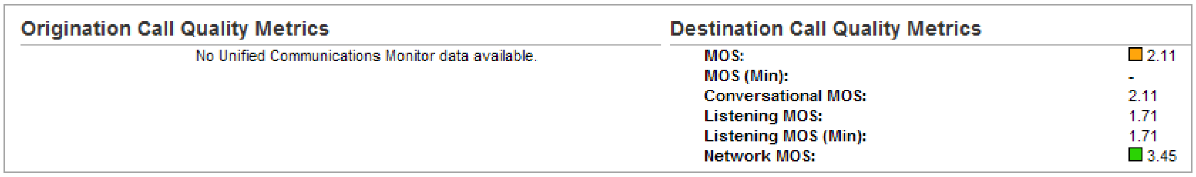
Call ID 6382; **Origination Time**: 06/12/2009 18:23:18; **Origination Number**: 15225678910; **Origination Location/Media Device**: mediator01.netqos; **Destination Number**: Jack.OShea@netqos.com; **Destination Location/Media Device**: Austin HQ; **Duration**: 37 secs; **Media Type**: Audio

These separate legs represent a single call, as you can see from the identical Origination Times, Origination Numbers, and Durations. They are shown in separate table rows because the call created distinct "legs":

- One leg traveled between Herbert (at 5225678910, the **Origination Number** in the PSTN) and the Mediation Server (mediator01), which translated it for the VoIP network.
- The other leg traveled between the Mediation Server (mediator01.netqos is the **Origination Media Device**) and Jack (the **Destination Number**, a URI in this case).

The separate metrics are useful for determining the location of a performance issue—at the Mediation Server, for example.

The presence of quality metrics in a **Call Quality Metrics** data view depends on the endpoints that handled a given call leg. If you clicked the Call ID that corresponds to the first call leg discussed above, you would see that no quality information is available in the Call Details for Herbert's phone in the PSTN:



Origination Call Quality Metrics

No Unified Communications Monitor data available.

Destination Call Quality Metrics

MOS:	🟧 2.11
MOS (Min):	-
Conversational MOS:	2.11
Listening MOS:	1.71
Listening MOS (Min):	1.71
Network MOS:	🟩 3.45

But the call leg that traveled from the Mediation Server to Jack's Communicator instance provides a full set of quality metrics for both the Origination and Destination sides of the call because both endpoints are able to report these metrics.

Calls Export

The Calls Export report is an export-only feature that provides data from the UC Monitor database, formatted as a spreadsheet. In some cases, the data available for export in the Calls Export format is not available in other reports.

No charts are included in this report. The raw data provides a deeper insight into call activity and performance on the network and is useful for troubleshooting Incidents. The resulting spreadsheet identifies the phone numbers and IP addresses of the phones within each Location, which can be useful for fine-tuning Location definitions.

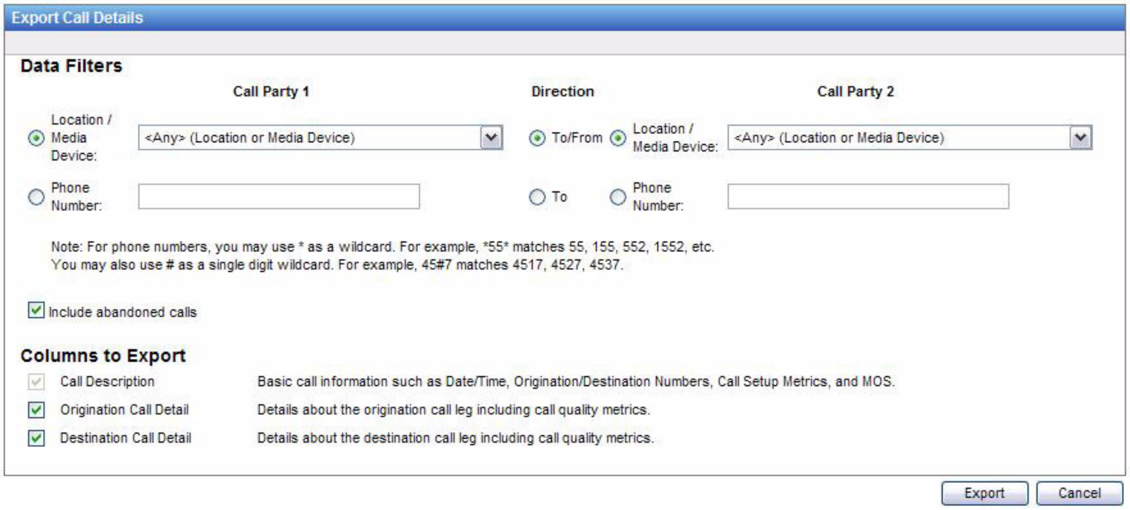
Data collected from watched calls (by means of the Call Watch feature) is not available for export.

You can change some report settings to select the details to include in the spreadsheet. You can select the individual phone, the Location, media device, or a pair of Locations or media devices whose call data you want to export.

To export details about call data:

1. In the navigation links, click **Troubleshooting > Calls > Export**.

   The Export Call Details page is displayed:



Export Call Details

Data Filters

Call Party 1		Direction	Call Party 2	
● Location / Media Device:	<Any> (Location or Media Device)	● To/From	● Location / Media Device:	<Any> (Location or Media Device)
○ Phone Number:		○ To	○ Phone Number:	

Note: For phone numbers, you may use * as a wildcard. For example, *55* matches 55, 155, 552, 1552, etc.
You may also use # as a single digit wildcard. For example, 45#7 matches 4517, 4527, 4537.

☑ Include abandoned calls

Columns to Export

☑ Call Description	Basic call information such as Date/Time, Origination/Destination Numbers, Call Setup Metrics, and MOS.
☑ Origination Call Detail	Details about the origination call leg including call quality metrics.
☑ Destination Call Detail	Details about the destination call leg including call quality metrics.

   This page provides the following options for the data to include and the database columns to export:

Field	Description
Data Filters	Set limits on the data that is exported.
Group Location/Media Device (Call Party 1) Location/Media Device (Call Party 2)	You can choose to export call data for: • a single group of managed items • a pair of groups of managed items • a single Location, media device, or phone number (see below) • a pair of Locations or media devices • a pair that consists of a Location and a media device • a pair of phone numbers • a pair that consists of a phone number and a Location or media device The lists include all available groups, Locations, and media devices. To export call data for a single group or managed item, select it from the **Call Party 1** list. Then click to enable the **To/From** directional indicator (see below). This option disables the direction filter and exports call data from all call legs that involve the item you selected. To export call data for a pair of groups, Locations, or media devices, select them from the **Call Party 1** and **Call Party 2** lists. You can then select a direction for the data flows to export (see below).
Phone Number	The directory number (DN) of a phone whose call data you want to export. Use the format 8887675443. Enter a direct-dial number. Individual extensions are not supported. Do not use hyphens (-) or periods (.) to separate the area code and number. International numbers (with country code appended) are not supported. Wildcards are supported. Use an asterisk (*) to indicate a wildcard substitution. Data corresponding to multiple phone numbers can be exported in this manner.
Direction	Determines the call data to include. The direction is an indication of the calling party (which placed the call) and the called party (which received the call) and thus indicates whether call setup metrics are included. For any selection, both directions (legs) of a call are always included. • Select **To** to export only the call data taken from calls made by the Call Party 1 **to** the Call Party 2. • Select **To/From** to export call data for all calls associated with the two call parties. To export data for a single Location or media device, select it as the Call Party 1, select a direction (**To** or **To/From**), and leave the default option, `<Any> (Location or Media Device)`, for the Call Party 2.
Include abandoned calls	Select the check box if you want to include data from calls that were connected successfully but were abandoned before data was sent.
Columns to Export	Click to select the columns from the database table that you want to include in the exported spreadsheet.
Call Description	Includes the following information about the call: Date/Time of call; called number; call setup metrics, MOS. Cannot be disabled in this version of NetQoS UC Monitor.

Field	Description
Origination Call Detail	Click to include detailed information about the phone that placed the call, including the phone number, make and model, its call server, codec, firmware version, serial number, and switch connection type. Availability of this information depends on the type of phone.
Destination Call Detail	Click to include detailed information about the phone that received the call, including the phone number, make and model, its call server, codec, firmware version, serial number, and switch connection type. Availability of this information depends on the type of phone.
Time Period	The time frame of the data to export. Aligned with the Time Frame selector used in reports; offers additional option of One Month.

2. When you have made your selections, click **Export**.
3. The File Download dialog box is displayed. You are asked whether you want to open or save the file. For fastest download times, click **Save**.
4. Enter or browse to the file save location and click **OK**.

   Note: We do not recommend the option to open the file. If you select this option and are attempting to export a large amount of data, the download may take longer, and Microsoft Excel, the default program that will likely be used to open the file, may not be able to handle a file of that size very easily.

The details you selected are exported to a file in `.csv` format. The process may take a few minutes to complete, depending on the amount of data available in the database and the parameters you selected.

Tips for Viewing Exported Data in Excel

If you open the exported file in Microsoft Excel, note that any fields containing data that is significantly wider than the available column area are shown as “###”. To see the data in those fields, expand the columns by clicking and dragging the resize indicator until the data is shown. The first row of the spreadsheet lists the parameters that were selected for export.

By default, Excel does not offer a format for showing a full date/time string in a single cell. To see date/time details in a single cell, you can specify Custom formats. Excel provides several custom formats that are suitable for this type of cell format, including the `m/d/yyyy h:mm` format, but this format lacks seconds. A separate procedure is needed to add the seconds.

To format an Excel spreadsheet to see a date/time format with seconds:

1. Select the column(s) you want to reformat.
2. Right-click over the column, and select **Format Cells**.
3. On the **Number** tab, click to set the Category to **Custom**.
4. In the **Type** field, click to select one of the d-m-y options, such as **d-mmm-yy**.
5. By typing in the field provided, edit your selection to be something like this: `m/d/yyyy h:mm:ss`.

   Or, to add leading zeroes, enter `mm/dd/yyyy hh:mm:ss`.
6. Click **OK**. The columns are reformatted to include the additional data.

Phones Report

Detailed information about the phones and endpoints known to all monitored call servers is available in the Phones report pages. This information is useful for troubleshooting device-related issues and failover situations, such as excessive phone registrations or missing or new phones.

The last 24 hours' worth of phone data in the UC Monitor database is shown.

The main **Phones** navigation link accesses the **Phones** data view, a table listing all phones registered system-wide. By default, the phones in the list are sorted by the time and date of their last call activity. The following table summarizes the information in the **Phones** List:

Item	Description
ID	An identifier, assigned by NetQoS UC Monitor, for each phone that has been discovered during monitoring of the UC system. Provides a link to the Phone Details Report page, with more detailed information about each phone.
IP Address	The IP address of the phone.
Phone Number	The directory number (DN) of the phone.
Name	The name or MAC address of the phone.
Location	The Location definition being applied to this phone. Location definitions are based on IP address subnets. See the *UC Monitor Administrator Guide* for more information.
Call Server	The call server where this phone was most recently registered.
Status	The most recent status information about this phone.
Last Activity	The date and time of the last call activity seen from this phone.

The ID number assigned to the phone in the system is a hyperlink to detailed information about a selected phone. See "Phone Details Report" on page 131 for more information. The phone IP address is a hyperlink to the phone's Web page, where status and error information is available.

Phone Details Report

The Phones List in the Phones Report provides preliminary details about each phone known to the call servers in the system. You can use this report to troubleshoot a hardware issue or a Call Server Incident.

When you click a hyperlinked phone ID number, you access the Phone Details Report. This report contains both phone details and call details from the last 24 hours' worth of phone data in the UC Monitor database for the selected phone.

The following information about the phone itself is available in the **Phone Details** view:

Field	Description
ID	The sequential number assigned to this phone when it was first discovered.
Name	The name or MAC address of this phone, or the hostname of the endpoint.
Phone Number	The DN assigned to this phone.
IP Address	The IP address of this phone.

Field	Description
Location	The Location definition being applied to this phone. Location definitions are based on IP address subnets. See the *UC Monitor Administrator Guide* for more information.
Model/Type	The phone hardware model and type.
Call Server	The call server where this phone is currently registered.
Previous Call Server	(*Cisco Only*) The call server where this phone was previously registered.
Protocol	The protocol being used by this phone for call setup.
Last Activity	The date and time of the last call activity seen from this phone.
Status	(*Cisco Only*) The most recent status information about this phone.
Previous Status	(*Cisco Only*) The previous status information about this phone.
Status Time	(*Cisco Only*) The date and time that the current status was updated in the UC Monitor database.
Firmware Version	The version of the phone firmware that is running on this phone.
Serial Number	The serial number assigned by the phone manufacturer.
Switch Address, Name, Port	The IP address and hostname of the switch the phone is using to send data to its call server, and the switch port number through which phone traffic is passing.

By default, the **Phone Call Details** table contains data from all calls made from the selected phone in the last 24 hours (from the time the page was accessed). This view provides information about the volume and quality of calls made by this phone recently, the call server with which it is currently registered, and any recent call setup failures. You can use the quick settings options to select the types of calls to view (the default Media Type is "`Audio and Video`") and the call direction; the default direction is "`To/From Phone`," but you can select an option that filters the Phone Call Details view so that only a single direction—from or to the selected phone—is included in the report.

By default, some of the available columns are excluded from the report so that the table can be more easily viewed, without scrolling. You can enable these columns by means of the **Display on Page** options in the Phone Details Settings dialog box.

The following information is available by default in the **Phone Call Details** table:

Column	Description
Call ID	The internal ID number assigned to the call by the collection device. These IDs are useful for identifying the calls in other reports. A link to the Call Details Report for this call.
Origination Time	The time and date when the call was made.
Origination Number	The directory number (DN) of the phone or endpoint that placed the call. Call quality statistics are for incoming data streams (data received by this phone). To see the phone hostname, check the **Phone Details** view, above

Column	Description
Origination Location/ Media Device	The assigned Location of the phone or endpoint that placed the call. Or the name of the gateway device through which the call was sent to the PSTN. Could be `<Unassigned>` or another default Location. See "Call Legs and Monitoring Reports" on page 65 for an explanation.
Destination Number	The DN of the phone that received the call. Call quality statistics are for incoming data streams (data received by this phone). To see the phone hostname, check the Phone Details view, above.
Destination Location/ Media Device	The assigned Location of the phone that received the call, or the name of the gateway device that handled the PSTN call.
Duration	The length of the call, in minutes and seconds.
Media Type	The type of call: either Audio or Video.
Origination MOS	The Mean Opinion Score (MOS) Listening Quality (LQK) is a call quality score that is updated every second during a single voice stream. This value applies to the call leg traveling toward the phone that placed the call. Appendix A, "Calculating a Mean Opinion Score" on page 147 contains a full discussion of MOS values and how they are derived.
Destination MOS	The MOS value of the call leg traveling toward the phone that received the call.
Call Setup Failure Code	If the call failed during the setup phase, the code that the call server returned, indicating the type of failure. See "Call Failure Cause Codes" on page 138 for more information.

Capacity Planning Reports

The Capacity Planning report pages are intended to help network engineers plan for network growth and track actual UC system usage statistics. They are helpful for determining the current operating levels of key UC components.

Reports in the Capacity Planning section focus on quality, volume, and utilization:

- **Quality** reports provide a view of the effects of call volumes on call performance.
- **Volume** reports provide detailed data about the utilization rates and performance of call servers and gateway media devices and help you track trends in call setup failure rates.
- The **Top Volume** report allows you to rapidly locate the areas of the network with the highest call volume.
- **Utilization** reports, which include per-gateway or per-interface statistics, are especially useful for understanding telephony resource usage and negotiating contracts with service providers.

The Capacity Planning section of the UC Monitor Management Console provides the following reports:

Report	Description
Audio Call Quality Report	Shows information about call volumes and call quality. MOS values for the entire system are graphed over an hourly scale. Filtering is available by Location and by media device. For more information, see "Audio Call Quality Report" on page 135.
Call Volume Audio Report	Shows information about call volumes and call setup performance, with a particular emphasis on failures. A breakdown of the types of call failures that occurred is available. You can use this report to determine busy-hour call attempts (BHCA) and busy-hour call completions (BHCC) on your network. Two types of volume report are available: • "Call Volume Audio Report" on page 137 • "Call Volume Total Report" on page 140
Top Volume Report	Compares the call volume of the groups, Locations, phones, or endpoints with the highest utilization during the selected time frame. Provides easy naviagation to the Calls Overview Report.
Voice Interface Utilization Report	Shows information about voice gateway, media device, and interface usage and capacity. Lists individual gateway voice interfaces and shows per-interface statistics.
Voice Interface Top Interfaces Report	Shows individual utilization statistics for all gateway voice interfaces, with the most heavily utilized interfaces listed first.

Observations in Capacity Planning Reports

The observation counts shown in all UC Monitor reports provide a gauge of the reliability of the statistics shown and also measure the relative level of system activity that applied during a particular time period. Stated simply, more observations equal greater system activity and, unless a unusually high level of activity was occurring, greater result validity.

Where Calls Originated and Call Minutes are the units of the observation counts that are used in the Call Performance reports, different units are used in the Capacity Planning reports. The units used for Call Performance reports are the same as those that apply to the performance thresholds for call setup and call quality. These thresholds do not generally apply to the Capacity Planning reports, which measure volume and utilization metrics. In the Capacity Planning section, the MOS is treated as a secondary statistic to show the effects of utilization on quality and is only included in the Audio Call Quality Report.

The following table defines the observation units that are used in Capacity Planning reports:

Observation Unit	Description
Calls Established	Calls that were successfully initiated during the selected time period. Includes both calls that were placed by phones or endpoints inside the monitored system and those that were placed by phones outside the system to phones or endpoints inside the system.

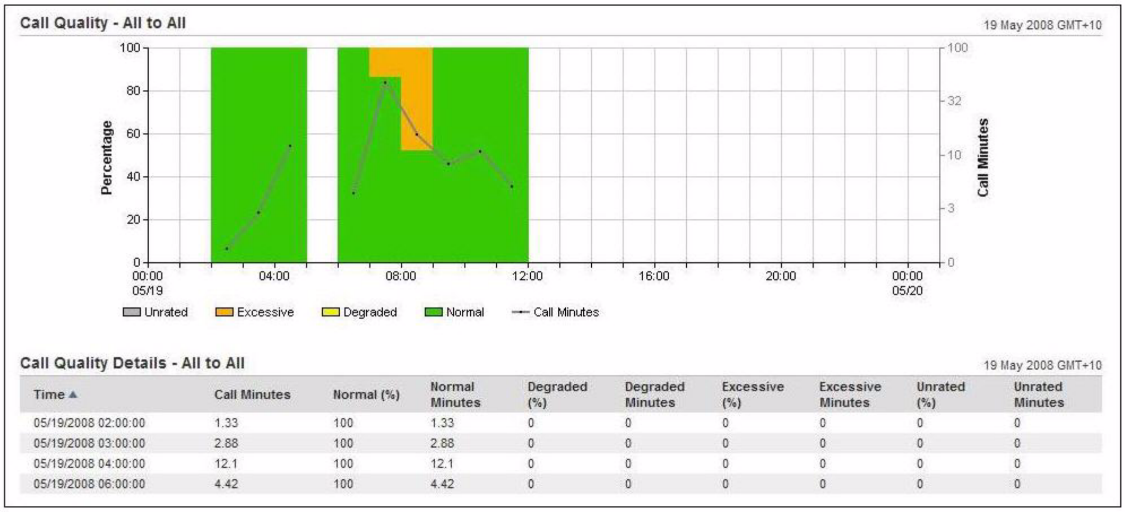
Observation Unit	Description
Calls Active	Calls that were *active* during the selected time period, but not necessarily *initiated* during that time period.
Calls	The total number of calls that were running between a selected pair of Locations or groups, or between a selected Location and any other Location, in both directions.
Total Calls	The total number of calls in the system during the selected time period.
Call Minutes	The number of minutes when calls of any type (audio only or audio and video) were running between a selected pair of Locations or groups, or between a selected Location and any other Location, in both directions.
Total Minutes	All minutes when calls of any type were running (that is, active) on the network.

Audio Call Quality Report

The Audio Call Quality Report provides a view of UC Monitor quality ratings that helps you track audio-only call quality system-wide. Mean Opinion Score (MOS) values are graphed over an hourly scale showing the percentage of all VoIP calls on the network that were rated Normal, Degraded, or Excessive. A secondary axis indicates the number of call minutes that contributed to the ratings.

By default, VoIP call activity to and from all groups and all Locations is graphed, using colors to show quality ratings. However, you can filter by group, Location, media device, or gateway voice interface by clicking the **Settings** link. A quick-filtering option lets you see quality as judged by MOS or network MOS values. See "Call Quality Metrics" on page 78 for information about these metrics.

Call minutes are graphed with a gray line graph to show the number of observations that composed the quality bar chart.



Call Quality Details - All to All

19 May 2008 GMT+10

Time ▲	Call Minutes	Normal (%)	Normal Minutes	Degraded (%)	Degraded Minutes	Excessive (%)	Excessive Minutes	Unrated (%)	Unrated Minutes
05/19/2008 02:00:00	1.33	100	1.33	0	0	0	0	0	0
05/19/2008 03:00:00	2.88	100	2.88	0	0	0	0	0	0
05/19/2008 04:00:00	12.1	100	12.1	0	0	0	0	0	0
05/19/2008 06:00:00	4.42	100	4.42	0	0	0	0	0	0

The Call Quality Details table, shown in the above image, is not included by default. To include it, click to select the **Call Quality Details** option in the **Display on Page** area of the Settings dialog box. The table shows the raw statistics used in the quality graph, including the number of call minutes observed for each hour of the day and their quality ratings. Clear the same option to remove this table from the report.

The following table describes the data that is available on the Call Activity Quality Report page:

View or Metric	Description
Call Quality - All to All	Call quality ratings for calls traveling among all Locations or, if any system groups or custom groups are defined, among all groups. Calls from the PSTN to these groups or Locations are also included. Quality ratings are based on the performance thresholds being applied to your Locations and are graphed as a percentage of all call minutes per hour. Click the **Settings** link and select any group, Location, or media device to narrow the data by that Location or device.
Call Quality Details Table	
Time	The hour of the day when calls were active on the network.
Call Minutes	The number of call minutes logged during that hour. Units are hours. Provides a sense of the scope of activity and helps determine the significance of the data, based on sample size. See "Observations in Capacity Planning Reports" on page 134 for more information.
Normal (%)	The percentage of call minutes with MOS values in the Normal range of the assigned threshold.
Normal Minutes	The number of call minutes with MOS values in the Normal range of the assigned threshold.
Degraded (%)	The percentage of call minutes with MOS values in the Degraded range of the assigned threshold.
Degraded Minutes	The number of call minutes with MOS values in the Degraded range of the assigned threshold.
Excessive (%)	The percentage of call minutes with MOS values in the Excessive range of the assigned threshold.
Excessive Minutes	The number of call minutes with MOS values in the Excessive range of the assigned threshold.
Unrated (%)	The percentage of call minutes that had no threshold values applied. The performance threshold for MOS was disabled for these Locations. See the *UC Monitor Administrator Guide* for more information.
Unrated Minutes	The number of call minutes that had no threshold values applied. The performance threshold for MOS was disabled for these Locations.

You can determine what's shown in the Call Activity Quality Report by selecting or clearing options in the Settings dialog box. Any **Display on Page** settings you select are associated with your user account and persist across login sessions.

Call Volume Audio Report

The Call Volume Audio Report provides a view of audio-only call volumes and call setup failures.

Information in this report is useful for tracking call volumes for:

- Locations (or groups of Locations)
- media devices
- call servers

Call setup failures are broken out by their cause. You can also use this report to determine busy-hour call attempts (BHCA) and busy-hour call completions (BHCC) for audio-only calls on your network. The complementary Call Volume Total Report shows volume levels for all calls, including audio-only and video calls.

The Call Volume category helps you understand both audio call volume metrics and call setup metrics on your network. By default, audio-only call activity to and from all Locations is shown in the **Call Volume** view. However, you can filter on call server or call server group, Location or group, media device, or voice gateway interface by clicking the **Settings** link.

The main unit of measurement used for the Call Volume Audio Report is calls attempted, or all audio-only calls that phones in the monitored system subnets attempted to place during the selected time period, either successfully or unsuccessfully.

The **Call Volume** data view includes the following information:

Metric	Description
Calls completed	The number of audio-only calls that were successfully completed during the selected time period. Includes both calls that were placed by phones in the monitored system and those that were placed by phones *outside* the system to phones *inside* the system. See "Observations in Capacity Planning Reports" on page 134 for more information about the observation units used in this report.
Calls attempted	The basic unit of measurement used for the Call Volume Report. All calls in the monitored system that were completed successfully, plus call setup failures.
Setup failures	Calls that failed during the setup phase. Slightly different from the traditional telecom "blocked" metric; includes any call setup failure, from any cause. The **Call Setup Failure Breakdown** chart provides more information about the causes of any failures.
Grade of Service	A ratio of call failures to call attempts. A percentage of probability, expressed as a decimal fraction. Grade of Service (GoS) provides an estimation of the probability that an attempted VoIP call will receive a busy signal. In more technical terms, GoS is the probability that a call in a circuit group could be blocked or delayed for more than a specified interval. This value is always expressed with reference to the busy hour when traffic intensity is greatest. The most desirable GoS value is 0. Grade of service is reported from the perspective of the Location or gateway device placing the calls (the outgoing direction). Grade of Service is calculated using the following equation: `number of setup failures / number of call attempts`

Any call failures that occurred during the reporting period can be seen in a pie chart in the **Call Setup Failure Breakdown** view. By default, this view is included in the report. To remove it from the report, click the **Settings** link. In the Settings dialog box, enable the **Call Setup Failure Breakdown** option in the **Display On Page** area. The Grade of Service data points can also be removed from the report.

Any **Display on Page** settings you select are associated with your user account and persist across login sessions.

The Call Setup Failure Breakdown chart shows a distribution of the most commonly observed call setup error codes. For more information about these codes, see the following topic, "Call Failure Cause Codes".

Call Failure Cause Codes

Call failure types are provided by the call server. The Failure Cause Code Breakdown view of call activity data shows the types of failures that occurred most frequently. Cisco Unified Communications Manager currently uses the following call failure cause codes. More information about many of these codes is available on the Cisco Web site in the Communications Manager CDR documentation.

Cause Code	Description	Cause Code	Description
0	No error	53	Outgoing calls barred within CUG
1	Unallocated/unassigned number	54	Incoming calls barred
2	No route to specified transit network	55	Incoming calls barred within Closed User Group (CUG)
3	No route to destination	57	Bearer capability not authorized
4	Send special information tone	58	Bearer capability not presently available
5	Misdialed trunk prefix	62	Inconsistency in outgoing access information and subscriber class
6	Channel unacceptable	63	Service or option not available, unspecified
7	Call awarded and being delivered in an established channel	65	Bearer capability not implemented
8	Preemption	66	Channel type not implemented
9	Preemption--circuit reserved for reuse	69	Requested facility not implemented
14	QoR: ported number	70	Only restricted digital information bearer capability available
16	Normal call clearing	79	Service or option not implemented, unspecified
17	User busy	81	Invalid call reference value
18	No user responding	82	Identified channel does not exist
19	No answer from user—user alerted	83	A suspended call exists, but this call identity does not

Cause Code	Description	Cause Code	Description
20	Subscriber absent	84	Call identity in use
21	Call rejected	85	No call suspended
22	Number changed	86	Call having the requested call identity has been cleared
23	Redirection to new destination	87	User not member of Closed User Group (CUG)
24	Call rejected due to feature at the destination	88	Incompatible destination
25	Exchange – routing error	90	Non-existent CUG or destination number missing
26	Non-selected user clearing	91	Invalid transit network selection
27	Destination out of order	95	Invalid message, unspecified
28	Invalid number format—address incomplete	96	Mandatory information element is missing
29	Facility rejected	97	Message type non-existent or not implemented
30	Response to `STATUS ENQUIRY`	98	Message not compatible with call state or message type non-existent or not implemented
31	Normal, unspecified	99	Information element /parameter non-existent or not implemented
34	No circuit/channel available	100	Invalid information element contents
35	Call queued	101	Message not compatible with call state
38	Network out of order	102	Recovery on timer expiration
39	Permanent frame mode connection out of service	103	Parameter non-existent or not implemented—passed on
40	Permanent frame mode connection operational	110	Message with unrecognized parameter discarded
41	Temporary failure	111	Protocol error, unspecified
42	Switching equipment congestion	122	Precedence level exceeded
43	Access information discarded	123	Device not preemptable
44	Requested circuit/channel not available	124	Conference full
46	Precedence call blocked	125	Out of bandwidth
47	Resource unavailable, unspecified	126	Call split
49	Quality of Service not available	127	Interworking, unspecified
50	Requested facility not subscribed	128	Drop any party/drop last party conference feature
52	Outgoing calls barred	129	Precedence out of bandwidth

Call Volume Total Report

The Call Volume Total Report shows traffic volume levels for all calls, including audio-only (VoIP) and video calls.

Note: Video calls are only monitored in Microsoft Office Communications Server 2007 environments.

The Call Volume category helps you understand both call volume metrics and call activity metrics on your network. By default, all call activity (audio and video, where applicable) to and from all Locations is shown in the **Call Volume** view. However, you can filter on call server or call server group, Location or group, media device, or voice gateway interface by clicking the **Settings** link.

To help you quickly access a filtered view of the report, two quick-filtering options are available just above the **Total Volume** view. These options let you filter the calls included in the report:

Setting	Description
Include volume of	Select the type of calls to include in the Total Volume data view, one of the following: • Audio and Video (calls of all types) • Audio • Video
Show calls	Select the state of the calls to include in the data view, either: • **Established**—Initiated during the selected monitoring interval, or • **Active**—Ongoing during the selected monitoring interval, but possibly initiated at another time Your selection determines the metric that is graphed on the left Y axis. See "Observations in Capacity Planning Reports" on page 134 for more information about observation units.

Quick-filtering options are associated with your user account and persist across login sessions.

The main unit of measurement used for the Call Volume Total Report is **calls established**, or all calls that were successfully placed during the selected time period, either to or by phones in the monitored system subnets.

The **Total Call Volume** data view includes the following information:

Metric	Description
Calls Established	The number of calls of all types (including audio-only and video calls) that were successfully initiated during the selected time period. Includes both calls that were placed by phones or endpoints inside the monitored system and those that were placed by phones *outside* the system to phones or endpoints *inside* the system. The bar graph indicates the number of **calls established** (graphed along the left Y axis) and the number of **minutes** when calls were active (graphed along the right Y axis). See "Observations in Capacity Planning Reports" on page 134 for more information about the observation units used in this report.

Metric	Description
Calls Active	The number of calls of all types (including audio-only and video calls) that were active during the selected time period, but not necessarily initiated during that time period. Shows the timeframe when calls were active. The bar graph indicates the number of **active calls** (graphed along the left Y axis) and the number of **minutes** when calls were active (graphed along the right Y axis).
Video Calls	Calls that included a video component (that is, contained both audio and video streams).
Audio Calls	Calls that only contained an audio stream (with no video).
Total Minutes	All minutes when calls of any type were running on the network. If the Total Minutes line graph appears by itself (that is, with no corresponding bar graph), it is showing call minutes from calls that were established during a previous reporting interval but still active during the interval being graphed.

Just below the Total Volume view is an optional table, the **Total Volume Details** table. To include it in the report, use the Settings dialog box and check the **Display on Page** option. The Total Volume Details table includes the following detailed information about the audio and video calls included in the Call Volume Total report:

Metric	Description
Time	The time of day when calls were placed. Usually shows one hour per table row.
Total Calls	The total number of calls in the system during the indicated time period. See "Observations in Capacity Planning Reports" on page 134 for more information.
Audio Calls	The total number of audio-only calls in the system during the indicated time period.
Video Calls	The total number of calls that contained both audio and video streams during the indicated time period.
Total Minutes	All minutes during the indicated time period when calls of any type were running.
Audio Minutes	All minutes during the indicated time period when audio-only calls were running.
Video Minutes	All minutes during the indicated time period when calls containing both audio and vide streams were running.

Top Volume Report

The Top Volume report compares the call volume of the groups, Locations, phones, or endpoints with the highest utilization during the selected time frame. Think of it as a list of the "top talkers" at a particular point in time. By default, all calls—audio-only, video-only, or audio and video—are considered when compiling the list of top call volumes. You can find this report in the Call Volume section of the Capacity Planning reports.

The **Volume** bar chart shows a comparison of call volumes among the groups, Locations, or phones with the highest volumes. Each bar represents a relative activity level so that you can easily compare call volumes among busy Locations.

To help you quickly access a filtered view of the report, two quick-filtering options are available just above the Top Volume view. These options let you filter the Locations, groups, phones, or endpoints included in the report:

Setting	Description
Media Type	Select the type of calls to include in the Top Volume data view, one of the following: • Audio and Video (calls of all types) • Audio • Video By default, calls of all types are included.
Calculate using	Select the observation units to use when selecting Locations or groups to include in the list of "top" talkers in the data view, either: • **Calls**—Initiated during the selected monitoring interval, or • **Call Minutes**—Ongoing during the selected monitoring interval, but possibly initiated at another time Your selection determines the metric that is graphed on the left Y axis. See "Observations in Capacity Planning Reports" on page 134 for more information about observation units.

The values in the **Calls** column are hyperlinks to the "Calls Overview Report," filtered by the selected group, Location, phone, or endpoint as the sender or recipient of calls, and showing only calls from the same time frame as the current Top Volume report.

In the **Top Phones Volume** view, the phone numbers or SIP URIs shown in the **Phone Number** column are hyperlinks to the "Phones Report," filtered to show call details for any calls involving the same phone or endpoint during the time period of the Top Volume report. In addition to information about the origination and destination of a selected call, you can also see the MOS and any applicable call setup failure information.

If no phone number is available for an endpoint, its IP address is provided in the **IP Address** column. Where available, the IP address is a hyperlink to the phone Web page, which provides hardware and software information about the phone. The phone name is also shown in the **Name** column.

Voice Interface Top Interfaces Report

A report of voice gateway utilization that provides individual gateway voice interface statistics. Use this report to find underutilized interfaces and check for overburdened interfaces, where performance may deteriorate.

Statistics for all known gateway voice interfaces are included. The busiest (that is, most heavily utilized) interfaces are shown first.

Important: The Administrator should make sure that all known gateway voice interfaces have the number of channels correctly configured (the **Discovered Capacity** parameter). The Collector can usually get this capacity information from polling the gateway, but if it changes, this information is not updated. The Top Interfaces report uses the known channel capacity for each interface to calculate utilization as a percentage of capacity. This report is therefore less accurate if the device MIB is incorrectly reporting the gateway voice channel capacity.

The Voice Interface Top Interfaces Report contains the following information:

Data or View	Description
Top Interfaces	The utilization of all gateway voice interfaces on all gateway devices in the monitored system over a particular time period (day, week, or month). All known interfaces are listed; those with the highest utilization are listed first.
Name	The name assigned to the interface. Click to drill down into an hourly breakdown of utilization for this interface. See "Voice Interface Utilization Report" on page 144 for more information about the drilldown view. By default, the interface name is based on information from the gateway and the naming convention employed by the trunking equipment. However, a UC Monitor Administrator can change the name of a discovered gateway voice interface during voice gateway configuration. See the online Help for more information.
Utilization	The average utilization for the specified gateway voice interface. Expressed as a percentage of the interface capacity divided by the selected time period. Sorting on this column lets you quickly see whether any interfaces are underutilized by listing the least utilized interfaces first. The interface capacity was either discovered during monitoring or has been manually configured during voice gateway configuration. See the online Help for more information.
Maximum Utilization	The highest recorded utilization for the specified gateway voice interface during the selected time period, expressed as a percentage of the interface capacity. Maximum utilization is a good indicator of potential capacity issues. Even if the average utilization is low, the maximum utilization is significant because it often indicates the utilization during the "busy hour" of the day. It is calculated based on the interface capacity, multiplied by the time period. The capacity is either discovered during monitoring or has been manually supplied during voice gateway configuration.
Grade of Service (GoS)	An estimation of the probability that an attempted VoIP call will receive a "fast-busy" signal indicating that the call could not be set up. In more technical terms, GoS is the probability that a call in a circuit group could be blocked or delayed for more than a specified interval, expressed as a decimal fraction. This value is always expressed with reference to the busy hour when traffic intensity is greatest. Along with the utilization statistics, the GoS indicates whether utilization levels present any problems for call performance. If the GoS is minimal, 100% utilization is not a problem. The most desirable value for GoS is 0. Grade of service is reported from the perspective of the Location or gateway placing the calls (the outgoing direction). Grade of Service is calculated using the following equation: `number of setup failures/number of call attempts`
Call Minutes	The number of call minutes on which the utilization statistics are based. Specifically, the number of minutes that call data traffic was passing through the indicated interface.
Call Minutes Capacity	The total number of call minutes that the indicated gateway voice interface is capable of supporting during the selected time frame.

Click the **Settings** link to see filtering and display options for the Voice Interface Top Interfaces report. In the Settings dialog box, you can select a single voice gateway by which to narrow the data included in the report. If any system groups or custom groups are defined, you can also filter by group. By default, data from all groups is included in the report.

Voice Interface Utilization Report

The Voice Interface Utilization Report provides information about utilization levels on voice gateway-type media devices. By default, gateway voice interface utilization is shown as a percentage of the capacity of all interfaces on all voice gateways. However, by means of the Settings dialog box, you can drill down into information about utilization for a group, for a single gateway device, or for a single gateway voice interface.

Information in this report is useful for assessing:

- gateway device usage and capacity
- voice gateway interface utilization

Important: The Administrator should make sure that all known gateway voice interfaces have the number of channels correctly configured (the **Discovered Capacity** parameter). The Collector can usually get this capacity information from polling the gateway, but if it changes, this information is not updated. The Voice Interface Utilization report uses the known channel capacity for each interface to calculate utilization as a percentage of capacity. This report is therefore less accurate if the device MIB is incorrectly reporting the gateway voice channel capacity.

By default, any interfaces that the Administrator has deleted from the system (by means of the Voice Gateway Properties page) are not shown in the report; however, you can select any deleted interfaces that might have data for inclusion in the report from the Settings dialog box. Click the **Settings** link to access it. Deleted interfaces that have data appear in the **Voice Interface** list.

Also by default, the Interface Utilization Details Table is not included in the report. Enable it in the Settings dialog box if you want to include it.

The Voice Interface Utilization Report contains the views and data points shown in the table below:

View or Data Point	Description
% Utilization	The utilization of all gateway voice interfaces on all voice gateway devices over a particular time period (day, week, or month), shown as a percentage of their capacity. The utilization for a selected gateway or interface is based on the number of channels the gateway or interface has, multiplied by the time frame. For 1 hour, a single channel could provide 60 call minutes; thus, a full PRI interface (23 channels) could support: `23 channels x 60 minutes/hour = 1380 call minutes / hour = 33120 call minutes / day`

View or Data Point	Description
Call Minutes	The number of call minutes used to calculate the utilization statistics, shown as a gray line graph. This information can be removed from the report by means of the Settings dialog box. Provides a sense of the scope of activity and helps determine the significance of the data, based on sample size.
Interface Utilization Details Table	
Time	The hourly time period from which the detailed data was collected.
Call Minutes	The number of minutes that calls were active on the gateways included in the report, or, if a drilldown view, on the indicated gateway or gateway voice interface. By default, applies to all call minutes logged on all gateways in the system.
Total Capacity	The capacity of the gateway device or gateway voice interfaces included in the report. By default, applies to all gateway voice interfaces discovered in the system.
Utilization (%)	The total utilization of the gateway media device or gateway voice interfaces included in the report, expressed as a percentage of the total available capacity.

Click the **Settings** link to see filtering and display options for the Voice Interface Utilization report. In the Settings dialog box, you can select either a single voice gateway or a single gateway voice interface by which to narrow the data included in the report. If any system groups or custom groups are defined, you can also filter by group. By default, data from all groups is included in the report.

By default, the Interface Utilization Details Table is not included in the report. You can choose to display or hide the call minutes values in the Interface Utilization chart, as well as the Interface Utilization Details table via the Settings dialog box. Any **Display on Page** settings you select are associated with your user account and persist across login sessions.

Scalability Considerations and Report Performance

The UC Monitor Release Notes contain specific information about the total call volume that the UC Monitor Management Console, database, and Collector were designed to handle. Scalability considerations also affect report performance. As a general rule, the larger the database size and the greater the number of defined Locations and media devices, the longer report queries take to complete.

Following are some guidelines to let you know what to expect from the reporting interface with a very large UC Monitor deployment:

- Reports based on three-hour time periods of data generate reasonably fast, even with a very large database size.
- Reports based on a full day of data usually complete and display within 60 seconds; however, the Call Leg Details Reports can take a little longer to display.
- Reports based on a full week of data can take several minutes to display. The Call Performance Overview Report takes the longest: in our testing, it took as long as eight minutes or more to

completely display. The Call Leg Details can take some time as well: four to five minutes, in our testing.

- We recommend generating reports with a one-day time period if you find that reports based on a full week of data are taking too much time.
- We also recommend careful database maintenance. Pruning older data that is no longer needed will help keep the database at a manageable size and enable reports to generate faster. The UC Monitor Administrator can control database maintenance settings to keep the database to the minimum desirable size.

The *UC Monitor Administrator Guide* contains more information about database maintenance options.

APPENDIX A

Calculating a Mean Opinion Score

This appendix discusses the Mean Opinion Scores (MOS values) that are reported in UC Monitor reports.

The MOS, a telecommunications industry standard for the measurement of call quality, was developed in an attempt to create a system of objective ratings for audio signal quality. It is based on the results of years of testing with human subjects, who gave their opinion of the signal quality after hearing test signals with various impairments, such as jitter and latency. Defined in the International Telecommunications Union (ITU) Recommendation P.800, the MOS can now be calculated from the signal quality without the involvement of actual listeners.

The MOS scale ranges from 5.00 to 1.00, with 5.00 representing the highest quality—that is, a score representing an audio signal free from impairments—and 1.00 representing the lowest quality. The MOS value provided in UC Monitor reports is an average derived from multiple samples, unless otherwise specified.

In its G.107 Standard, the ITU provides a scale that relates MOS values to user satisfaction:

MOS Range	Likely User Opinion of Call Quality
4.3 - 5.0	Very Satisfied
4.0 - 4.3	Satisfied
3.6 - 4.0	Some Users Dissatisfied
3.1 - 3.6	Many Users Dissatisfied
2.6 - 3.1	Nearly All Users Dissatisfied
1.0 - 2.6	Not Recommended

The MOS value for a VoIP call leg partly depends on the codec used to packetize the audio signal. Codecs of different types therefore advertise different *theoretical maximum MOS values*—the highest possible score they are capable of achieving in the absence of other impediments, such as packet loss between the endpoints.

The MOS values in UC Monitor reports are calculated slightly differently in a Cisco or Avaya environment than they are in a Microsoft Office Communications Server system. See the following topics for information about the differences.

Cisco MOS Calculations

When monitoring Cisco IP telephony environments, NetQoS UC Monitor relies on the IP phones to gather data on the MOS values of the calls made on the monitored network. Each Cisco IP phone calculates and reports the MOS of the last call made or received to its call server. The Collector inspects the packets sent to the call server to find the MOS information being reported. For VoIP calls that were placed by phones in the PSTN, the Collector polls the gateway for MOS information.

The MOS calculated by Cisco phones is usually referred to as the listening quality MOS (MOS-LQ) to distinguish it from the conversational quality MOS (MOS-CQ), which is described in the ITU-T G.107 standard. Unlike MOS-CQ, MOS-LQ does not account for echo or delay.

To derive MOS values for IP phone calls, Cisco uses a proprietary algorithm based on P.VTQ, an ITU-T project to develop an objective, real-time quality assessment methodology based solely on IP packet information. Like the ITU E-Model, the Cisco algorithm allows for an estimation of voice listening quality in a VoIP call by taking into account perceptual weighting factors and the various quality impairment factors that affected the audio stream, such as the type of codec used.

While NetQoS UC Monitor relies on information from Cisco IP phones to report MOS values for calls that do not leave the data network, a different method is required when monitoring calls that involve a party in the PSTN. To calculate a MOS from voice gateway call legs using either MGCP or H.323, the Collector uses the ITU-T G.107 standard discusssed above in "Calculating a Mean Opinion Score" on page 147.

Avaya MOS Calculations

NetQoS UC Monitor uses a technique similar to that used in Cisco environments to calculate a MOS for Avaya phones and endpoints. As in a Cisco deployment, the Avaya phones calculate and report MOS values every few seconds during an active call. These phones use an algorithm similar to the Cisco voice gateways, using the ITU-T G.107 standard discusssed above in "Cisco MOS Calculations". The scores are thus based on MOS listening quality.

Microsoft MOS Calculations

As do the phones in a Cisco VoIP system, the endpoints in a Microsoft Office Communications Server 2007 system use advanced algorithms to objectively predict the results of a MOS test in which human listeners rated the quality of an audio signal. Endpoints that support VoIP and video quality metrics in a Microsoft system provide two types of MOS values, listening quality MOS (MOS-LQ) and conversational quality MOS (MOS-CQ), and the system also reports a Network MOS metric. Typically, the Office Communicator instances report these values and other quality metrics at the end of each call, sending a quality report to the Quality of Experience Monitoring Server.

The Microsoft **MOS-LQ** metric isolates the listening quality of audio by excluding bidirectional effects, such as delay and echo. By contrast, the **MOS-CQ** metric comprises the listening quality in each direction of the call, taking into account any impairments from delay and echo.

The **Network MOS** also attempts to predict the MOS-LQ of the audio signal received by the listener. But this value only takes into consideration the network factors, such as codec used, packet loss, packet reordering, packet errors, and jitter. Network MOS is not calculated in a Cisco VoIP environment.

The difference between Network MOS and Listening MOS is that the Network MOS considers only the impact of *network* factors on the listening quality, where the MOS-LQ metric also considers payload factors, such as speech level and noise level. The Network MOS value therefore helps to isolate network impediments on audio quality.

Because the Microsoft-proprietary codecs, RTAudio and Siren (used for conference calls), can operate in two bandwidth modes, the MOS-LQ and Network MOS predicted by Microsoft endpoints are reported on a wideband (WB) scale, which differs from the more familiar MOS scale discussed in the previous topic.

According to Microsoft, the following impairments are included in the Microsoft MOS-LQ metric:

- The codec, and its operating mode (wideband or narrowband)
- The characteristics of the audio device (microphone) used by the person speaking
- Any transcoding or mixing applied to the signal
- Observed levels of packet loss or packet loss concealment
- Speech level and background noise on the speaker’s end

APPENDIX B

Integration with the NetQoS Performance Center

Several key data views from UC Monitor reports can be viewed in the NetQoS Performance Center and added to other custom reports. In addition, groups of Locations and devices, user accounts, and their associated roles can be created and managed in the NetQoS Performance Center once you have registered the UC Monitor data source.

This appendix explains the process for registering NetQoS UC Monitor with the NetQoS Performance Center and describes the data views that are exported and formatted in a "Unified Communications Dashboard" report. For more information about group management, see the appendix about grouping in the *UC Monitor Administrator Guide*.

This appendix covers the following topics:

- "About the NetQoS Performance Center"
- "Integration with the NetQoS Performance Center"
- "Understanding the Unified Communications Dashboard"
- "Customizing Reports in the NetQoS Performance Center"

About the NetQoS Performance Center

The NetQoS Performance Center is a Web-based interface that enables you to view informative data from supported products in various formats so that you can effectively manage your networks, applications, and devices. By combining different types of analytical data for viewing in one place and offering seamless drilldown designed for troubleshooting, the NetQoS Performance Center offers a unique perspective for executives and for Engineering, Operations, and other groups who want to resolve issues quickly and maintain current resources as well as plan for future initiatives.

The NetQoS Performance Center helps you continuously monitor the end-to-end performance of applications across the network. Knowing what constitutes "normal" application performance helps you validate the impact of planned changes such as VoIP or UC deployments, MPLS migrations, QoS policy implementation, and application rollouts. The NetQoS Performance Center helps you see which applications are using network bandwidth, who is using the bandwidth, and when. It facilitates troubleshooting by helping you identify inappropriate application usage and anomalous traffic volumes. Finally, the NetQoS Performance Center helps you monitor and manage device performance, which means that you can manage capacity issues specific to individual devices such as routers and servers and diagnose availability problems.

Supported Data Sources

Integrated performance data is critical for effectively managing network and application performance. The NetQoS Performance Center can display data from several underlying products in unique combinations to help solve specific problems. These underlying products are called *data sources*. In addition to UC Monitor, the following data sources are fully supported by the NetQoS Performance Center:

Device	Description of Data
NetQoS SuperAgent	Collected from end-to-end network, application, and server performance monitoring.
NetQoS ReporterAnalyzer	Network traffic analysis data collected from NetFlow-enabled routers.
NetQoS NetVoyant Standard NetQoS NetVoyant Enterprise	Device-specific management and monitoring data collected from SNMP polling. • NetVoyant Standard is a single-appliance SNMP polling solution that monitors up to 5,000 poll instances. • NetVoyant Enterprise is a distributed polling solution that includes one or more deployed polling stations that monitor up to 10,000 or more poll instances and share information with a single console.
NetQoS Event Manager	Collects events, alerts, traps, and log streams from multiple data sources (including NetQoS UC Monitor), displays them in a correlated list view in the NetQoS Performance Center, and provides automatic notifications. See Appendix C, "Viewing Events in the Event Manager" on page 169 for a full description.
NetQoS Anomaly Detector	Identifies and alerts on abnormally high flow and volume sources that can indicate issues in the system.

Device	Description of Data
Cisco WAAS Connector	Couples NetQoS SuperAgent functionality with the native Cisco Central Manager to provide an integrated means of understanding the effect of WAN traffic optimization on bandwidth reduction and the end-user experience.
VMWare vCenter Connector	Leverages the data from VMWare vCenter and displays it next to SuperAgent data. Shows not only correlated response time and device health views that are context-based and VM-specific, but also the impact to the ESX host itself

Other data sources from third-party platforms are partially supported by means of the data export feature referred to as *inbound integration*.

Using the NetQoS Performance Center

The NetQoS Performance Center provides a full set of documentation, including comprehensive, context-sensitive online Help, to assist you in using the product. However, for purposes of this appendix, it is helpful to understand a few characteristics of the user interface and some key terms.

Like NetQoS UC Monitor, the NetQoS Performance Center uses the concepts of report *pages* and *views* of data within those pages. But the NetQoS Performance Center offers the additional capability of editing both pages and views. Views, or charts and graphs of data from selected data sources, are displayed on pages, with multiple views on each page. You can change the views contained on a given page. In the User Settings section, you can select the reports to be made available as separate menu items on the **Reports** tab. And each data view offers drilldown options to provide more context for the metrics displayed there.

The NetQoS Performance Center does not collect or analyze data. NetQoS products and third-party monitoring platforms provide data, either by direct support in the NetQoS Performance Center or by exporting their data in a supported format, to be displayed in views on NetQoS Performance Center report pages.

If your user account has the appropriate permissions, you can access data source interfaces from the NetQoS Performance Center user interface by drilling into a view or by clicking a link to the data source interface.

Most view data is nested in *tiers*, which allow for drilldown from overviews to more detailed data. For example, if a particular view shows data for a list of routers, you can click on a specific router to view more information pertaining to that router. Each tier provides greater detail. The NetQoS Performance Center offers two main reporting tiers:

- **overviews** comparing servers, routers, interfaces, or protocols in one view
- **details** of a particular item in one view

The data displayed in a particular view is also dependent on the *context*. A context narrows the scope of the view data. When you select a context for a view, the data shown in the view is selected with respect to that context. For example, if you choose a server group, the data displayed in the views that you select within that context is limited to that server group.

You can design a report page to display data for different groups, devices, or interfaces. For example, if you select a server group and add a few views to the page, and then select a router group and add a few more views to the page, the first set of views will display data for the server group and the second set of views will display data for the router group.

Centralized User Management

UC Monitor integration with the NetQoS Performance Center is similar to that provided by other NetQoS data sources. In addition to the shared data views and seamless drilldown path discussed below in "Integration with the NetQoS Performance Center" on page 155, NetQoS Performance Center version 4.0 and later also provides centralized management of user accounts, permissions, and groups among all NetQoS data source products. Centralizing user account and group management tasks makes it much easier to assign user access permissions and share information from different NetQoS data sources among IT teams.

To take advantage of the centralized management feature, you simply add the UC Monitor data source to the NetQoS Performance Center. As the UC Monitor data source is contacted, it is also automatically registered with the NetQoS Performance Center. Registration of a NetQoS data source product allows the NetQoS Performance Center to assume certain management tasks in that product and make them accessible to users with the appropriate administrative product privileges.

Note: The registration process is sometimes referred to informally as "binding."

Before you register the UC Monitor data source with the NetQoS Performance Center, the Security pages in the Administration section allow the UC Monitor Administrator to view all the predefined and custom UC Monitor user accounts and roles, edit or delete those accounts and roles and their associated product privileges, or add new, custom users and roles.

Once you have registered the data source with the NetQoS Performance Center, you are redirected to the NetQoS Performance Center for all administrative tasks associated with users, privileges, and roles. All users and roles defined in the system, including those created in other NetQoS products that are registered with the NetQoS Performance Center, are displayed on the UC Monitor User List and Role List Administration pages after registration. However, they can no longer be managed from those pages. Instead, a link is provided to the appropriate Administration page in the NetQoS Performance Center where management tasks can be performed.

Centralized management of the user accounts and roles created in NetQoS UC Monitor with those created in other NetQoS data source products is explained in the "Setting Up Security" chapter of the *UC Monitor Administrator Guide*, where you can also find an appendix that discusses the creation and management of groups in the NetQoS Performance Center.

Integration with the NetQoS Performance Center

The integration features in NetQoS Performance Center version 4.0 and later allow users with the appropriate permissions to view data in both NetQoS UC Monitor and the NetQoS Performance Center. Users can click a link in one of the Unified Communications Dashboard data views and instantly access the relevant report in the UC Monitor Management Console, with the appropriate context selected.

For example, clicking a link to a specific Location in the Call Performance by Location view takes the user directly from the Unified Communications Dashboard in the NetQoS Performance Center to the Call Performance Overview Report with the data narrowed by that Location. To return to the NetQoS Performance Center, the user would then click the **NPC** link at the top of the Management Console window.

An additional integration feature is support for grouping of Locations and VoIP devices. An appendix to the *UC Monitor Administrator Guide* provides more information about creating and using custom groups and permission group management in the NetQoS Performance Center.

The Unified Communications Dashboard report page is accessible in the NetQoS Performance Center if you have both products installed and have performed some minimal configuration.

To view data from a NetQoS data source product in the NetQoS Performance Center, you must register the data source. Registration allows for a seamless drilldown path among the various NetQoS network management products. The necessary steps to register the UC Monitor data source are explained below.

Adding the UC Monitor Data Source

To centralize the management of NetQoS groups, users, and roles and to access data collected in NetQoS data source products in the NetQoS Performance Center, you must add each NetQoS data source product to the NetQoS Performance Center. The process of adding the data source automatically registers it and integrates user and role management.

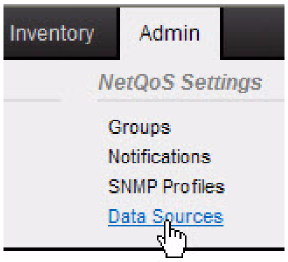
Adding data sources requires the Administrator product privilege. First, log into the NetQoS Performance Center with an Administrator account. The following instructions apply to NetQoS Performance Center version 6.0 and differ slightly from previous versions.

To add a UC Monitor data source to the NetQoS Performance Center:

1. On the NetQoS Performance Center main page, click the **Admin** link on the toolbar.

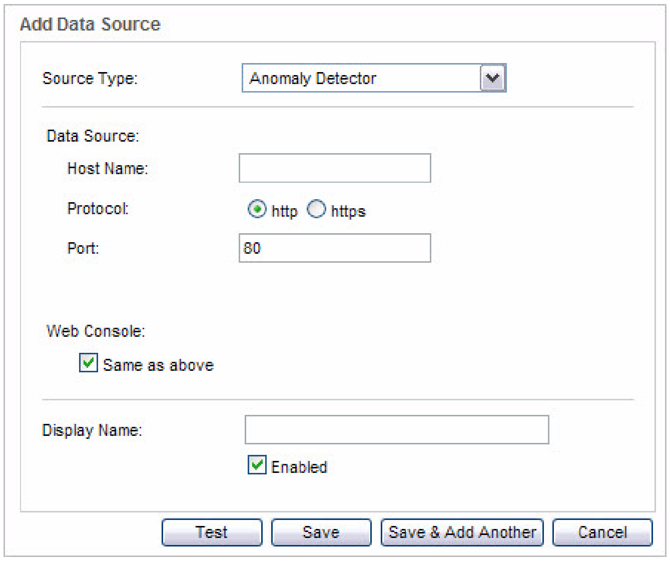
   The Admin menu contains several sections with different options.

2. In the **NetQoS Settings** section, click the **Data Sources** link, as shown below:



A list of the data sources you have already configured is displayed, along with the Global Synchronization Status, the last time that the NetQoS Performance Center contacted each data source for configuration information and performance data.

3. Click **New**.
4. On the Add Data Source page, select **Unified Communications Monitor** from the **Source Type** list.



Add Data Source

Source Type: Anomaly Detector

Data Source:

Host Name:

Protocol: ● http ○ https

Port: 80

Web Console:

☑ Same as above

Display Name:

☑ Enabled

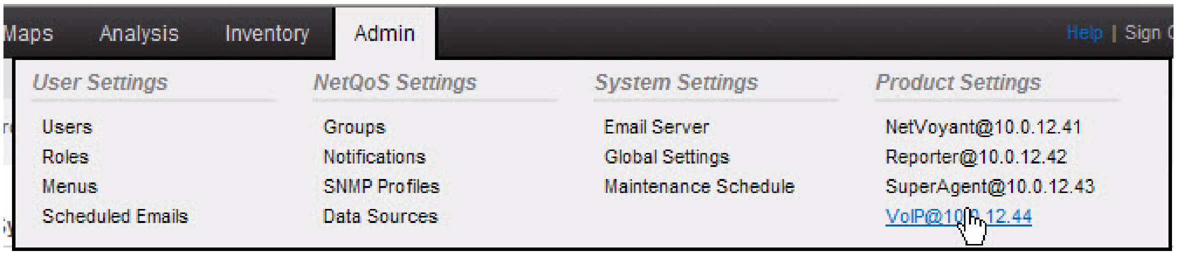
5. In the **Host Name** field, enter the hostname of the computer where the UC Monitor database is installed (in a distributed system, the Management Console computer, not the Collector).
6. Select the appropriate **Protocol** and port for the NetQoS Performance Center Web service to use to contact the corresponding UC Monitor Web service.

   By default, HTTP over Port 80 is used, but if Secure Communications have been enabled in IIS for the `VoIPMonitorWebService` site, you should select **HTTPS** and Port **443**.
7. Confirm whether the Web Console address for the data source is the same as the hostname of the server. If it isn’t, clear the check box labeled **Same as above** and supply the Web Console information in the fields provided:
   - **Host Name**: The hostname of the computer where the UC Monitor database is installed
   - **Protocol** (see Step 6, above)
   - **Port** (see Step 6, above)

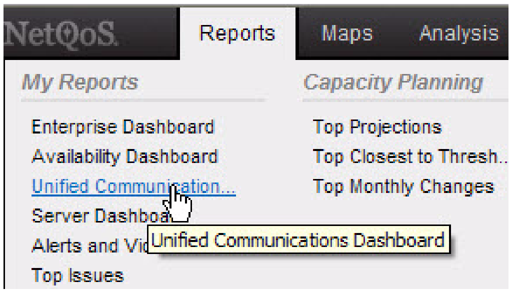
8. Supply a **Display Name**. This is the name that is used to identify the data source. If you are adding multiple UC Monitor data sources, you might want to change the default data source names to help identify them in the NetQoS Performance Center.
9. Leave the **Enabled** check box selected. This check box allows you to quickly disable a data source without unregistering it. If the box is cleared, no data is received from this data source.
10. Click **Test**. The NetQoS Performance Center attempts to contact the UC Monitor server. If contact is successfully established, a message states, "`Successfully connected to UC Monitor Web Service`."
11. Click **Save** to save the data source. The UC Monitor data source appears in the **Data Sources** list.

Verifying the UC Monitor Data Source

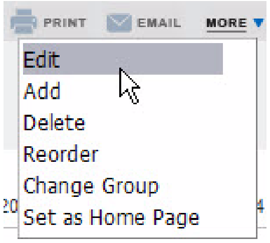
Once you have added NetQoS UC Monitor as a data source in the NetQoS Performance Center, you should be able to see it in the list of data sources. Click the **Admin** tab, and check the Product Settings section. A **VoIP** data source should have been added to the list of data source addresses. The hostname of the UC Monitor server that you configured as a data source is a link that provides quick access to the UC Monitor Login page, as shown in the following image:



To view the Unified Communications Dashboard, click the **Reports** tab on the toolbar. The Unified Communications Dashboard report appears in the **My Reports** section by default:



Click the **More** link on the Report-level Action Bar (at the top right on the dashboard page) if you want to edit this page to include more views, or to set the Unified Communications Dashboard as your home page:



See "Modifying the Unified Communications Dashboard" on page 163 for more information about editing a report page in the NetQoS Performance Center.

Understanding the Unified Communications Dashboard

As soon as you have successfully added NetQoS UC Monitor as a data source in the NetQoS Performance Center, you can view VoIP and video performance data on the NetQoS Performance Center Unified Communications Dashboard page. This report page provides a network manager or higher-level executive with a daily or weekly overview of overall VoIP and video call performance. More detailed views of data that is summarized in the Unified Communications Dashboard are available in the UC Monitor interface.

The integration features in NetQoS Performance Center version 4.0 and later mean that any user with permissions to view data in both NetQoS UC Monitor and the NetQoS Performance Center can click a link in one of the Unified Communications Dashboard data views and immediately access the appropriate report in the UC Monitor Management Console, with the appropriate context selected.

For example, clicking a link to a specific Location in the **Call Performance by Location** view takes the user directly from the Unified Communications Dashboard page in the NetQoS Performance Center to the Call Performance Overview Report with the data narrowed by that Location. To return to the NetQoS Performance Center, the user would then click the **NPC** link at the top of the Management Console window.

Integration features also allow for a seamless drilldown path that does not require a second authentication (that is, with no intervening login page). For more information about these integrated authentication features, see the *Single Sign-On Guide*, available on the NetQoS Self-Service Portal, or the relevant topics in the "Setting Up Security" chapter of the *UC Monitor Administrator Guide* for a full discussion.

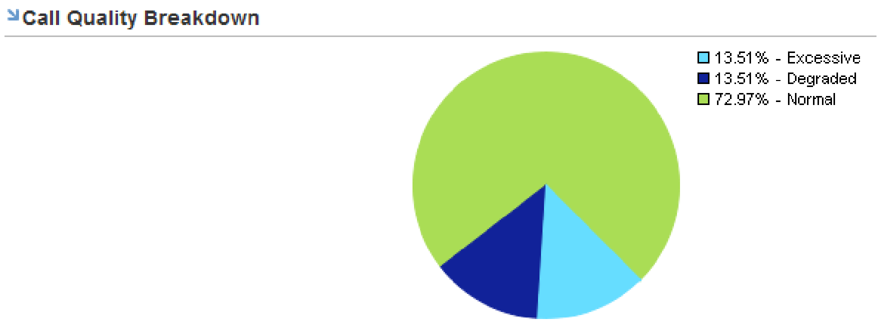
The Unified Communications Dashboard consists of the following data views:

- "Call Quality Breakdown" on page 159
- "Call Quality Trend" on page 160
- "Call Performance by Group" on page 160
- "Call Performance by Location" on page 161
- "Call Performance by Media Device" on page 162
- "Call Performance by Call Server" on page 162

Each view is described in a separate section below.

You can easily edit the report page in the NetQoS Performance Center to remove these views, or to add views from other NetQoS data sources. For example, NetQoS NetVoyant offers IP SLA testing of VoIP devices, and views of the resulting data can be added to the Unified Communications Dashboard once both data source products are registered. See "Modifying the Unified Communications Dashboard" on page 163 for more information.

Call Quality Breakdown



This view provides a pie chart showing a rollup of systemwide call quality for the given time period (the default setting is "Last Hour"). The percentage of all call minutes that fell into each severity range is displayed in the chart.

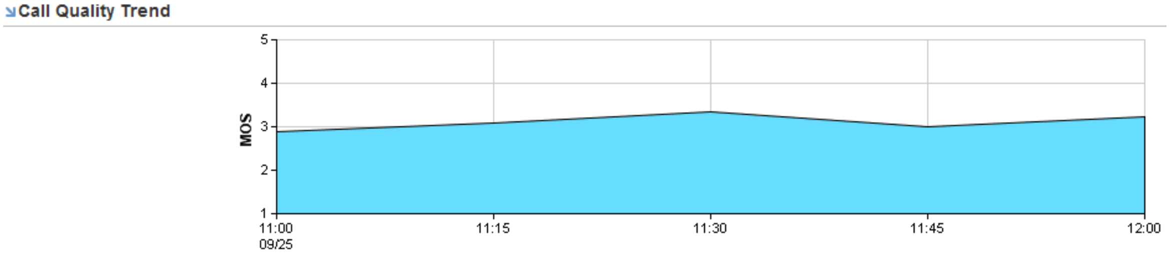
The call quality data in this chart comes from the Mean Opinion Score (MOS) values of every call leg that was measured within that time frame. The default Call Quality performance thresholds assign severity based on the VoIP codec used for each call.

For the Call Quality Breakdown, MOS values are evaluated according to the Call Quality performance thresholds that were assigned to the Locations where call activity occurred during the selected time period. The thresholds determine which MOS values are rated "Normal" and which "Degraded" and "Excessive." The threshold values in these severity categories can be customized per Location or assigned automatically per codec.

Note: MOS values do not apply to video streams. Network MOS is not included.

A unique color value has been assigned to each severity level shown in the pie chart. For example, the "Excessive" severity rating receives a light blue color in the chart. A legend explains the color assignments. Any data that is "Unrated" may indicate that the Minimum Observations threshold for that Location was not met during the selected time period.

Call Quality Trend

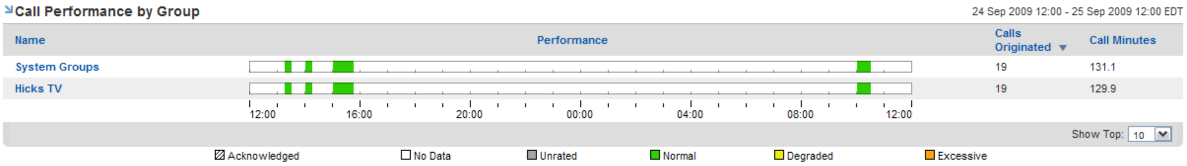


The Call Quality trend chart provides an enterprise-level view of the trend in Mean Opinion Score (MOS) values. It is a rollup view from across the entire system of MOS data from all calls detected during the selected time frame.

Note: MOS values do not apply to video streams. Network MOS is not included.

Related data is available by drilling down into the Metric Details page from the Call Performance Overview Report in NetQoS UC Monitor. The trend chart does not include an indication of the number of observations (the number of call minutes) used to derive the metrics. To find out the number of observations behind the trend, navigate to the UC Monitor data source and click to view the Call Performance Overview report. Click the **Metric Details** link at the top of the report page. Scroll down to see the Call Quality - MOS chart. If necessary, click the time frame link to select the desired time frame. The smallest granularity available in UC Monitor reports is three hours.

Call Performance by Group


Call Performance by Group

24 Sep 2009 12:00 - 25 Sep 2009 12:00 EDT

Name	Performance	Calls Originated ▼	Call Minutes
System Groups		19	131.1
Hicks TV		19	129.9

The Call Performance by Group view lists the groups of UC Monitor subgroups, Locations, or devices that had call activity during the selected time frame and rates their average call performance. A horizontal bar graph displays the average call performance severity ratings for all Locations within the indicated group. The color-coded bars show the number of calls originated or call minutes whose performance was rated Normal, Degraded, or Excessive.

- Calls Originated—Calls placed by phones in Locations within the indicated group
- Call Minutes—Minutes during which phones in this group were actively sending data

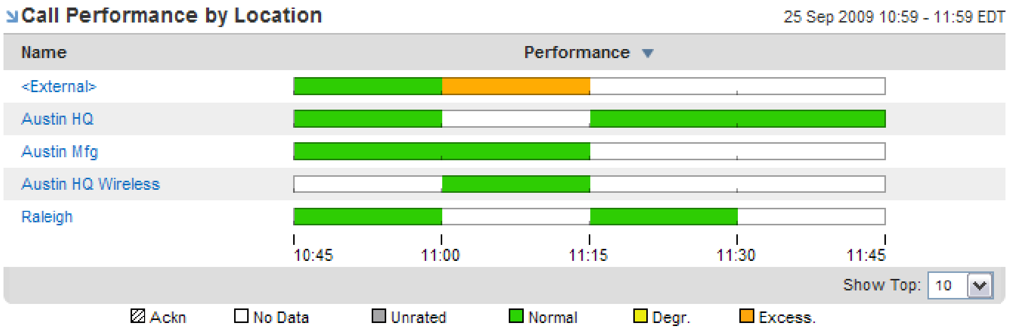
The Call Performance category includes both call-quality and call-setup metrics. Where available, video metrics are included. Call-setup and call-quality metrics were evaluated according to the performance thresholds that were assigned to the Locations within the indicated groups. The thresholds determine which values are rated “Normal” and which “Degraded” and “Excessive.” The threshold values in these severity categories can be customized per Location.

The group ratings are rollups of data from all items included in each group. Typically, a UC Monitor group is composed of Locations, media devices, and call servers. The Data Sources system group consists of all UC Monitor data sources that have been registered with the NetQoS Performance Center.

The names of each group are hyperlinks that provide a drilldown path to individual Locations or devices included in that group. They are sorted by worst call performance. For any group defined in a single UC Monitor data source, you can click a group name link to navigate out to the Call Performance Overview Report page in the data source with that group selected. Views of data from any subgroups and from any members contained within the selected group are included in the Overview report.

By default, the last hour's worth of collected data is shown in the Unified Communications Dashboard. If you navigate out to the UC Monitor data source, the default is to show the last three hours' worth of data. You can change the time frame for this view; however, the views of three months' and 12 months' worth of data are not supported in the NetQoS Performance Center.

Call Performance by Location


Call Performance by Location

25 Sep 2009 10:59 - 11:59 EDT

Show Top: 10

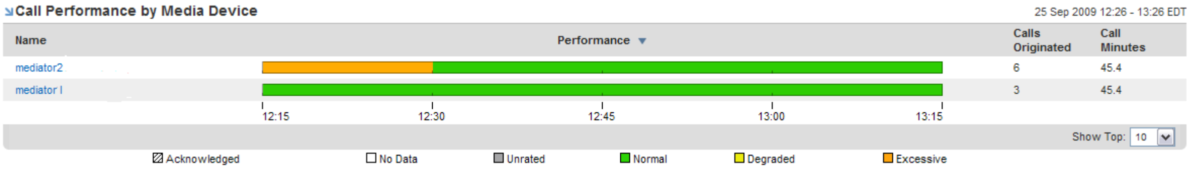
The Call Performance by Location view lists Locations that had call activity during the selected time period and includes a horizontal bar graph that rates call performance. The Call Performance category includes both call-quality and call-setup metrics. Where available, video metrics are included. By default, data from the ten worst-performing Locations is displayed, sorted by severity.

The severity ratings reflected in the Call Performance by Location chart are based on call performance data from all phones in the indicated Location. Any data that is "Unrated" may indicate that the Minimum Observations threshold for that Location was not met during the selected time period.

The names of each Location are hyperlinks that allow further investigation in NetQoS UC Monitor for users with the required permissions. For any Location defined in a single UC Monitor data source, you can click a link in the **Name** column to navigate out to the Call Performance Overview Report in the data source with that Location selected.

You can change the time frame for this view from within the NetQoS Performance Center; however, the views of three months' and 12 months' worth of data are not supported.

Call Performance by Media Device



Call Performance by Media Device

25 Sep 2009 12:26 - 13:26 EDT

Name	Performance	Calls Originated	Call Minutes
mediator2		6	45.4
mediator I		3	45.4

Show Top: 10

▨ Acknowledged □ No Data ■ Unrated 🟩 Normal 🟨 Degraded 🟧 Excessive

The Call Performance by Media Device view rates the call performance of media devices (typically voice gateways, which route calls to and from the public switched telephone network) that had call activity during the selected time frame. It includes a horizontal bar graph that rates call performance and shows when calls occurred.

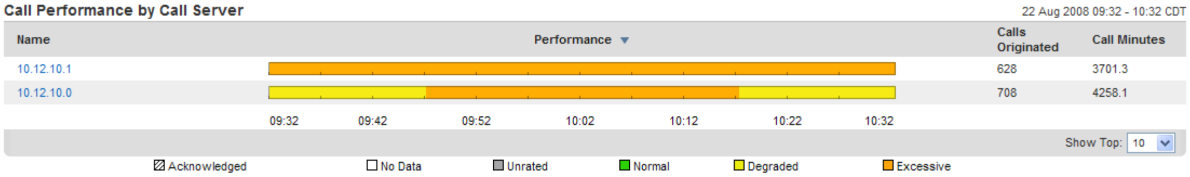
The Call Performance category includes both call-quality and call-setup metrics. Where available, video metrics are included. The bar graph represents the number of calls originated or call minutes reported by each device that were rated Normal, Degraded, or Excessive.

- Calls Originated—Calls placed by phones that used this media device to send calls to the PSTN
- Call Minutes—Minutes of call activity reported by this media device

Device names (shown in the **Name** column) are usually hostnames and are sorted by worst call performance. The name of each device is a hyperlink that allows further investigation in NetQoS UC Monitor. For any media device known to a single UC Monitor data source, you can click a device link to navigate to the Call Performance Overview Report with that device selected.

You can change the time frame for this view from within the NetQoS Performance Center; however, the views of three months' and 12 months' worth of data are not supported.

Call Performance by Call Server



Call Performance by Call Server

22 Aug 2008 09:32 - 10:32 CDT

Name	Performance	Calls Originated	Call Minutes
10.12.10.1		628	3701.3
10.12.10.0		708	4258.1

Show Top: 10

▨ Acknowledged □ No Data ■ Unrated 🟩 Normal 🟨 Degraded 🟧 Excessive

The Call Performance by Call Server view rates the call performance of call servers (such as Cisco Unified Communications Managers, Avaya Communication Manager, or Microsoft Office Communications Servers) that had call activity during the selected time frame. It includes a horizontal bar graph that rates call performance and shows when calls occurred.

The Call Performance category includes both call-quality and call-setup metrics. Where available, video metrics are included. The bar graph represents the number of calls originated or call minutes reported by each device that were rated Normal, Degraded, or Excessive.

- Calls Originated—Calls placed by phones that are registered to this call server
- Call Minutes—Minutes of call activity reported by this call server

Call server names (shown in the **Name** column) are usually hostnames and are sorted by worst call performance. The name of each server is a hyperlink that allows further investigation in NetQoS UC Monitor. For any call server known to a single UC Monitor data source, you can click a device link to navigate to the Call Performance Overview Report with that call server selected.

You can change the time frame for this view from within the NetQoS Performance Center; however, the views of three months' and 12 months' worth of data are not supported.

Modifying the Unified Communications Dashboard

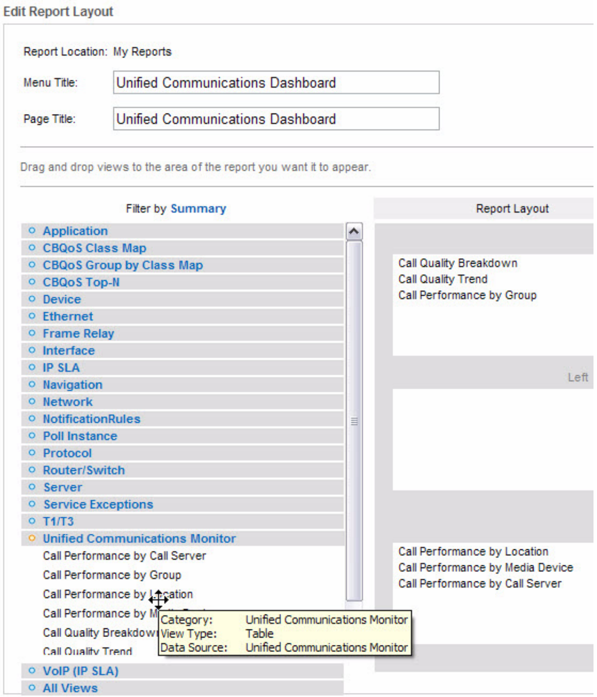
The Unified Communications Dashboard page can be modified, just as any other NetQoS Performance Center report page can be modified to change the view layout or to include views from other data sources or with other contexts. The reporting interface makes it easy to combine metrics from different sources in one page or report. If you are logged into the NetQoS Performance Center as an Administrator or Power User, you can modify existing reports or create new reports and save them as private or shared reports.

To modify the Unified Communications Dashboard:

1. Select the Unified Communications Dashboard report from the **Reports** tab.
2. From the More menu (the arrow labeled **MORE**), select **Edit**.

   The Edit Report Layout page is displayed.
3. If desired, you can change the title of the menu item that appears on the **Reports** tab by typing a new menu item name in the **Menu Title** field.

   Or you can change the title of the Dashboard page by typing a new title in the **Page Title** field.



Edit Report Layout

Report Location: My Reports

Menu Title: Unified Communications Dashboard

Page Title: Unified Communications Dashboard

Drag and drop views to the area of the report you want it to appear.

Category: Unified Communications Monitor
View Type: Table
Data Source: Unified Communications Monitor

The available UC Monitor views are shown in a bulleted list, which is collapsed by default (and expanded in the above image).

Note: By default, the context setting is **Summary**, which means that the available views provide summary data and do not require designation of a specific group or managed item. You cannot change the context for views already on the page. However, you can remove existing views and choose a different context for new views that you add from other supported data sources.

4. If desired, change the context of the available views by clicking the **Filter by Summary** link.
5. In the Select Context dialog box, click to select another **Type** of item whose context view you want to add to the Unified Communications Dashboard.

   For any type you select, a table is displayed containing all the available managed items of that type.
6. Select an item from the table.

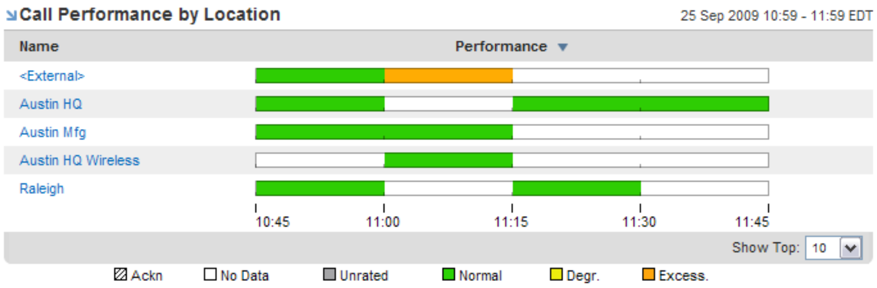
   The list of available views that can be added to the Dashboard page is now filtered by the selected item. (You can clear the filter by clicking the [**Clear Filter]** link.)
7. In the Report Layout pane, click:
   - **Clear Report Layout** to change the positioning of all views on the Dashboard page, or
   - A **[Remove]** link to remove an individual view from the page.
8. Click a UC Monitor view in the bulleted list shown in the left pane, drag it to the Report Layout pane, and drop it into the desired position.
9. If desired, expand one of the other available data sources, such as NetQoS SuperAgent, in the Context pane.
10. Click and drag to add views from other supported data sources.

When you have completed your changes, click **Save**. The edited page appears in the My Reports section of the Reports menu; by default, a new or edited page is included in the menu section you are accessing when you create or modify it. You can also move the page to another section or add it to multiple sections of the Reports menu.

Report pages added to the My Reports section of the **Reports** tab are private unless an Administrator or Power User adds those pages to other shared menus. If you want to make the edited report page available to other users, the NetQoS Performance Center online Help explains how to add a menu, add a report page to a menu, and ensure that other users have the necessary permissions to view the new menu.

Accessing More Information about Dashboard Views

Several of the UC Monitor data views you can access in the NetQoS Performance Center, “Call Performance by Group,” “Call Performance by Location,” “Call Performance by Media Device,” and “Call Performance by Call Server,” offer a drilldown capability to help you troubleshoot degraded or excessive performance.



The drilldown path places you in the appropriate context for the data being accessed. For example, the **Call Performance by Location** and **Call Performance by Media Device** data views provide links from the NetQoS Performance Center to views of data from the Locations or devices whose performance is being rated in the bar charts. Click a Location, device, or call server to return to the UC Monitor user interface. You are directed automatically to the Call Performance Overview Report page, with that Location or device selected for closer analysis.

Customizing Reports in the NetQoS Performance Center

The NetQoS Performance Center provides a unique capability: it enables you to combine metrics from different sources in one page or report. The steps provided in the previous section show how to add views to the Unified Communications Dashboard page. Customizing report pages by combining views of data from multiple data sources can help you make the most of the data that NetQoS and other supported monitoring platforms can provide.

The following list provides just a few examples of useful report pages you can create from data views available in the NetQoS Performance Center:

- Application Performance—You can add one or more of the UC Monitor views to a page containing views of application performance from NetQoS SuperAgent and see whether a VoIP deployment is affecting the performance of existing network applications.
- Device Performance—Similarly, adding selected views from NetQoS NetVoyant to the VoIP Dashboard can provide insight into problems at a media device.
- Troubleshooting Schemes—Depending on the other data sources you have installed, the NetQoS Performance Center enables you to combine end-to-end performance, traffic analysis, VoIP and video call performance, and device performance data on a single report page. Such reports can be extremely valuable for an operations team, who can use the information to quickly identify issues, eliminate potential causes, and then identify the real cause of a problem.

  If you design troubleshooting pages that your operations team can check several times a day, your team becomes proactive rather than reactive.

- Overviews—Views available in a summary context are overviews of network performance, as opposed to individual device statistics. They are generally from a higher tier and can be drilled into for more component detail. The summary views in the Unified Communications Dashboard can be added to your existing overview pages to provide a high-level report of system health.

ReporterAnalyzer and NetVoyant Data in the UC Dashboard

NetQoS ReporterAnalyzer provides some especially useful data to help with your VoIP deployment. You may want to add some views from the ReporterAnalyzer data source to the Unified Communications Dashboard to find out:

- How much bandwidth VoIP and video traffic is consuming. This information helps you make capacity-planning and purchasing decisions.
- Whether VoIP and video traffic flows are traveling over the right interface(s) and taking the network path you want them to take, or whether something is misconfigured.
- Whether the VoIP and video traffic is being marked with the correct TOS markings. Knowing this information is important for several reasons, starting with the crucial need for QoS to ensure peak VoIP performance. There are plenty of places in the network where routers might change the TOS markings in the IP header and effectively disable QoS for the VoIP and video packets.

The following is just a brief list of the complementary ReporterAnalyzer views that you should consider adding to the Unified Communications Dashboard:

ReporterAnalyzer View	Description
Stacked Protocol Trend Total	Get a view of the “big picture” of the network from the perspective of individual protocols. Lets you determine whether voice traffic is unusually heavy during a particular time period, or whether traffic from another application or service is consuming too much bandwidth and crowding out the VoIP traffic.
Interface Utilization	In the event of poor VoIP or video performance, you’ll be able to see at a glance whether a network bottleneck is to blame and be able to isolate the problem quickly.
Custom Report of VoIP Traffic: Summary Table of VoIP Traffic on All Interfaces	View the total volume and average rate of VoIP and video traffic on all interfaces. Use this information for UC infrastructure capacity planning.

NetQoS NetVoyant already offers some support for active monitoring of VoIP performance. NetVoyant can collect data from IP SLA testing, which can provide data to complement the passive call monitoring that UC Monitor performs. IP SLA tests, which simulate the network data associated with typical applications and services, are performed by IP SLA-enabled Cisco devices and enable you to measure network performance between selected locations. You can configure these tests from the NetVoyant user interface.

We recommend constructing IP SLA tests to run from key network locations, such as between core routers. You can then add views of VoIP jitter or latency from NetVoyant to complement the views included in the Unified Communications (VoIP) Dashboard.

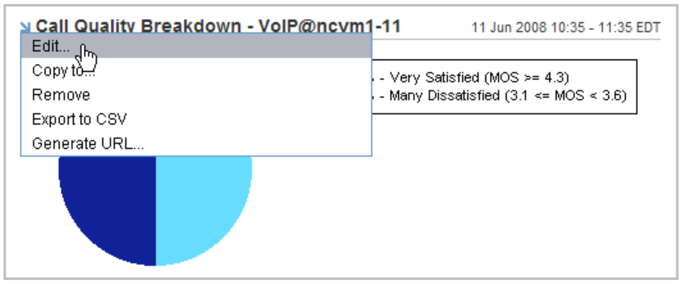
Support for Multiple Instances of a Data Source

The NetQoS Performance Center allows you to add multiple instances of a data source; you can add up to four NetQoS UC Monitor data sources to a single NetQoS Performance Center, for example. By default, only data views from the data source that was added first are displayed in the VoIP Dashboard report. However, you have several options for viewing data from the other UC Monitor instances:

- Manually edit the Unified Communications Dashboard report page to add data views from other instances of NetQoS UC Monitor.
- Manually edit another report page, such as the Enterprise Dashboard, to add data views from multiple instances of NetQoS UC Monitor.
- Edit a selected UC Monitor data view from the View-level menu (the blue arrow just to the left of each view) to select a different data source instance.

  The presence of multiple instances of the same data source enables an editing feature in the View-level menu for each UC Monitor data view. You can edit the view to display equivalent data from a different data source instance.

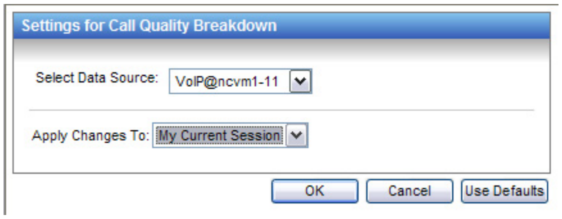
For example, if you added three UC Monitor data sources to an instance of the NetQoS Performance Center, you could then edit the Unified Communications Dashboard page to add views, as described in “Modifying the Unified Communications Dashboard” on page 163. Or in one of the UC Monitor data views, you could select **Edit** from the View menu, as shown in the following image:


Call Quality Breakdown - VoIP@ncvm1-11
11 Jun 2008 10:35 - 11:35 EDT
Edit...
Copy to...
Remove
Export to CSV
Generate URL...
- Very Satisfied (MOS >= 4.3)
- Many Dissatisfied (3.1 <= MOS < 3.6)

The Settings window that is displayed provides an option to select a different data source instance for the current view. The **Select Data Source** list includes all *instances of the current data source* that you have added to the NetQoS Performance Center.

Note: You could not, for example, select NetQoS NetVoyant as the data source for a data view taken from NetQoS UC Monitor.

You can also choose whether to apply the new view setting to the current login session or to your user account:


Settings for Call Quality Breakdown

Select Data Source: VoIP@ncvm1-11

Apply Changes To: My Current Session

APPENDIX C

Viewing Events in the Event Manager

Events related to the unified communications system being monitored can be sent to the NetQoS Event Manager, a data source for the NetQoS Performance Center. Once you install and register the UC Monitor and Event Manager data sources, each incoming UC Monitor Incident is converted to an event and displayed in a list of events on the Events report page, available in the **Operations** section of the NetQoS Performance Center **Reports** menu.

Events from the UC system and from other NetQoS data sources, such as NetQoS NetVoyant, are correlated to reduce duplication. Event status and closure rates that are available in selected Event Manager data views can be used to track IT staff MTTR and the number of instances of events of differing severity in the system.

Version 5.0 or later of the NetQoS Performance Center is required.

The following topics provide information about how UC Monitor events are handled in the Event Manager:

- "Event Manager Overview" on page 170
- "UC Monitor Support for the NetQoS Event Manager" on page 170
- "Viewing UC Monitor Incidents in the Event List" on page 172
- "UC Monitor Event Status in the Event Manager" on page 175

Event Manager Overview

The NetQoS Event Manager collects events, alerts, traps, and log streams from multiple data sources and displays them in a standard report format within the NetQoS Performance Center. It performs event correlation and de-duplication, summarizing events to reduce alert "noise" and point the diagnostic team toward the likely cause of each problem. The event notification feature gathers data from specific types of events and presents actionable information to IT Operations staff or performs an automatic action. And a reporting feature provides management reporting on event status and the frequency and timing of repeat offenders systemwide.

Although it is installed separately, the Event Manager must be registered as a data source for the NetQoS Performance Center and requires at least one other data source, such as NetQoS UC Monitor or NetQoS NetVoyant. Once both data sources are registered, most UC Monitor Incidents are automatically sent to the Event Manager and displayed as events in NetQoS Performance Center versions 5.0 and later.

The NetQoS Event Manager is typically installed on the same server as the NetQoS Performance Center. It provides the status information necessary to support the Maps feature, a graphical display to help you view and manage network and system events in the NetQoS Performance Center. The events and status displayed in the main Event Manager data view (the **Event List**) are not exactly the same as those shown in the Map. Although the Map page includes a **Map Event List**, which resembles the corresponding Event List in the Event Manager, the list shown on the Map is filtered so that only the most recent events are shown, in near real time.

Note: At least one NetVoyant data source, version 6.0 or later, is required to enable the Maps feature.

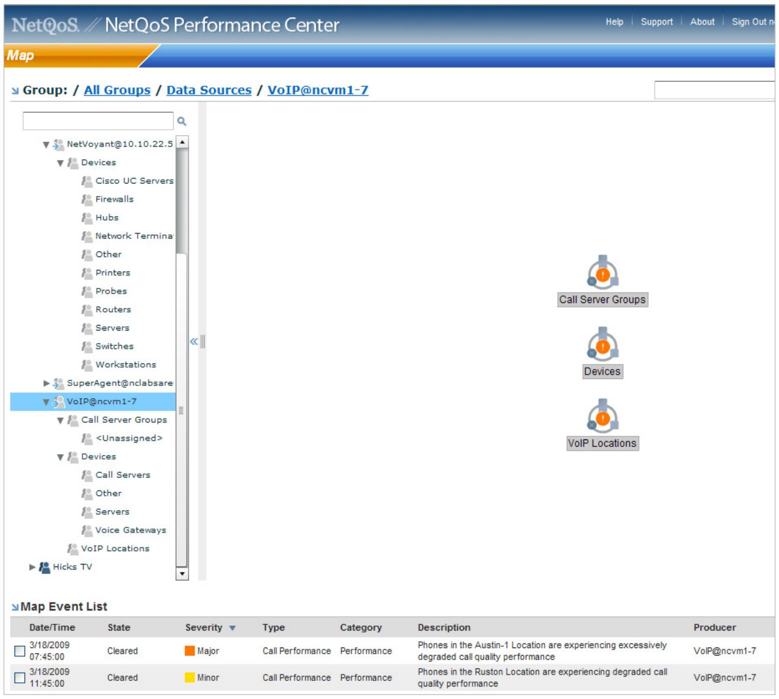
UC Monitor Support for the NetQoS Event Manager

Where NetQoS UC Monitor communicates information about potential issues by means of *Incidents*, the Event Manager reports on *events*. The UC-related events you can view in the Event Manager have been converted from Incidents into events.

Only Incidents that report on items that are managed by the NetQoS Performance Center can be sent to the Event Manager. When you register the UC Monitor data source, five types of Incident—all of the Call Server and Call Performance Incidents—are converted into events and displayed in the NetQoS Performance Center. By contrast, Collectors are not managed in the NetQoS Performance Center; therefore, Collector Incidents can only be viewed in the UC Monitor Collector Incidents report.

Because the Event Manager performs event correlation, it provides additional tables, with data that is not available in UC Monitor reports. For example, the **Event Severity** summary table provides data related to event severity and status to help you track the efficiency of IT troubleshooting procedures. The **Event Source** table correlates event types with the Locations, call servers, or media devices where the most recent events have occurred and provides a drilldown path into data for those items. The metrics reported in the Event Manager also help you track the relative frequency of reporting for events of different severity levels.

Once converted to events by the Event Manager, UC Monitor Incidents can also be viewed in the Map. The following image provides an example (from NetQoS Performance Center version 5.1):



Map Event List

	Date/Time	State	Severity ▼	Type	Category	Description	Producer
□	3/18/2009 07:45:00	Cleared	🟧 Major	Call Performance	Performance	Phones in the Austin-1 Location are experiencing excessively degraded call quality performance	VoIP@ncvm1-7
□	3/18/2009 11:45:00	Cleared	🟨 Minor	Call Performance	Performance	Phones in the Ruston Location are experiencing degraded call quality performance	VoIP@ncvm1-7

Adding and Editing the Event Manager Report Page

Most Event Manager data views are not available in the NetQoS Performance Center Events report by default. The Event Manager is installed as a separate product, and the Administrator must add it as a NetQoS Performance Center data source. In addition, at least one other NetQoS data source that supports the Event Manager must be registered to the same NetQoS Performance Center instance.

When you access the NetQoS Performance Center by logging in with user-level privileges, you will need to either navigate to a custom Events page that the Administrator has created for you or navigate to the Events page in the **Operations** section of the **Reports** menu. By default, one Event Manager data view is available on this page, the **Event List**. If you want to see other Event Manager views, you must either add them to the Events report by selecting **Edit** from the **More** menu, or create a custom report page, which is then available in the **My Reports** section of the Reports menu.

Note: To perform the following procedure, you must be logged in with a user account that has either Administrator or Power User privileges.

To add Event Manager data views to the Events page:

1. First, check to see whether a custom Events page is already accessible. Click **Events** in the **Operations** section of the **Reports** menu. The default Events report page only contains the **Event List** view.

   If you want to see additional Event Manager data views, such as the Event Summary views, and if your user account has the required permissions, you can create a custom page and add those views.

2. From the Events report page, click the **More** menu and select **Edit**.

   The Edit Report Layout page is displayed.

3. In the left pane, scroll down to the **All Views** section, and click to expand it.

The available views are listed in alphabetical order. All the Event Manager views begin with the word *Event*.

4. Click and drag the **Event List** view and any of the **Event Summary** views you want to see, and drop them on different sections of the **Page Layout** area.

   Note: It's a good idea to place the **Event List** in the section of the page layout labeled **Top** so that you see a summary of recent events when you first access the Event Manager page.

   If desired, you can also add UC Monitor views to this page. They are listed under **All Views** and also under **Unified Communications Monitor**.

5. Click **Save**.

The views you added to the Events page should now be visible to all NetQoS Performance Center users.

If you would like to make the Events page the default page you see when you log into the NetQoS Performance Center, click the **More** menu again, and select **Set as Home Page**. Home page settings apply only to individual login accounts.

Viewing UC Monitor Incidents in the Event List

When they are displayed as events in the Event Manager **Event List** data view, UC Monitor Incidents use some terminology that differs slightly from that used in UC Monitor Incident reports. To regularize event reporting among all NetQoS data sources, NetQoS Event Manager assigns new severity levels to UC Monitor Incidents and also displays several additional parameters that are not used in the UC Monitor Incident List or Details reports. The following table provides a summary of the information provided in the Event Manager Event List:

Column	Description
Date/Time	The date and time that the Incident was opened, which led to the event's being opened in the Event Manager.
Count	The number of times that an event has occurred. UC Monitor events shown in the Event List are aggregations of similar Incidents.
State	Current status of the event. One of the following: • **Opened**—The condition that triggered the Incident (and thus, the event) is still applicable, and the event has not been acknowledged. • **Acknowledged**—The event has been assigned to a user for diagnosis or resolution. • **Closed**—The event was closed by a user. Because UC Monitor Incidents cannot be closed by user action, UC Monitor events with this state appear as **Acknowledged** Incidents in the UC Monitor interface. • **Cleared**—The condition that triggered the Incident (and thus, the event) is no longer true. The Incident has closed in NetQoS UC Monitor. See "UC Monitor Event Status in the Event Manager" on page 175 for more information about how event status is reflected slightly differently in the data source interface.

Column	Description
Severity	Event severity, derived from the Incident severity. • An Incident with **Degraded** severity becomes an event with **Minor** severity. • An Incident w'ith **Excessive** severity becomes an event with **Major** severity.
Type	The type of data that UC Monitor sent to the NetQoS Performance Center. For NetQoS UC Monitor, the type of an event is one of the following: • **Call Performance**—Corresponds to either a Call Quality or Call Setup Incident. • **Call Server**—Corresponds to either a Call Server or Call Server Group Incident.
Category	A classification of the event into a category from the FCAPS model (fault management, configuration, accounting, performance, and security). Always "Performance" for a UC Monitor event. Other categories are applicable to other data sources.
Description	The description of the Incident that is sent in any automated notifications that are associated with the applicable threshold.
Producer	The NetQoS data source that sent the Incident report to the Event Manager for correlation and display.

Click any column in the Event List table to sort by that data parameter.

Drilling down to Event Details

The NetQoS Event Manager report page (titled **Events** by default) offers different options for accessing detailed information about a given event. The main drilldown path to take, from the Event List, provides a quick way to navigate to the Incident report in the underlying UC Monitor data source.

To access detailed information about a UC Monitor event:

1. Navigate to the Events report page in the NetQoS Performance Center.

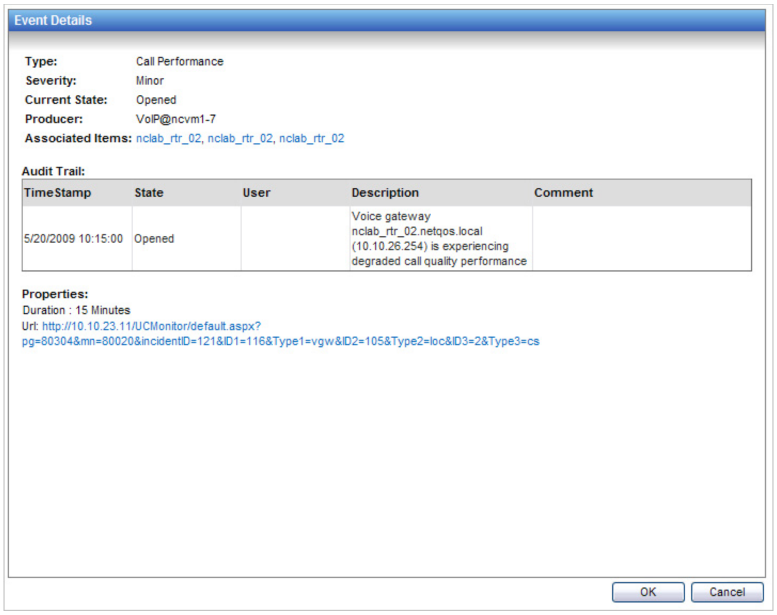
   In the **Reports** menu, the Events page is listed under **Operations** by default.

2. By default, only events from the last hour are shown on the Events report page. If the UC Monitor Incident occurred in the past, use the Time Period selector to select a longer timeframe, such as **Last Day**.

3. Find the event in the **Event List**. Click the page numbers at the bottom of the **Event List** view if necessary to see the full list of recent events.

4. Right-click the event, and select **Details**.

   The Event Details dialog box is displayed.



Type: Call Performance
Severity: Minor
Current State: Opened
Producer: VoIP@ncvm1-7
Associated Items: nclab_rtr_02, nclab_rtr_02, nclab_rtr_02

Audit Trail:

TimeStamp	State	User	Description	Comment
5/20/2009 10:15:00	Opened		Voice gateway nclab_rtr_02.netqos.local (10.10.26.254) is experiencing degraded call quality performance	

Properties:
Duration : 15 Minutes
Url: http://10.10.23.11/UCMonitor/default.aspx?pg=80304&mn=80020&incidentID=121&ID1=116&Type1=vgw&ID2=105&Type2=loc&ID3=2&Type3=cs

5. If desired, click one of the hyperlinked devices listed in the **Associated Items** section.

   Clicking the name of a router, for example, gives you access to the Router Performance report for the selected router. Where available, detailed router performance metrics collected by NetQoS NetVoyant are displayed.

   The **Audit Trail** helps you track event status and shows whether the event has been acknowledged or closed and reopened.

   A list of event **Properties** is provided below the Audit Trail. This information is particularly useful if you are setting up event notifications, which can be triggered by events with specific properties.

   Note: The NetQoS Performance Center online Help contains a full set of instructions for setting up notifications in the Event Manager. This feature is only available in versions 6.0 and later of the NetQoS Performance Center.

6. Click the URL provided at the bottom of the Event Details dialog box (see the above image).
7. You navigate to the UC Monitor data source, where the "Incident Details" report is displayed.

The Incident report that triggered the event in the Event Manager is shown, filtered by the appropriate Location, call server, and media device (if applicable).

UC Monitor Event Status in the Event Manager

UC Monitor Incidents cannot be closed by user intervention. Acknowledging an Incident does not contribute to its closure. The rules that determine Incident closure are discussed in "More about UC Monitor Incident Reporting" on page 95; to summarize these rules, an Incident is closed after the metric that triggered the Incident has returned to a normal level for a full clock-hour, or after 24 hours have passed.

The Event Manager has its own set of status conditions for events. Users can manually close events from some NetQoS Performance Center data sources, changing them to a **Cleared** status, but the closure action is not actually valid for UC Monitor events. The following points describe UC Monitor event status in the NetQoS Event Manager:

- When the metric that triggered a UC Monitor Incident exhibits one clock-hour of normal performance, the Incident will close, and the corresponding NetQoS Event Manager event status will be **Cleared**.

  A new Incident and event will open later if the metric shows new data that exceeds the threshold.
- When a UC Monitor Incident reaches 24 hours in duration, the Incident will close in NetQoS UC Monitor regardless of its current status. The corresponding event status will be **Cleared** in the NetQoS Event Manager.
- If, after 24 hours, the metric still shows Excessive or Degraded status in the UC Monitor data source, a new UC Monitor Incident will open and will be tied to the existing Event Manager event.
- If a NetQoS Performance Center user tries to change the state of a UC Monitor event to **Closed**, the event actually changes to an **Acknowledged** state in the UC Monitor interface, while appearing to be **Closed** in the Event Manager. This behavior conforms to UC Monitor rules for Incident closure. It applies to events that are closed by Event Manager users or by an external system, such as a system management platform.
- The same event appears as **Cleared** if the associated Incident closes successfully (and automatically) in NetQoS UC Monitor.

Use the **Audit Trail** feature to determine whether a UC Monitor event with Closed status is actually still open in the UC Monitor data source. You can see the Audit Trail by right-clicking an event and selecting **Details**.

Acknowledging Events

As stated above, NetQoS Performance Center operators can manually close some types of events in the Event Manager. The act of closing an event changes its status to **Cleared**. However, the events that originated as Incidents in NetQoS UC Monitor or in NetQoS SuperAgent obey a closure logic that prevents them from being manually closed. These events can be acknowledged by NetQoS Performance Center operators, but not closed. They are only placed in Cleared state by their own Incident closure logic, which is automatic.

Placing an event in **Acknowledged** state notifies other NetQoS Performance Center operators that an IT staff member has been assigned to investigate the event.

To acknowledge a UC Monitor event in the Event Manager:

1. Navigate to the Events report page in the NetQoS Performance Center.
2. By default, only events from the last hour are shown on the Events page. If the UC Monitor Incident occurred in the past, use the Time Period Selector to select a longer timeframe, such as **Last Day**.
3. Find the event in the Event List. If necessary, click the page numbers at the bottom of the **Event List** view to see the full list of recent events.
4. Right-click the event, and select **Acknowledge**.

Starting with version 6.0 of the NetQoS Performance Center, you can set up notifications to alert you when an event changes status, including when it is acknowledged. The NetQoS Performance Center online Help contains a full set of instructions for using the Event Manager notifications feature.

Index

Corporate Headquarters
5001 Plaza on the Lake
Austin, TX 78746

tel: 512.407.9443
877.835.9575
fax: 512.407.8629

www.netqos.com