Cisco Unified Service Monitor Tutorial

Cisco Unified Communications Management Suite

About This Tutorial

- Explore the Unified Communications environment and tools
- Highlight the key features of Cisco Unified Service Monitor
- Follow along with various scenarios detailing how to use Service Monitor for managing Unified Communications
- Provide system administration guidelines for Service Monitor
- Provide links to additional information on Service Monitor

About This Tutorial

Welcome to the Service Monitor (SM) tutorial! This tutorial provides self-paced training focused on using the key features of Cisco Unified Service Monitor, Cisco 1040 sensors, and CVTQ – the Cisco Voice Transmission Quality algorithm .

The tutorial is structured as a series of self-paced chapters that explore the architecture, key features, common usage, and system administration guidelines for the product. Also included as part of the tutorial is a helpful reference section containing links to technical documents on component products, concepts, and terminology. The tutorial material is presented through text, illustrations, hypertext links, and typical scenarios.

This tutorial is an excellent resource to introduce you to using the many features found in the Service Monitor product.

How the Tutorial Is Organized

Chapter 1 Introduction	Explore the Unified Communications environment, the challenges, and tools for managing
Chapter 2 Service Monitor (SM) Product Features	Learn about the key features of SM for managing the Unified Communications infrastructure
Chapter 3 Service Monitor Scenarios	Using several examples, learn how to deploy and configure SM and the Cisco 1040 sensors
Chapter 4 System Administration Guidelines	Review important system requirements, installation guidelines, and system administrative functions
Chapter 5 Helpful Links to Reference Material	A comprehensive set of links to more information on Service Monitor and related topics

How This Tutorial Is Organized

The tutorial is divided into five chapters:

Chapter 1: Introduction to IP Communications

This chapter highlights challenges often encountered in the IP Telephony environment and ways to manage the IP Communications (IPC) devices and services.

Chapter 2: Service Monitor Product Features

This chapter discusses the key features of the Service Monitor (SM) and the Cisco 1040 sensors which report to SM. The product is presented through both discussions of the major functional components and screen shots of many key features.

Chapter 3: Service Monitor Scenarios

This chapter walks you through step-by-step examples to provide hands-on experience using the Service Monitor application and the Cisco 1040 sensors. The case studies begin with steps on planning, how to get started, followed by using various features to monitor and analyze call streams.

Chapter 4: System Administration Guidelines

This chapter provides information about the client and server requirements, software installation guidelines, security administration, periodic maintenance, and troubleshooting tips.

Chapter 5: References

This chapter contains a list of additional product information, such as links to related white papers and documentation.

<Intentionally Left Blank>

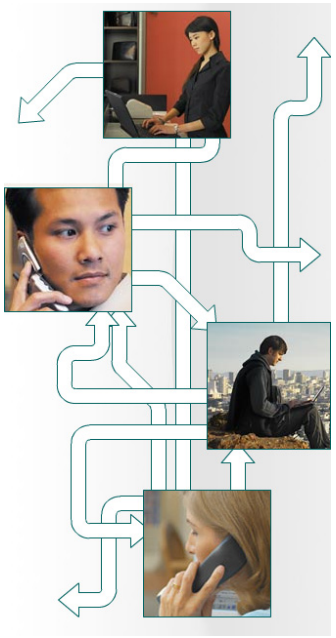
Cisco Unified Service Monitor

Introduction

Chapter 1

Chapter 1 Outline

- Managing Unified Communications
  - Environment
  - Challenges
- Cisco's Solution
  - Unified Service Monitor
  - Unified Service Monitor



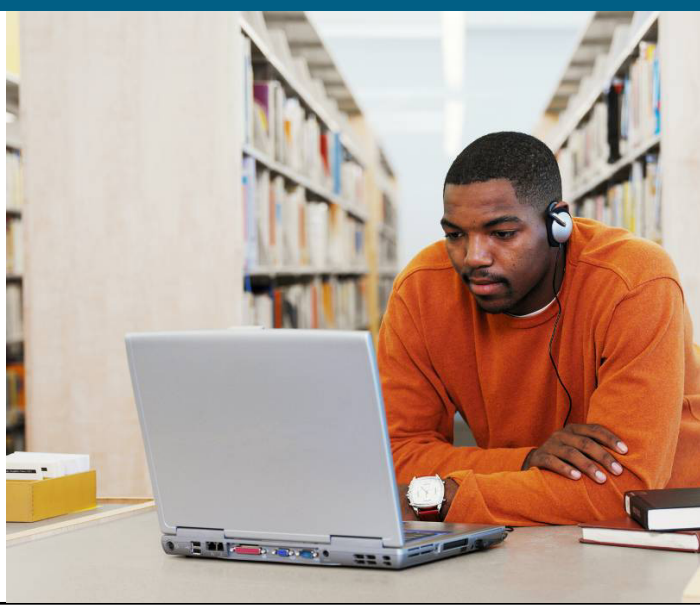
Chapter 1 Outline

This chapter will set the stage for managing Unified Communications devices and services and introduce you to a family of CiscoWorks products that can help you overcome the challenges to managing the Unified Communications environment.

Chapter 2 will then focus on all the features provided specifically by Service Monitor and the Cisco 1040 sensors, followed by several scenarios in Chapter 3 that illustrate how to deploy and use some of the key features of these products. Chapter 4 will present system administration topics, including installation requirements, post installation tasks, features or tasks specific to the system administrator, and troubleshooting tips. Finally, use Chapter 5 as a way to find all your links to important information on Service Monitor.

Managing Unified Communications

- **Managing Unified Communications**
- Cisco's Solution



What is Unified Communications?

Cisco Unified Communications is an integrated and open portfolio of products and applications that unify and simplify all forms of communications, independent of location, time, or device

Unified Communications that ….

- Eliminate Chaos
- Control Costs
- Improve Processes
- Increase Satisfaction
- Enhance Productivity
- Improve Competitive Advantage

What is Unified Communications?

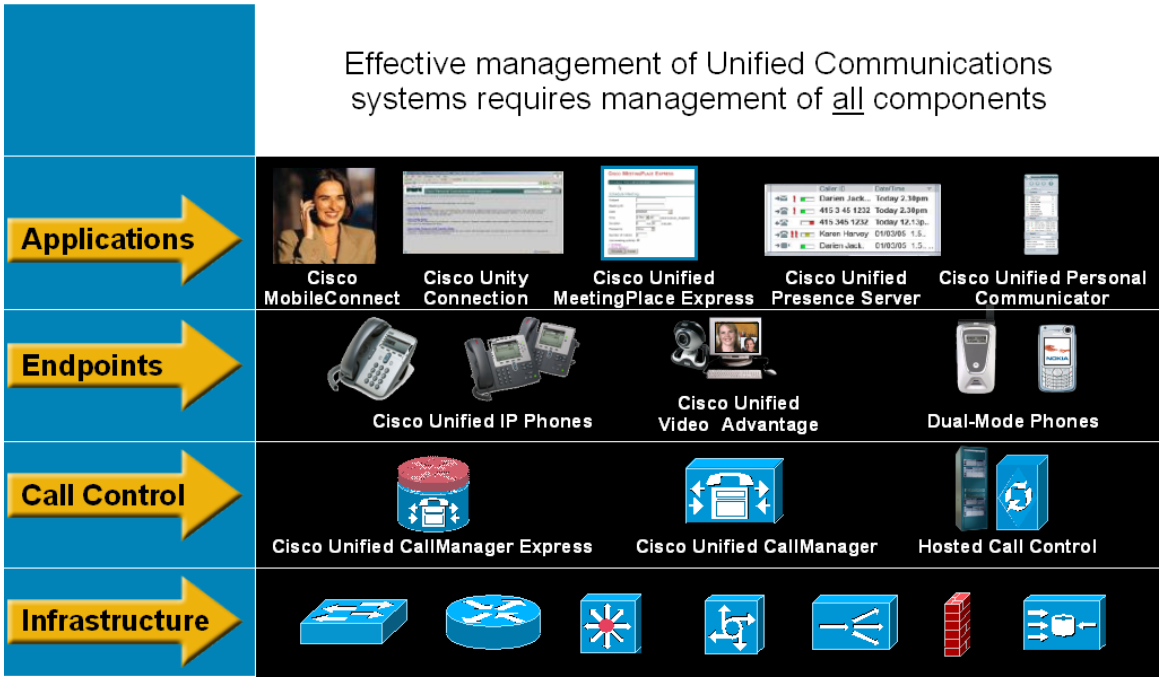
Today's organizations must contend with increasingly complex communication environments featuring a wide array of communication methods. Employees, business partners, and customers communicate with one another through infinite combinations of phones, voice messaging, e-mail, fax, mobile clients, and rich-media conferencing. Too often, however, these tools are not used as effectively as they could be. The result is information overload and misdirected communications that delay decisions, slow down processes, and reduce productivity.

Unified Communications solutions have proven their ability to help organizations solve such problems, enabling them to streamline business processes and reduce costs. For years, companies of all sizes have been realizing the benefits that carrying voice, data, and video communications across a common, IP infrastructure can bring.

Today, with the Cisco Unified Communications system of voice and Unified Communications products, those benefits are greater than ever. Instead of simply connecting products, the Cisco Unified Communications system provides structure and intelligence that helps organizations integrate their communications more closely with business processes, and ensure information reaches recipients quickly, through the most appropriate medium.

Businesses can collaborate in real time using advanced applications such as videoconferencing; integrated voice and Web conferencing; mobile IP soft phones; voicemail; and more-from an integrated, easy-to-use interface. The solution saves time and helps control costs, while improving productivity and competitiveness. In a 2005 Sage Research study, 86 percent of companies using Unified Communications reported that productivity benefits have grown. More than 60 percent reported savings of three or more hours per week for each mobile worker. Such studies confirm that migrating to a Unified Communications system provides a substantial return on investment (ROI) and a reduced total cost of ownership (TCO).

The Cisco Unified Communications portfolio is an integral part of the Cisco Business Communications Solution-an integrated solution for organizations of all sizes that also includes network infrastructure, security, network management products, wireless connectivity, and a lifecycle services approach, along with flexible deployment and management options, financing packages, and third-party communications applications.



Managing Unified Communications

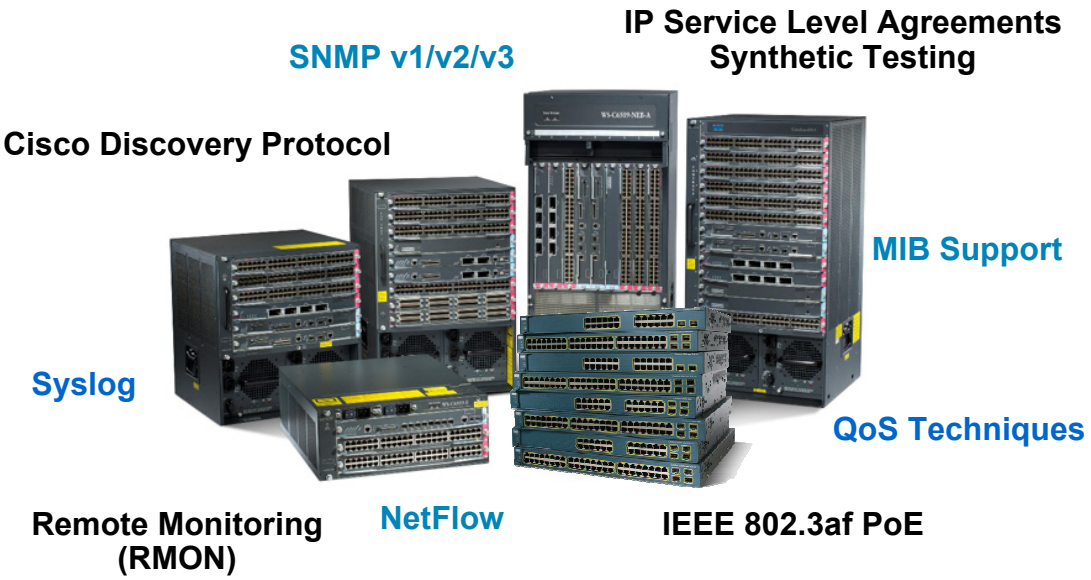
Not long ago, Unified Communications was synonymous with IP telephony and organizations adopted it primarily to save money on phone bills and network support. But today, Unified Communications encompasses so much more than IP telephony, and companies are capitalizing on their quality of service (QoS)-enabled IP networks that they built for IP telephony for more advanced multi-media applications.

The Unified Communications environment consists of the IP transport devices and the IP communications intelligence built into the Unified Communications application services. It is a comprehensive system of powerful enterprise-class solutions which include:

- IP Telephony—provides the full array of telephony services users expect in a business communications solution. It bridges IP communications protocols with the existing time-division multiplexing (TDM) network. It enables you to use either the TDM public network or managed IP networks to connect locations.
- Unified Messaging—delivers powerful messaging tools (e-mail, voice, and fax messages sent to one inbox) and intelligent voice messaging over a single integrated system
- Rich Media Collaboration—bringing video and high-quality audio together to make conferencing as productive and natural as face-to-face meetings.
- IP Customer Contact solutions—delivers intelligent contact routing, integrated interactive voice response, and multimedia contact management to contact center agents over an IP network.

Enabled by an intelligent wired or wireless network, communication now extends to wherever your employees are. Deployed as a comprehensive system, Unified Communications is more than dial-tone replacement. The benefit is a dramatic improvement in operational efficiencies, organizational productivity, and customer satisfaction. With the deployment of Unified Communications you create a collaborative workforce, increase competitive advantage, and deliver measurable ROI. A smooth operation does not come without obstacles; the Unified Communications environment needs to be carefully designed, deployed, and managed.

Managing Unified Communications
Intelligent Infrastructure

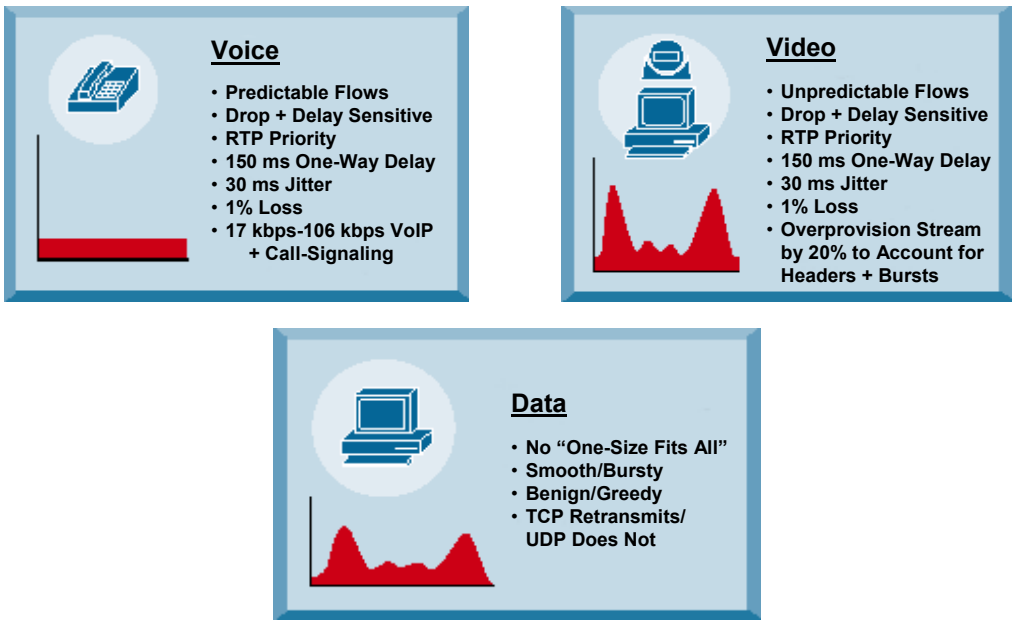


Using a Knowledgeable Infrastructure

Routers and switches comprise the basic infrastructure elements of your network. There are few important factors when choosing a router or switch for IP Communications, including the number of phones, which call-processing solution you select, and the other functions the router will perform.

Technology-specific resources available in Cisco devices can assist you with network design, configuration, maintenance and operation, troubleshooting, and other network management support.

Managing Unified Communications
Understanding Traffic and Acceptable Service Levels



Understanding Traffic and Acceptable Service Levels

The actual bytes and packets that travel across the network all look the same. The difference lies at its endpoints when you combine the packets together. How quickly the packets travel through the network and how they are handled at each interconnect make a big difference in the final product. These difference can either be tolerable or they can completely ruin the end product.

For example, take data traffic, consisting of and e-mails, file transfers, or web browsing. Data like this is bursty in nature as people work locally at their computers and then send large amounts of data across the network through email attachments or file transfers. The data will arrive at its destination sooner or later and may need to be queued or retransmitted when the network bandwidth is low. But overall, the user never notices the delay unless they are in a hurry.

But voice and video across the IP network is much different. The type of traffic is sensitive to queuing or delays in the network. Voice traffic requires that the inter-arrival time of the packets holding the voice data is consistent (little or no jitter) and that there be little or no packets lost. Therefore, network managers look for measurable statistics such as jitter, packet loss, and end-to-end network latency, in order to ensure acceptable service levels.

Managing Unified Communications
Terminology

RTP	Real-Time Protocol) is an IP protocol used to transfer voice traffic across the IP network
SPAN Port	A port on a device used to copy packets, such as RTP packet streams) from other ports or VLANs for further analysis by another device (probe or sensor)
ITU R-Factor	ITU standards based scoring value (1-100) calculated from evaluating a monitored IP call
MOS Scoring	(Mean Opinion Score) A widely accepted scoring value (1-5) also used to evaluate a monitored IP call
QoS	(Quality of Service) Improve the performance of specific applications that are intolerant to delays using techniques (queuing, marking) and algorithms
QoV	(Quality of Voice) – Evaluation of voice over IP by monitoring packet loss and Jitter characteristics of the call stream

Terminology

As we move forward, a good understanding of these commonly used terms is important. These terms will be used frequently in this tutorial. If you need more information on these terms, inks to more information on IP Communications can be found in Chapter 5 of this tutorial. Also, more information on the R-factor and MOS scoring and the meaning of the scores can be found in Chapter 2 of this tutorial.

Managing Unified Communications
Measurable Service Quality Metrics

Response Time / Latency	The elapsed time between the end of a query on one end of a conversation pair and the beginning of a response from the other end of a pair. Latency, a function of response time, is any characteristic of a network or system that increases the response time.
Availability / Outages	Critical to IP Communications is the availability of the network and the Unified Communications services (CallManager, Unity, SRST)
Jitter	The amount of variation in the delay of received voice/video packets. Packets are sent in a continuous stream with the packets spaced evenly apart. Due to network congestion, improper queuing, or configuration errors, this steady stream can become lumpy, or the delay between each packet can vary instead of remaining constant which is desired for good quality.
Network Utilization Patterns	Trending how the network is being used, by protocols, users, and how the patterns are changing is critical in a converged data/voice networks
Thresholds	User defined limits that when metrics cross the threshold value, it triggers an alert or event condition

Measurable Service Quality Metrics

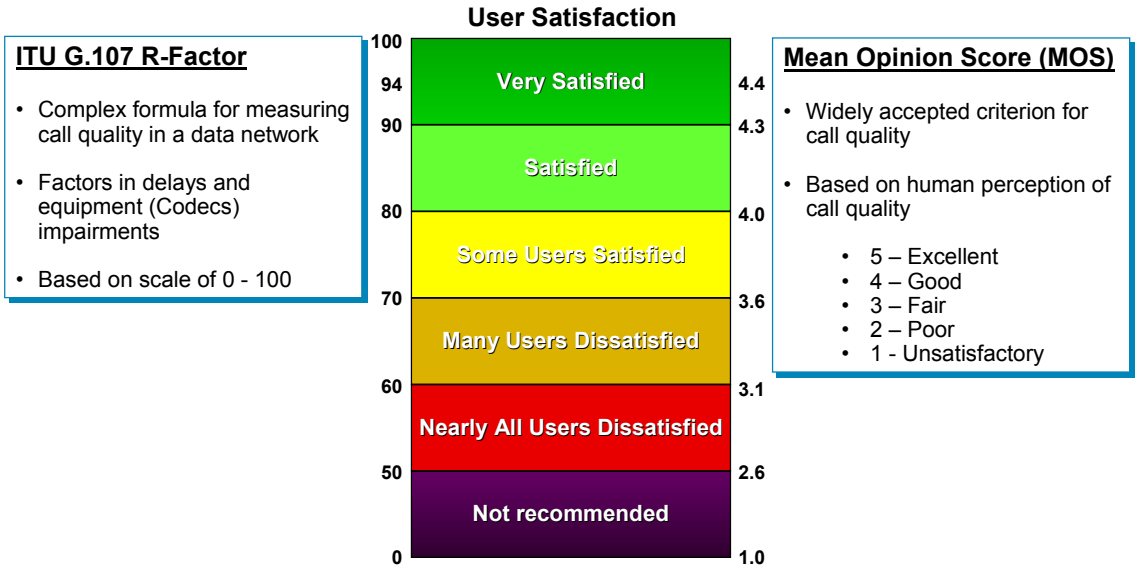
Network managers look for measurable statistics such as jitter, packet loss, and end-to-end network latency, in order to ensure acceptable service levels. Familiarize yourself with these metrics and what they mean in terms of absolute value, or when comparing or trending over time.

Utilization, response time, latency (delays), packet loss, and availability metrics are familiar statistics to most network managers. What may be new to some managers is the metric, Jitter. To better explain jitter, let's look at an example:

- If a source device sends multiple packets consecutively to a destination at ten millisecond intervals, and if the network is operating optimally, the destination should receive them at ten-millisecond intervals. However, delays (i.e. queuing, or arriving through alternate routes) in the network can cause inter-packet arrival delay of greater or less than ten milliseconds.
- Positive jitter implies that the packets arrived at intervals of more than ten milliseconds. If they arrive twelve milliseconds apart, then positive jitter is equivalent to two milliseconds. Negative jitter is computed similarly. Greater values of jitter (both positive and negative) are undesirable for voice networks, and a jitter value of zero is ideal for delay-sensitive networks.
- Voice and video traffic is recommended to have 30 ms of jitter or less.

As with all monitoring metrics, the statistics should be gathered periodically and evaluated regularly for upward trends or irregular conditions.

Managing Unified Communications
Measurable Voice Quality Metrics



Measurable Voice Quality Metrics

These types of metrics provide the network manager with voice quality statistics that can gauge the user's call satisfaction level.

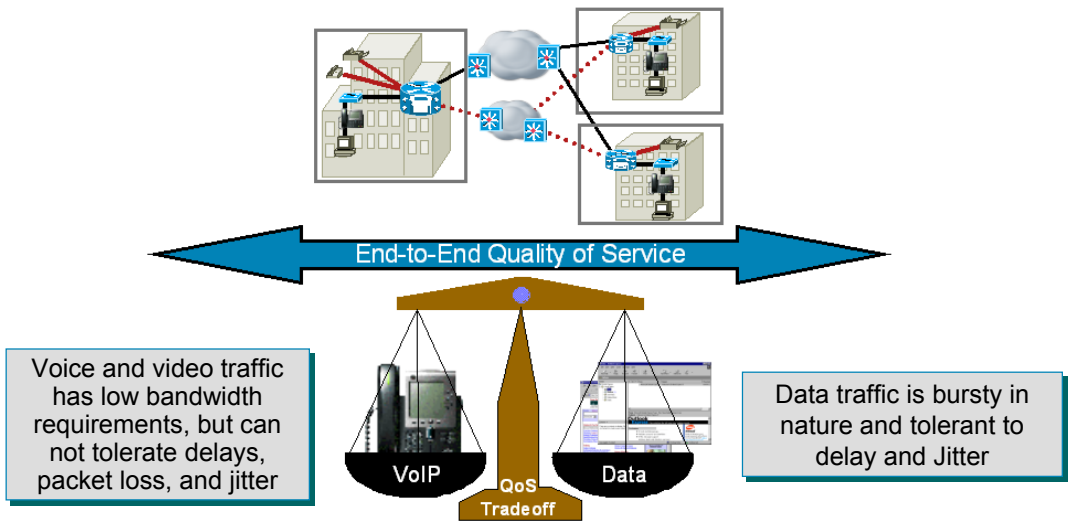
Traditionally, measuring call quality has been very subjective: a human picks up the phone and listens to the voice and provides his or her perception on the quality of the call. In fact, this is the basis for the widely accepted criterion for call quality, the *Mean Opinion Score (MOS).*

In the past, a group of humans would listen to various calls and rate them from 1 to 5 or Unsatisfactory to Excellent. Obviously, this is not a very good mechanism for evaluating call quality for a large number of calls (never mind the privacy issues!). Luckily, many algorithms have become quite adept at predicting the human perception of a call. Unfortunately, some of these algorithms do not scale well, and are not suited for determining voice quality when the calls are transmitted over data networks since many other factors now come into play.

G.107 R factor is an algorithm that was developed specifically for determining voice quality in a data network. Among other things, this algorithm takes into account delays and equipment impairment factors, and creates a score between 0 and 100 (poor to excellent). So using G.107 would be an excellent way to gather measurable statistics for call quality. However, since the MOS is still the most widely used metric for call quality, converting the R factor into a MOS value is desirable.

Managing Unified Communications
The Challenges

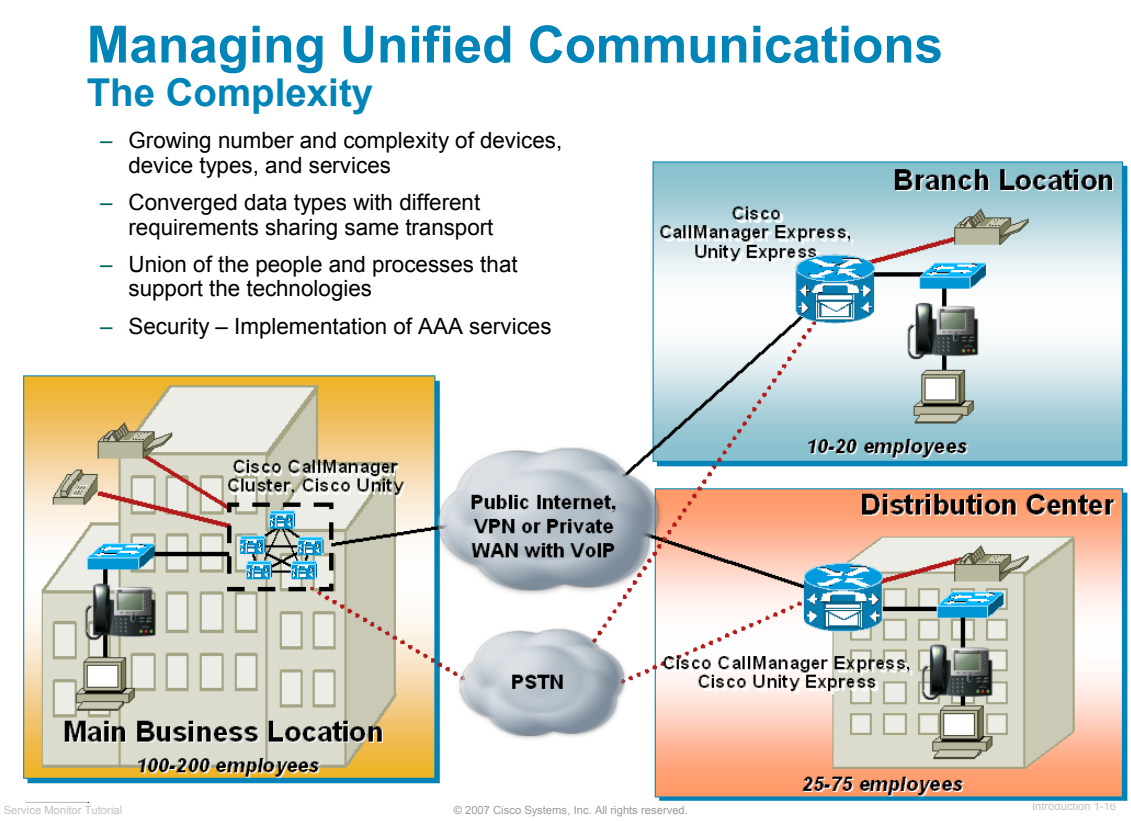
With converged networks, network administrators need to ensure adequate availability and bandwidth for deploying multiple services over IP packet-based networks



The Challenges

Businesses are constantly searching for methods to increase their effectiveness while attempting to cut costs. One cost savings step was the convergence of their voice, video, and data networks. Converged networks present businesses with a new communications paradigm, which has the potential to create new business efficiencies and increased employee productivity while cutting cost dramatically.

Cisco's AVVID (Architecture for Voice, Video, and Integrated Data) brings a standards-based open-architecture to multi-service networking. Cisco AVVID does away with the extremely inefficient disparate facilities for each application transport by allowing the enterprise network to converge over a common IP transport. Of course, the flexibility provided to voice and video solutions by AVVID also presents new management challenges for the network managers; namely the ability to ensure adequate availability and bandwidth for the mixed services now running over a single network.



The Complexity

Deployment of IP telephony is not simply a convergence of voice and data technologies, rather it is a convergence of the people and processes that support the technologies. To approach the challenge, companies often divide IP telephony into two components: the infrastructure and the services. One set of people and processes for each.

The converged infrastructure of components is ever growing. Now consisting of complex voice and data networking elements, new modules, new configurations for quality of service algorithms, and not to mention the IP phones themselves.

Through all the advances in technology, a network manager must never forget the importance of securing the services provided. Luckily, the same advanced security technologies that protect data networks can now protect converged networks carrying data, voice, and video traffic. Cisco recommends an integrated security policy to protect the integrity, privacy, and availability of a Cisco Unified Communications system. Integrating multiple layers of security technologies increases overall security by preventing a single configuration error or compromise from impacting the system. The three primary categories for securing the deployment are: network security, host security, and Authentication, Authorization, and Accounting (AAA) services.

(Links to more information on Unified Communications can be found in Chapter 5 of this tutorial.)

Managing Unified Communications
The Questions

- What device conditions lead to voice service degradation?
- What attributes should be polled or monitored to determine these conditions?
- How can the availability of critical voice services be ensured on a regular basis?
- How can the quality of voice be ascertained for active VoIP calls?

The Questions

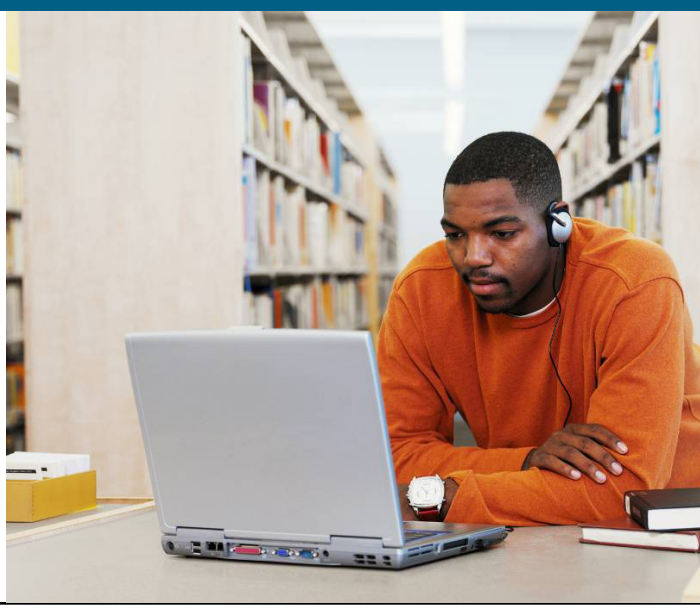
So the decision was made a long time ago to deploy IP telephony and now that has expanded to more than just voice calls over your IP network. Your role as a network manager is ever changing and now you are asking questions like these above.

So where does one begin to answer some of these questions? Let's take a further look.

<Intentionally Left Blank>

Cisco's Solution

- Managing Unified Communications
- **Cisco's Solution**



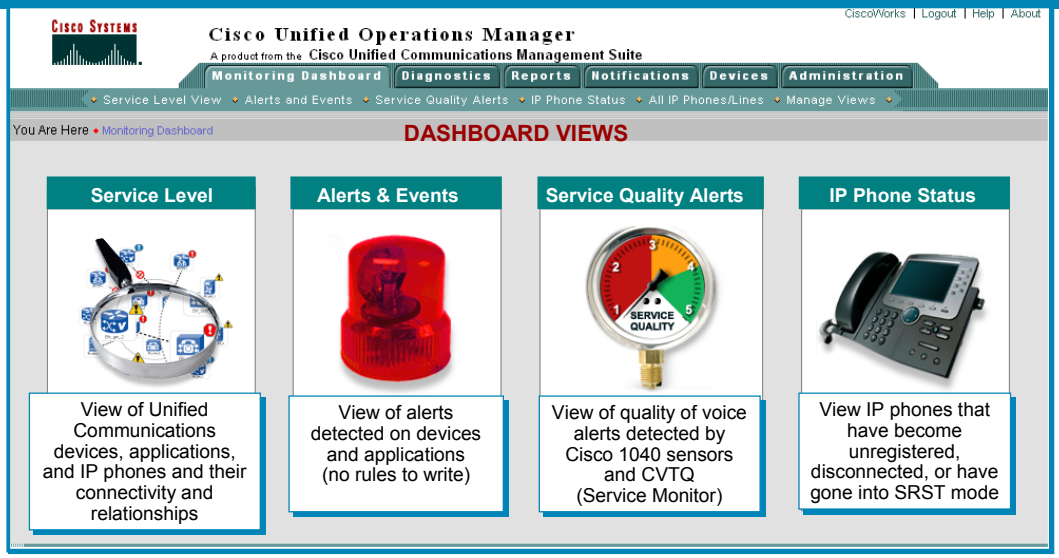
Cisco's Solution
Unified Communications Management Suite

Unified Communications Management Suite

The Cisco Unified Communications Management Suite is designed to work with the Cisco Unified Communication portfolio of products to improve productivity and reduce total cost of ownership through automation, integration, and simplification.

Cisco's Solution
Cisco Unified Operations Manager (OM)

Presents a comprehensive real-time view of the Unified Communications infrastructure including the operational status of each component…



Cisco Unified Service Monitor

Cisco Unified Operations Manager is part of the Cisco Unified Communications Management Suite. Operations Manager (OM) uses open interfaces and numerous types of diagnostic tests to continuously monitor and evaluate the current status of both the Unified Communications infrastructure and the underlying transport infrastructure of the network. Operations Manager does not deploy any agent software on the devices being monitored and thus is non-disruptive to system operations.

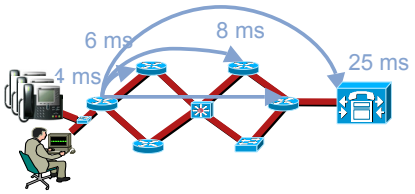
Information is presented by a series of 4 dashboards (representing different service-level views of the network), providing the network manager with a comprehensive view of the Unified Communications infrastructure and its current operational status.

Learn more about Operations Manager by reviewing the Cisco Unified Operations Manager Tutorial and Chapter 5 of this tutorial for more information.

Cisco's Solution
Cisco Unified Service Monitor, (Cont.)

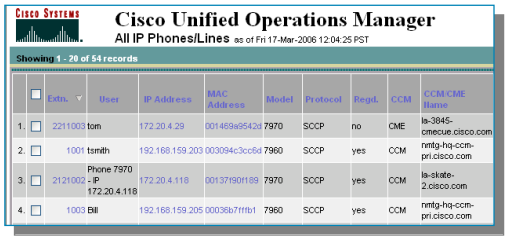
Diagnostic Tests

- Replicate **end user activities** (end-to-end calls, phone registration, dial tone, conference, message waiting, emergency call)
- Replicate **protocol traffic** (IP SLA-based) to measure latency / Jitter / packet loss; Gateway registration



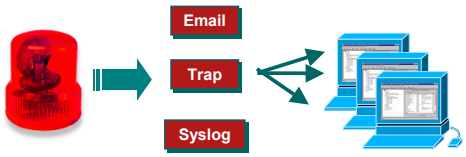
Report Generation

- IP Phone and Device Inventory / Change Reports / Video enabled IP Phone reports
- Service Impact Reports
- Alert and Event History
- Personalized Reports
- Performance Reports (72 hr.)



Notification Services

- Immediate notification of selected alerts using Email, SNMP traps, or Syslog messaging



Cisco Unified Operations Manager, (Cont.)

In addition to the Dashboard Views, Operations Manager has many other features that automate and simplify the network management tasks. These features include:

Diagnostic Tests

Operations Manager comes with a rich set of diagnostic tests that can be used to aid in trouble isolation and resolution. There are primarily three types of tests: synthetic tests, phone status tests, and node-to-node IP SLA tests. The synthetic tests serve to replicate user activity (getting dial tone, making phone calls, leaving voice mail, and creating or joining conference calls). The phone status tests can be used to determine the current operational status of the IP phones in terms of signaling (SIP and SCCP) and IP connectivity. The node-to-node tests use the services of the Cisco IP Service Level Agent (IP SLA, formerly known as Service Assurance Agent [SAA]) in Cisco routers to simulate traffic in the network and then determine network characteristics such as reachability status, response time, latency, jitter, packet loss, and network quality.

Report Generation

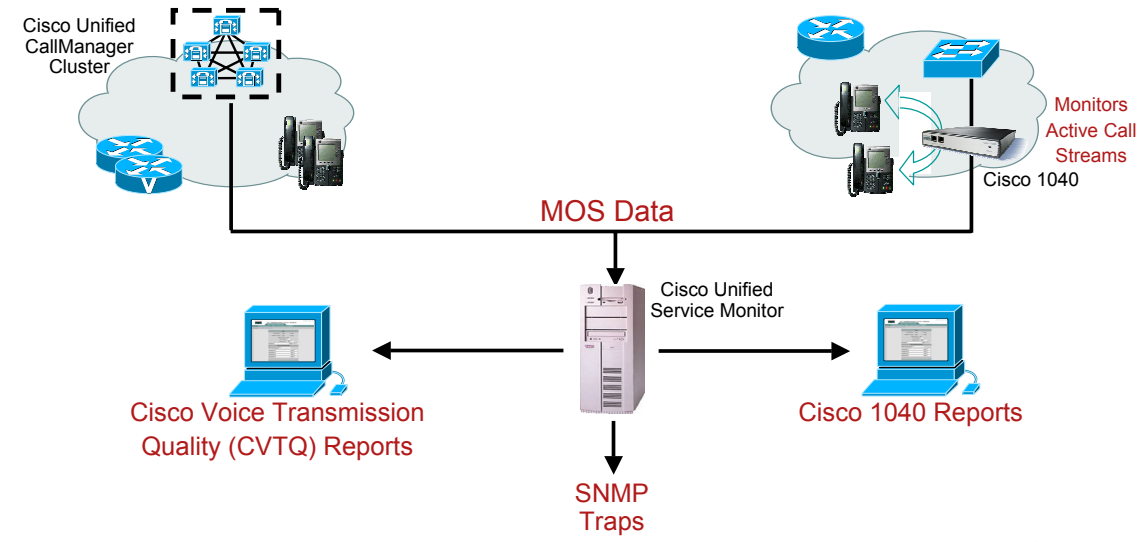
Operations Manager provides an extensive set of reports that help network managers maintain information about their Cisco Unified Communications deployment. The historical alert, event, and service-quality reports maintain information about all the alerts and events reported by Service Monitor for up to 30 days. This enables network managers to document any past outage and have access to it for long-term trending purposes.

Notification Services

Operations Manager allows the administrator to notify end-users based on type of event for a given subset of devices. The notification can be in the form of an email, Syslog message, or SNMP trap.

Cisco's Solution
Service Monitor (SM) and Cisco 1040 Sensors

Service Monitor manages Cisco 1040 sensors and analyzes and reports on voice quality using Mean Opinion Scores (**MOS**) received from Cisco Unified CallManager clusters and the Cisco 1040 sensors



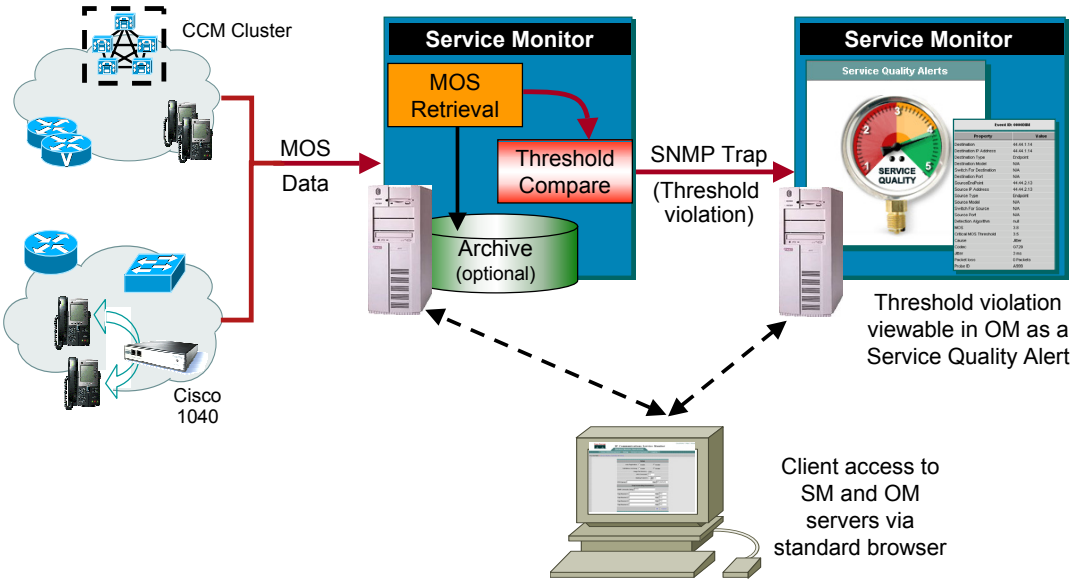
Cisco Unified Service Monitor / Cisco 1040 Sensors

Cisco Unified Service Monitor is another application in the Cisco Unified Communications Management Suite. Service Monitor (SM), Cisco 1040 sensors, and the Cisco Unified CallManager clusters provide a reliable method of monitoring and evaluating voice quality for IP phones. The Cisco 1040 sensor continuously monitors active calls supported by the Cisco Unified Communications system. Cisco Unified CallManagers store MOS values for calls that are calculated on gateways and phones using the Cisco Voice Transmission Quality (CVTQ) algorithm. The Service Monitor gathers the MOS statistics from the sensors and CallManagers and provides near-real-time notification when the voice quality of a call fails to meet a user-defined quality threshold.

Below is a brief description of the Cisco Unified Service Monitor components:

- ***Cisco 1040 Sensor*** – A hardware appliance or probe used to monitor quality of voice for up to 80 active RTP streams. The call quality is calculated using the ITU G107 R-factor algorithm and converted into a Mean Opinion Score (MOS). The sensor then forwards a quality of voice metric (MOS) for each monitored stream every 60 seconds to the Service Monitor server.
- ***Service Monitor***– Compares the quality of voice metrics incoming from the Cisco 1040 sensors and managed Cisco CallManagers to user-defined thresholds. If a threshold violation is detected, Service Monitor will forward a SNMP trap containing the pertinent information to up to four trap recipients. Service Monitor can also optionally archive all incoming metrics, and is used to manage the configuration and image files for the Cisco 1040 sensors.

Cisco's Solution
Product Integration



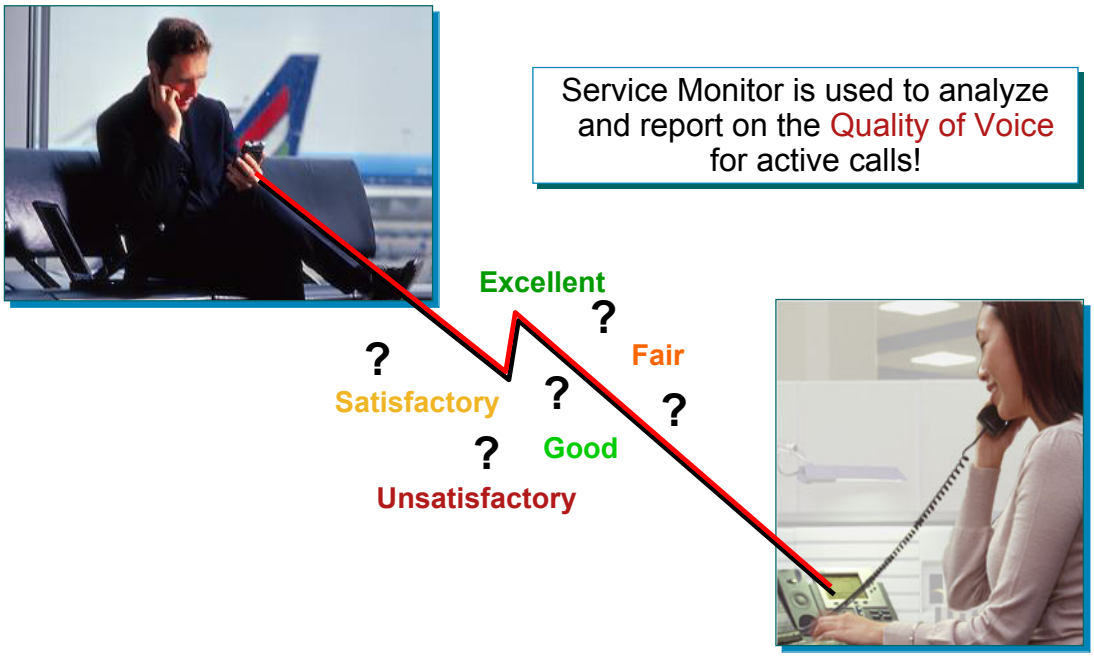
Product Integration

The products within the Cisco Unified Management Suite work together to form a complete solution to managing Cisco Unified Communications.

The Cisco Unified Communications Management Suite consists of the two applications previously introduced: Unified Operations Manager and Unified Service Monitor. When integrated together, the Service Monitor application provides Quality of Service information to Operations Manager, which then displays the information in the Service Quality dashboard.

How to configure the integration is describe within the Operations Manager tutorial.

Tutorial Focus - Service Quality Reporting
Service Monitor (SM)



Service Monitor (SM)

This tutorial focuses on the Service Monitor application of the Cisco Unified Management Suite. Service Monitor provides a low-cost, reliable method of monitoring and evaluating the quality of a user's IP Communications-based telephony experience. The end-user experience is analyzed by the Cisco 1040 sensor, and reported as a MOS score every 60 seconds to the Service Monitor server. The MOS score defines the quality of the call.

The quality of voice metrics are optionally summarized and stored in a data file on the SM server for subsequent analysis and reporting by any of several third-party applications.

Thank You!

Continue on to Chapter 2 to discover the many features of Service Monitor.

Cisco Systems

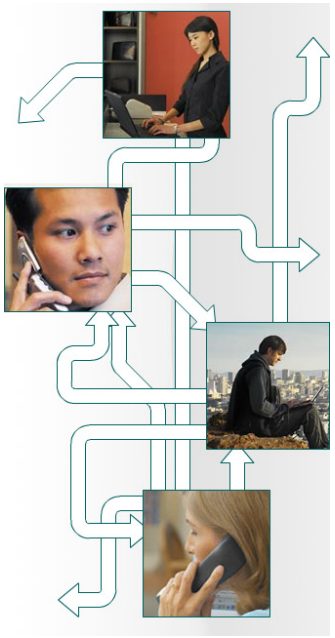
Cisco Unified Service Monitor

Product Features

Chapter 2

Chapter 2 Outline

- Product Overview
- Functional Architecture
- Deployment Options



Chapter 2 Outline

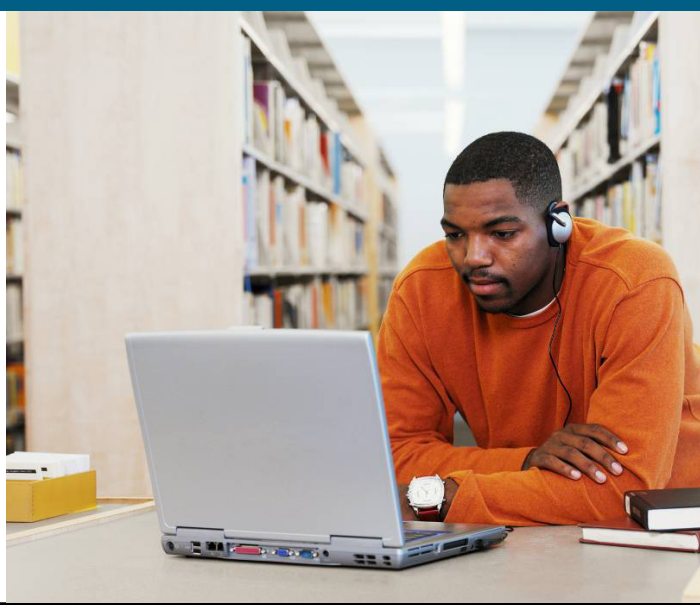
Hopefully Chapter 1 has excited you to the benefits of monitoring the quality of voice for active calls using Cisco Unified Service Monitor (SM)!

The first section of this chapter takes a high level look at Service Monitor and its key features and functions. Next, the functional architecture of the Service Monitor solution is discussed, and finally, this chapter presents different options for deploying Service Monitor in the network.

By the conclusion of this chapter, the reader should have a good understanding of Service Monitor and its features. Chapter 3 will then provide the jumpstart to using Service Monitor through a series of scenarios that takes you from Getting Started through the viewing of quality of voice alerts detected by Service Monitor.

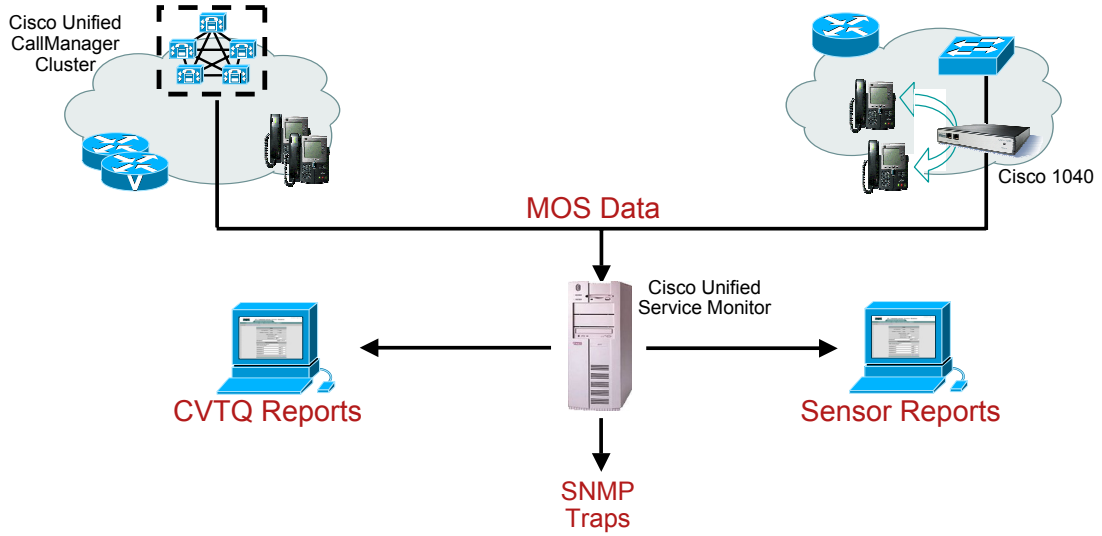
Product Overview

- **Product Overview**
- Functional Architecture
- Deployment Options



Product Overview
Cisco Unified Service Monitor

Service Monitor analyzes and reports on voice quality using Mean Opinion Scores (**MOS**) received from Cisco Unified CallManager clusters and Cisco 1040 Sensors



Product Overview - Cisco Unified Service Monitor

Cisco Unified Service Monitor is an application in the Cisco Unified Communications Management Suite used to monitor quality of voice in real-time. Cisco Unified Service Monitor analyzes and reports on voice quality using Mean Opinion Scores (MOS) received from Cisco Unified CallManager clusters and Cisco 1040 Sensors.

This solution helps enable IP network and IP telephony managers to more effectively manage their IP communications infrastructure by providing near real-time quality of voice metrics and providing alerts when the voice quality falls below a user-defined threshold.

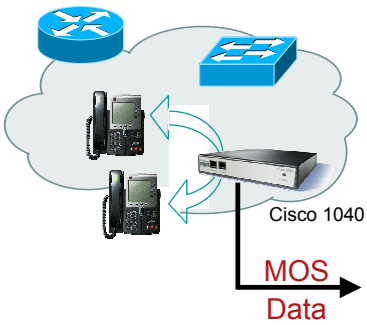
The solution consists of these components:

- ***Cisco 1040 Sensor*** – A hardware appliance or probe used to monitor quality of voice for up to 100 active RTP streams per minutes. The sensor then forwards a quality of voice metric in the form of a Mean Opinion Score (MOS) for each monitored stream every 60 seconds to the Service Monitor server.
- ***Cisco Unified CallManager*** – stores the CVTQ data from gateways and phones in Call Detail Records (CDRs) and Call Management Records (CMRs), which is then sent or retrieved by Service Monitor.
- ***Service Monitor Server*** – Compares the quality of voice metrics incoming from the Cisco 1040s to a user-defined threshold. If a threshold violation is detected, Service Monitor will forward a SNMP trap containing the pertinent information to as many as four trap recipients. Service Monitor can also optionally archive all incoming call metrics, and is used to manage the Cisco 1040 sensors.

Each of these components is described in more detail next.

Overview
Cisco 1040 Sensor Hardware Component

- Real-Time Voice Quality Monitoring
  - Cisco 1040 sensor analyzes active RTP streams between IP phones and calculates a Mean Opinion Score (MOS) value using the ITU G107 R-factor algorithm
  - Monitors up to 100 active RTP streams/min
  - Cisco 1040 MOS value forwarded to Service Monitor via Syslog message every 60 seconds and is then evaluated against user-defined thresholds
- Easy to Deploy and Use
  - Cisco 1040 works like IP Phones – receives power from the connecting switch using IEEE 802.3af Power over Ethernet (PoE) and receives its configuration from TFTP server



Cisco 1040 forwards MOS values every 60 seconds via Syslog message

Cisco 1040 Sensor Hardware Component

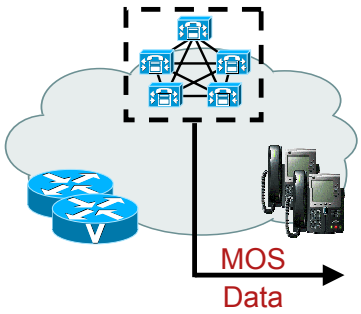
The Cisco 1040 sensor is a hardware appliance strategically placed in the network to monitor active RTP calls streams for voice quality.

Cisco 1040 sensors are strategically deployed in the network and are connected to the SPAN port of a switch to perform the call monitoring aspect, receive power from ports that support Power over Ethernet (PoE), and are easily configured and installed just like an IP phone.

Using a Syslog message, the Cisco 1040 sensors forward call metrics in the form of a MOS value, which is evaluated by the Service Monitor server against a user-defined threshold.

Overview
Cisco Unified CallManager Cluster Component

- Call-based Voice Quality Monitoring
  - A MOS value for an entire call is calculated on gateways and phones using the Cisco Voice Transmission Quality (CVTQ) algorithm
  - At the termination of a call, Cisco Unified CallManager stores the data in Call Detail Records (CDRs) and Call Management Records (CMRs)
  - MOS data is received by Service Monitor and evaluated against user-defined thresholds
    - CCM 4.2.x – Service Monitor pulls the data from the CCM CDR/CMR tables
    - CCM 5.x –The CCM pushes the CDR/CMR records to Service Monitor
  - IP Phones Supported
    - Cisco 7940, 7960, 7941, 7961, 7970 and 7971 IP Phones supported in SCCP mode (New firmware required and can be downloaded from CCM 4.2 or 5.X)
    - All other Cisco IP phones including 7985 does not support CVTQ
    - All SIP based phones do not support CVTQ



Cisco Unified CallManager Cluster Component

A Mean Opinion Score or MOS value for an entire call is calculated on some gateways and IP phones using the Cisco Voice Transmission Quality (CVTQ) algorithm. At the termination of a call, Cisco Unified CallManager stores the CVTQ data in Call Detail Records (CDRs) and Call Management Records (CMRs).

MOS data is received by Service Monitor and evaluated against user-defined thresholds. Depending upon the version of CallManager, the retrieval of MOS data differs:

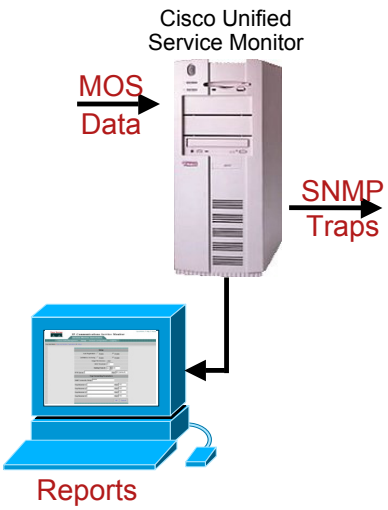
- CCM 4.2.x – Service Monitor pulls the data from the CCM CDR/CMR tables
- CCM 5.x –The CCM pushes the CDR/CMR records to Service Monitor

CVTQ is supported / not supported in the following IP Phones:

- Cisco 7940, 7960, 7941, 7961, 7970 and 7971
- IP Phones supported in SCCP mode (New firmware required and can be downloaded from CCM 4.2 or 5.X)
- All other Cisco IP phones including 7985 does not support CVTQ
- All SIP based phones do not support CVTQ

Overview
Service Monitor Software Component

- Manages and Configures Cisco 1040s
  - Creates Cisco 1040 configuration file
  - Defines Cisco 1040 image file
- Scalability and Redundancy
  - Up to 50 Cisco 1040 sensors per instance of Service Monitor
  - Multiple Service Monitor instances can be deployed (*discussed later in course*)
  - Multiple Service Monitors can be defined for each Cisco 1040 (primary and secondary)
- Integration via North-Bound Interface
  - MOS values forwarded to Service Monitor and evaluated against user-defined thresholds
  - Threshold violations forwarded as SNMP trap; Operations Manager can receive and display traps as Service Quality Alerts
- Reporting
  - Out of the box and customizable voice quality reports



Service Monitor Software Component

Cisco Unified Service Monitor not only retrieves service quality data from Cisco 1040 sensors and Cisco Unified CallManagers. Service Monitor also manages and configures the Cisco 1040 sensors.

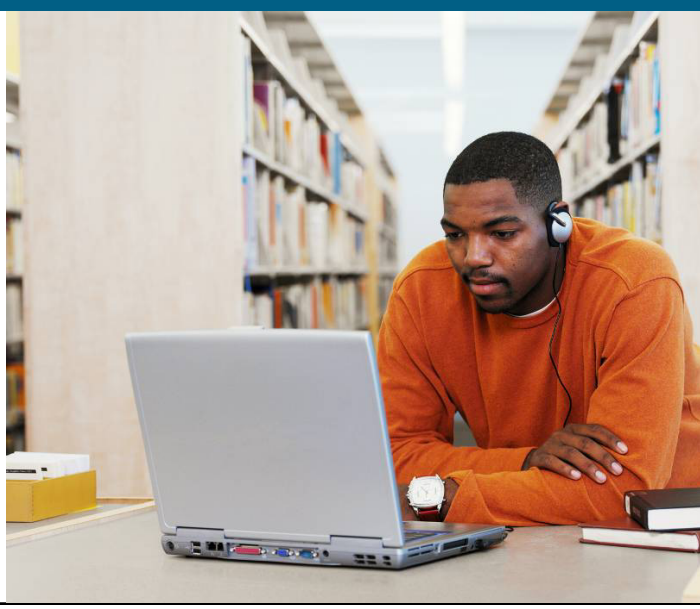
Each instance of Service Monitor software installed is used to receive and evaluate the MOS call metrics for up to 50 Cisco 1040 sensors. There are no limits to the number of Service Monitor servers that can be deployed in a network. For redundancy purposes, each Cisco 1040 can be configured with a primary and secondary Service Monitor server. In the event that the Cisco 1040 loses communication with its primary server, it will start forwarding its metrics to the secondary server automatically.

The MOS value sent by the Cisco 1040 sensor is evaluated by the Service Monitor application and compared against a user-defined threshold. If a threshold violation is detected, Service Monitor sends the violation information as a SNMP trap to up to four recipients. One such recipient, Operations Manager (OM), displays the information on the real-time Service Quality dashboard that also provides a launch point for diagnostic tools and processes.

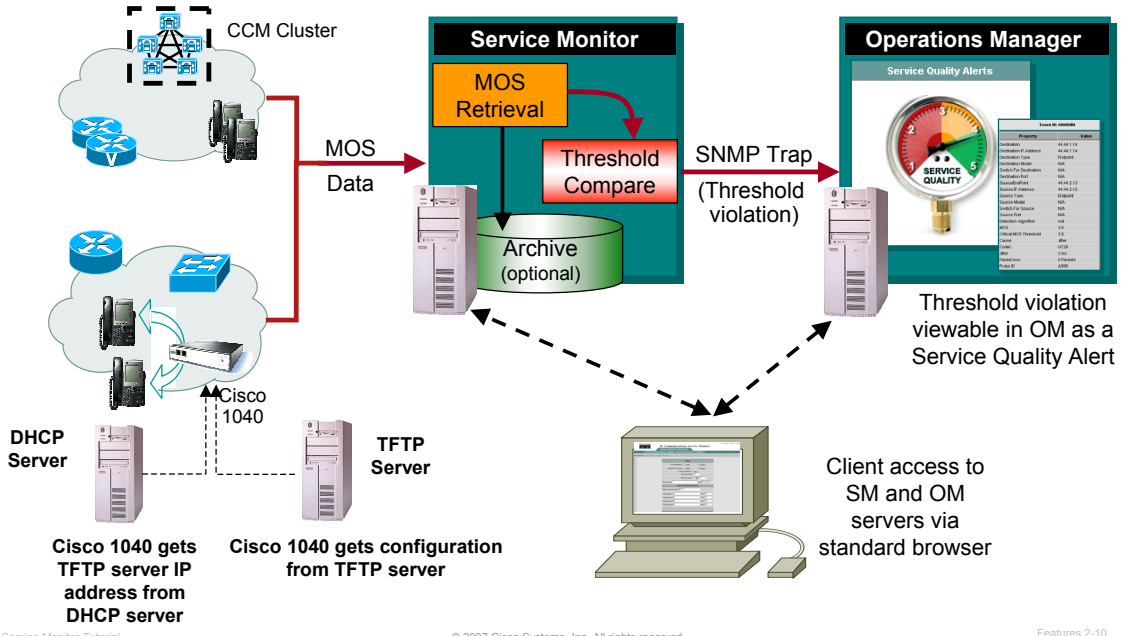
<*Intentionally Blank*>

Functional Architecture

- Product Overview
- **Functional Architecture**
- Deployment Options



Service Monitor Functional Architecture
Overview



Service Monitor Functional Flow

The figure above provides more details about the Service Monitor architecture and how all the pieces work together.

One of the functions of the SM server is to manage the Cisco 1040 sensors. This entails creating the configurations for the sensors which informs the sensor where to forward the quality of voice metrics. These configurations (as well as the Cisco 1040 binary image) must then be manually copied from the SM server to a TFTP server. The reason for this is the Cisco 1040 operates similar to an IP Phone - when it is first booted up it receives not only its IP address from a DHCP server, but also the IP address of a TFTP server (DHCP option 150) where it can find its binary image and configuration.

The sensors have two Ethernet interfaces: one to report the call metrics to the SM server, and the other is connected to the SPAN port of a switch used to continuously monitor active calls. This means that the administrator needs to SPAN the appropriate ports or VLAN to a SPAN port on the connecting switch. The sensor also receives its power from switch ports that support Power over Ethernet (PoE). The sensors monitor each call stream for 60 seconds and then forwards the metrics to the SM server in the form of a Syslog message.

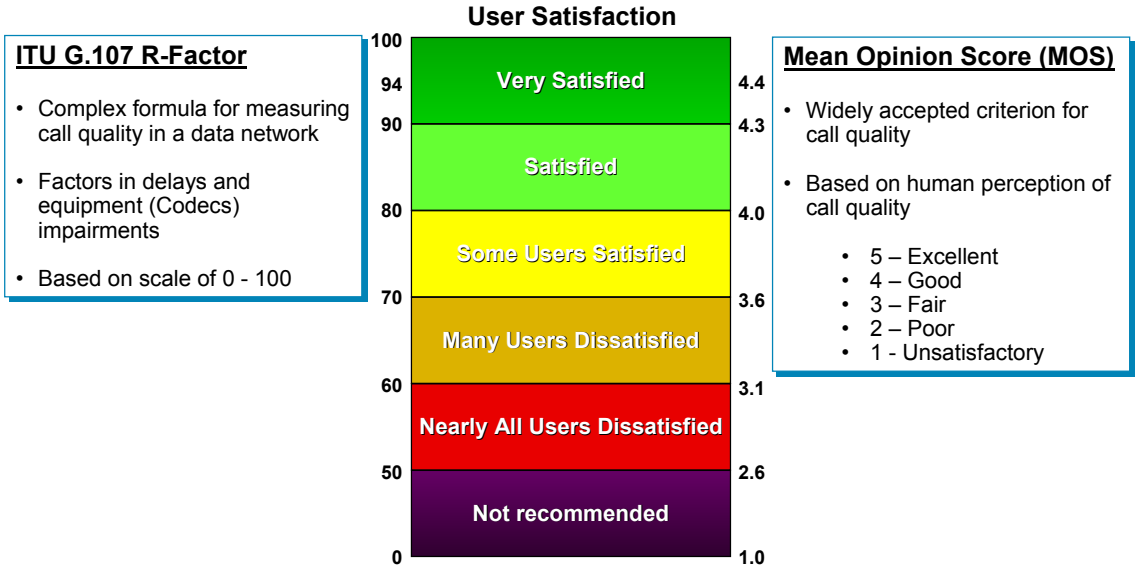
In addition, a MOS value for an entire call is calculated on some gateways and IP phones using the Cisco Voice Transmission Quality (CVTQ) algorithm. At the termination of a call, Cisco Unified CallManager stores the CVTQ data in Call Detail Records (CDRs) and Call Management Records (CMRs).

The SM server retrieves the MOS values from the Cisco 1040s and the Cisco Unified CallManagers and compares the MOS metric against the user-define threshold. Any threshold violation is then forwarded as an SNMP trap to up to four trap receivers. Typically, one of those receivers is Operations Manager which then displays the trap on its Service Quality Alerts dashboard.

Access to both Operations Manager and Service Monitor is via a standard web-browser. (Refer to Chapter 4 for more information on server and client requirements.)

Service Monitor Functional Architecture
Measuring Voice Quality

Cisco 1040s use G.107 and convert score to MOS value to be forwarded to Service Monitor



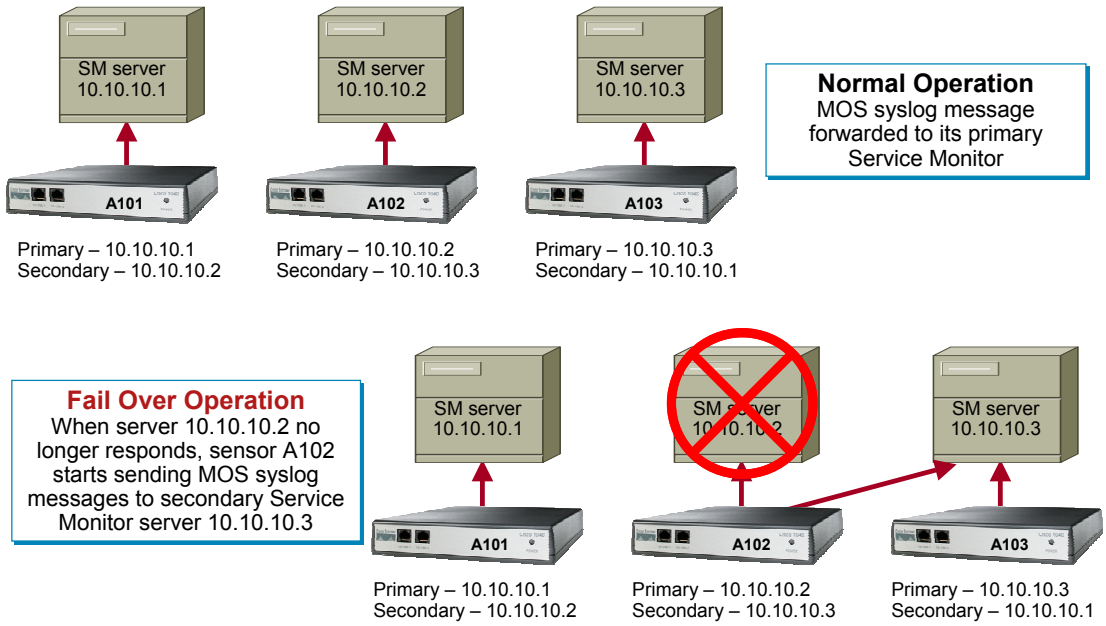
Measuring Voice Quality

Measuring call quality has traditionally been very subjective: a human picks up the phone and listens to the voice and provides his or her perception on the quality of the call. In fact, this is the basis for the widely accepted criterion for call quality, the *Mean Opinion Score (MOS)*. In the past, a group of humans would listen to various calls and rate them from 1 to 5 or Unsatisfactory to Excellent. Obviously, this is not a very good mechanism for evaluating call quality for a large number of calls. Luckily, many algorithms have become quite adept at predicting the human perception of a call. Unfortunately, these algorithms do not scale well, and are not suited for determining voice quality when the calls are transmitted over data networks since many other factors now come into play.

The Cisco 1040 sensors use an algorithm specifically created for determining voice quality in a data network – G.107 R factor. Among other things, this algorithm takes into account delays and equipment impairment factors, and creates a score between 0 and 100 (poor to excellent).

Since the MOS is still the most widely used metric for call quality, the sensor converts the R factor into a MOS value and transmits this to the SM server.

A similar algorithm is used for the CVTQ values. In the end, both the Cisco 1040 sensors and Cisco Unified CallManagers report MOS to the Service Monitor application.



Cisco 1040 Reporting Redundancy

When determining the number of Service Monitors to deploy, the administrator should keep in mind the potential need for redundant and/or fallback applications.

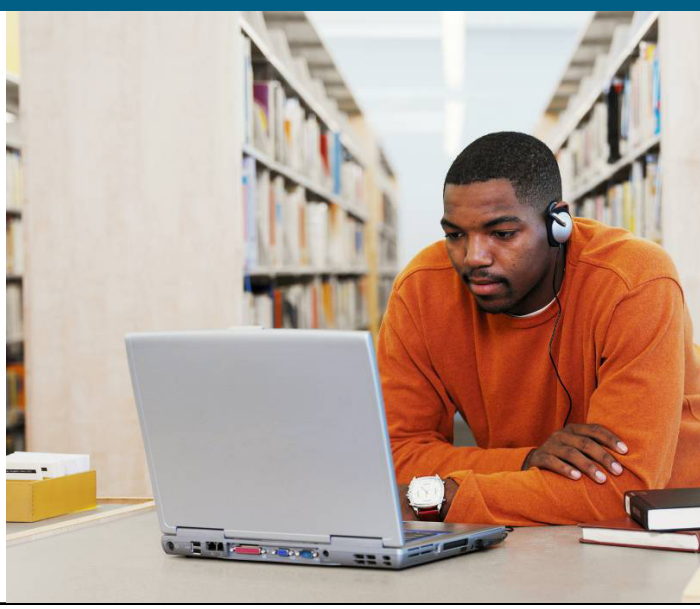
Each sensor forwards call quality metrics to the Service Monitor server every 60 seconds by sending a Syslog message. There is also a keep-alive between the two to ensure connectivity. If the sensor fails to receive the keep-alive message from the primary Service Monitor server, it will then register with a secondary Service Monitor server (if defined in its configuration) and begin sending call quality metrics to it. This design ensures that no threshold violations are missed.

Note(s):

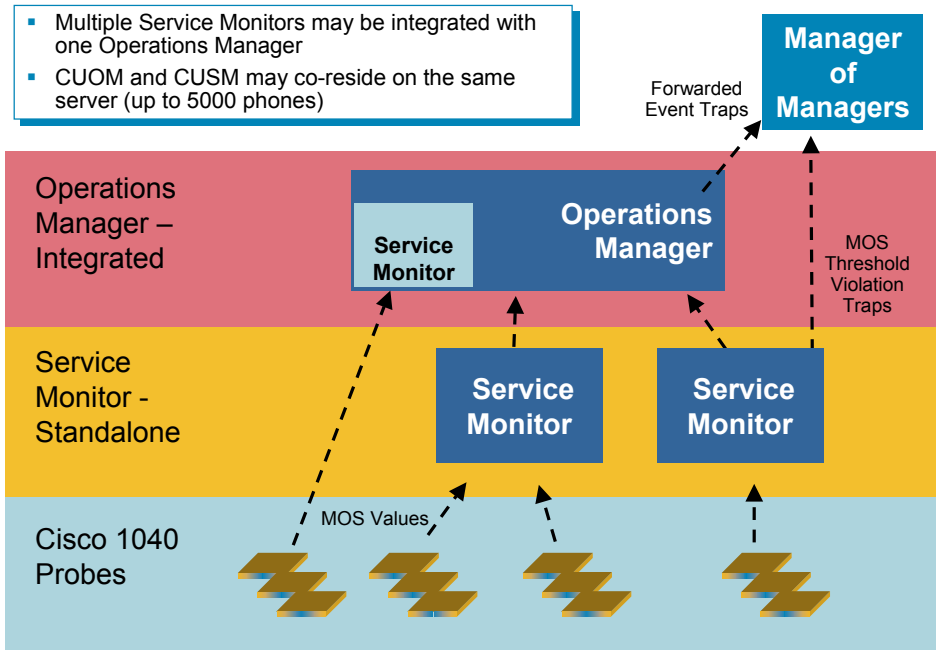
- Any redundant or fallback Service Monitor should also be the primary server for other Cisco 1040s.
- When considering that each Service Monitor can support up to 50 Cisco 1040s, this should include the Cisco 1040s that are defined for the primary and secondary servers.

Deployment Options

- Product Overview
- Functional Architecture
- **Deployment Options**



Service Monitor Deployment Options
Overview



Service Monitor Deployment Options

The products within the Cisco Unified Communications Management Suite (Cisco Unified Operations Manager and Cisco Unified Service Monitor)can be deployed on a single server or their own standalone server.

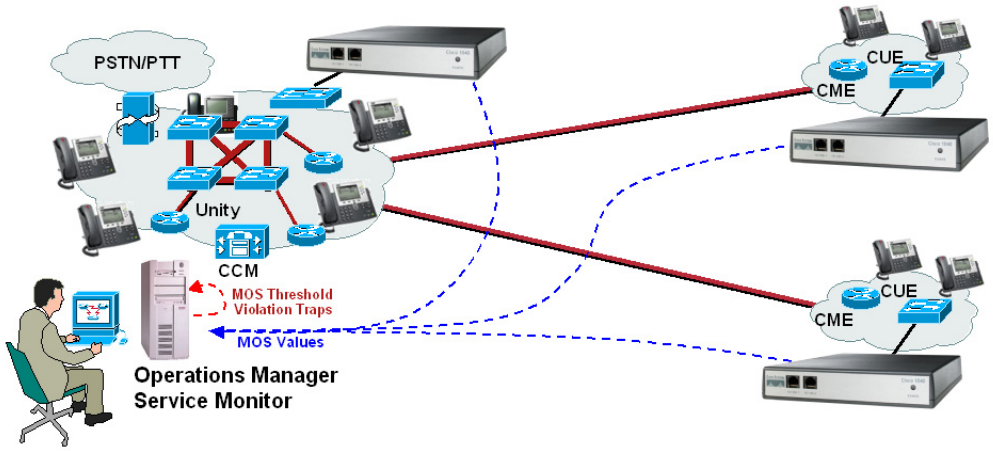
Since the data collected by the Service Monitor application is forwarded to Operations Manager for display, it makes sense to deploy them on the same server, if possible. In fact, when installing Operations Manager a copy of Service Monitor is also loaded on the server. Even though the two applications are on the same server they each still require their own license to operate.

Networks typically tend to be very geographically dispersed so it may not make sense to have all sensors reporting to the same instance of Service Monitor. In fact, Service Monitor is limited to supporting 50 Cisco 1040 sensors. Also, it may be advisable to include redundant copies of both applications in case of failure. The products of the management suite are scalable to many different possibilities in network size and deployment configurations.

The figure above shows a possible installation of the Unified Communications Management Suite. One server has a copy of both applications. Several Cisco 1040 sensors are reporting to this instance of Service Monitor. The deployment also has a second copy of Service Monitor on a stand-alone server (perhaps in a different region) with several Cisco 1040 sensors reporting to it. Both copies of Service Monitor are reporting their voice quality findings to the single copy of Operations Manager.

Both Service Monitor and Operations Manager can forward their findings to a third party network management system (NMS).

Service Monitor Deployment Options
Small and Medium Enterprise Deployments



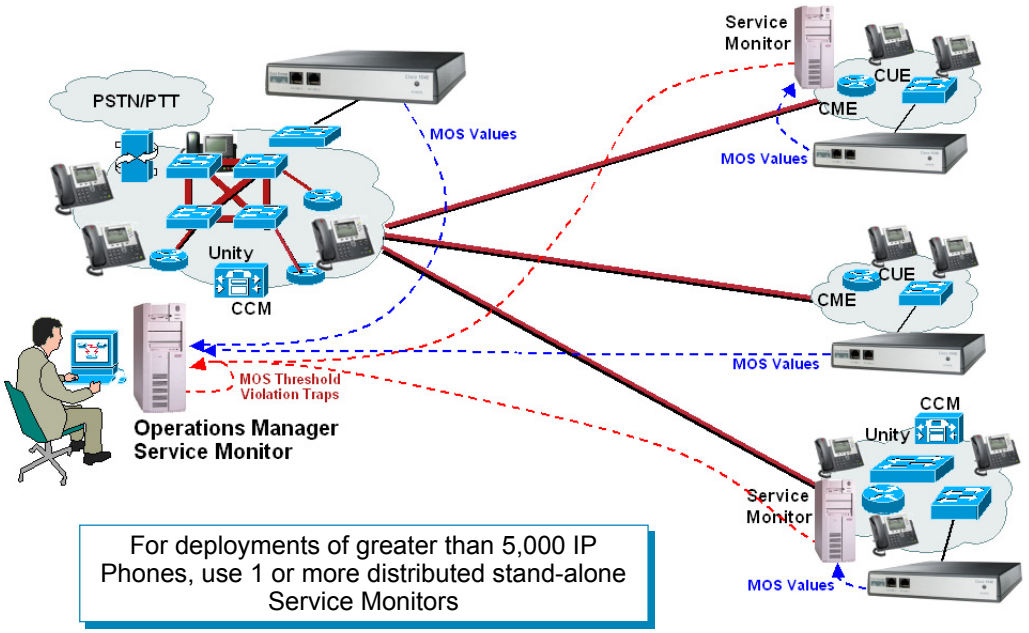
For deployments of less than 5,000 IP phones, Operations Manager and Service Monitor can reside on the same platform

Small and Medium Enterprise Deployments

In small to medium enterprises (generally less than 5,000 phones), it is generally possible to have Operations Manager and Service Monitor co-reside on the same platform. If necessary, as additional sensors are purchased and deployed, additional stand-alone SM instances can also be deployed.

Note: The sensors come separately packaged so that they can be shipped to their destination site without additional packing material.

Service Monitor Deployment Options
Large Enterprise Deployments



For deployments of greater than 5,000 IP Phones, use 1 or more distributed stand-alone Service Monitors

Large Enterprise Deployments

For larger enterprises (generally more than 5,000 phones), it is possible to have Operations Manager and Service Monitor co-reside on the same platform depending on the number of calls to be monitored, but a separate platform is recommended. Depending on the number of calls to be monitored, multiple instances of SM can be deployed and still all report to a single instance of Operations Manager or other trap receiver.

Each dedicated SM server can support up to 50 Cisco 1040s to provide a distributed, highly scalable, and redundant mechanism to analyze IP telephony voice quality.

A separate SM is not required at each remote branch location. The sensors' configuration file specifies the location of the primary and secondary SM servers

Service Monitor Deployment Options
Cisco 1040 Sensors and CVTQ

- Cisco 1040 sensors and CVTQ complement each other and bring total solution to voice quality measurement
- Cisco 1040 sensors provides real-time voice quality information for all voice calls monitored by sensors
- Cisco 1040 sensors have no restriction on the version of CallManager and end points
- Cisco 1040 sensors support CME/CUE environment as well as CCM/Unity
- CVTQ support provides customers the ability to monitor voice quality of all calls in the network with CallManager 4.2 or higher, 794X, 796X and 797X IP Phones
- In a CallManager 4.2 or higher environment, Cisco 1040 sensors can be used to monitor key Executive phones/Voicemail system/Gateway/Troubleshooting and CVTQ can be used to understand overall voice quality

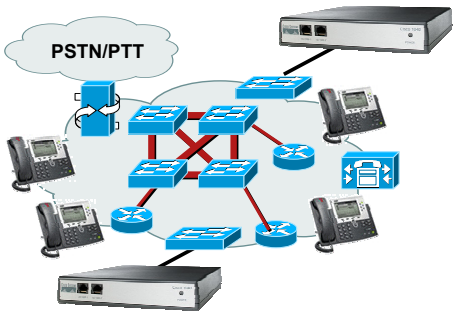
Service Monitor Deployment Options – Cisco 1040 Sensors & CVTQ

The Cisco 1040 sensors and CVTQ complement each other and bring a total solution to voice quality measurement. Here are some things to consider when using both in your monitoring solution.

MOS values are forwarded to the Service Monitor for voice quality evaluations by both the Cisco 1040 Sensors and by the Cisco Unified CallManagers. The Cisco 1040 Sensors calculate real-time a MOS value every 60 seconds for a monitored call stream. Cisco Unified CallManagers receive a MOS value for an entire call at the termination of a call. The MOS value for an entire call is calculated on gateways and phones using the Cisco Voice Transmission Quality (CVTQ) algorithm. Cisco Unified CallManager stores the data in Call Detail Records (CDRs) and Call Management Records (CMRs), which then forwards it to SM and then is evaluated against user-defined thresholds.

Service Monitor Deployment Options
Strategic/Tactical Monitoring

Strategic



- Install multiple probes in locations of high traffic and visibility
- Monitor RTP streams continuously and pick up the data records for analysis
- "Six-pack" package

Tactical

- On-demand troubleshooting of poor voice quality
- Probe can be shipped overnight to location where problems are happening
- Alerting can start within minutes of deployment
- "Two-pack" package

Strategic/Tactical Deployment

The key to successfully monitoring quality of voice in real-time is the placement of the Cisco 1040 sensors. There are two types of monitoring:

Strategic – This is the continuous sampling of RTP streams. Sensors should be placed based on monitoring goals of critical segments or phone banks. Typically, sensors are deployed in pairs since a sensor close to one end of the call would not see any appreciable call degradation; rather it is the far end that will see call degradation.

Tactical –One or more Cisco 1040 sensors can be used in an on-demand basis to troubleshoot spots not covered under strategic monitoring when experiencing poor quality of voice. The sensors can be inexpensively shipped overnight to a site, installed immediately, and begin to monitor and assess the quality of IP-based calls without elaborate setup or complicated installation issues

To help determine sensor placement, the administrator can take advantage of other Cisco tools they may have been deployed. If the *Call Detail Records* (CDR) option is enabled in *CallManager*, the administrator may be able to determine places in the network that have a history of poor quality of voice, and place sensors accordingly. Also, *Operations Manager* can be helpful in determining locations of phones, their switch connectivity, and their VLAN membership; thereby dictating a switch to be configured with a SPAN port (and connected to a sensor for monitoring), and which ports or VLANs to SPAN.

Thank You!

Continue on to Chapter 3 to use the many features of Service Monitor.

Cisco Systems

<*Intentionally Blank*>

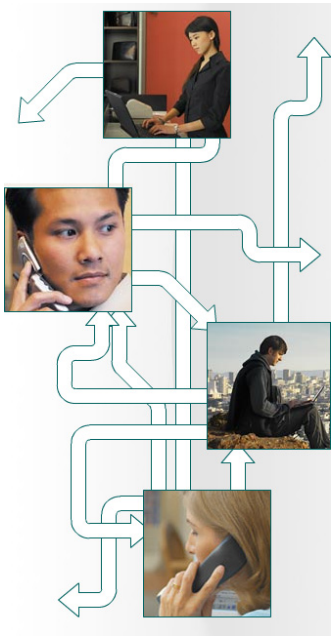
Cisco Unified Service Monitor

Usage Scenarios

Chapter 3

Chapter 3 Outline
Scenarios

1. Planning
2. Getting Started
3. Monitoring Active Calls

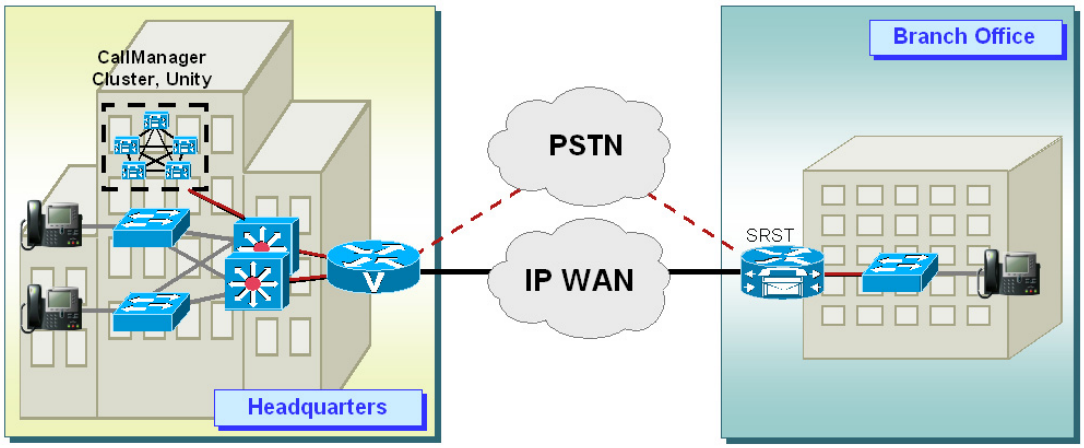


Chapter 3 – Service Monitor Scenarios

This chapter uses several scenarios to illustrate how to setup and use Cisco Unified Service Monitor (SM) to gain visibility into the quality of active calls.

In general, these scenarios will briefly look at the planning process to determine how to deploy Service Monitor for use with the Cisco 1040 Sensors and Cisco CallManagers (CVTQ), and then walk through the steps required to set them up. Finally, steps will be presented to show you how to view potential voice quality concerns of an active call, as well as, how to view the call metrics archive as a mechanism to help verify conformance to any Service Level Agreements (SLAs) in place.

Network Description for Scenarios
Company XYZ



Network Description – Company XYZ

To help you better understand of the setup and use of Service Monitor, the scenarios will follow the deployment of Service Monitor in a fictitious company – XYZ.

Company XYZ has recently adopted Cisco's strategy for converging voice, video, and data onto a single network infrastructure using the Cisco AVVID (Architecture for Voice, Video and Integrated Data). Company XYZ is also considering using several other CiscoWorks products (LAN Management Solution (LMS) and QoS Policy Manager (QPM)) to help ensure their network could both support voice and was properly configured for it.

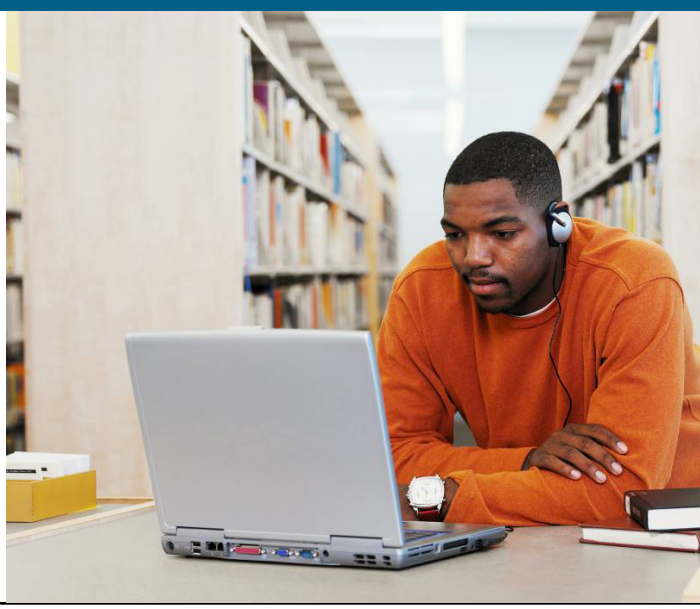
The best of planning does not always ensure that problems won't arise; therefore, Company XYZ wishes to protect their investment by monitoring the quality of voice calls to both detect potential problems and to ensure conformance to the voice SLAs negotiated with their provider.

Dean Jones, a lead network engineer for Company XYZ, has been tasked with the monitoring of active calls. Let's peek over Dean's shoulder as he goes about his assignment.

<Intentionally Left Blank>

Scenario 1: Planning

- **Planning**
- Getting Started
- Monitoring Active Calls



Planning
Use of Cisco 1040 and CVTQ

Requirements	SLA Verification (Combination of Cisco 1040 & CVTQ)	Real-Time Alerting (Cisco 1040 Sensors)
SM Function	Call Metrics Archiving	MOS Violation Trap Forwarding
Event Notification	Review Archive	SM forwards SNMP traps to OM or Enterprise NMS
Cisco 1040 Placement	Continuous - Near Phones on all segments regulated by SLA	Continuous – critical segments Strategic – place as needed
Numbers of Cisco 1040s	Based on Monitoring Requirements • Geographical • BHCC per switch	Based on Monitoring Requirements • Geographical • BHCC per switch
Instances of Service Monitor	• Max 10 Cisco 1040s per instance • Secondary or tertiary instance for fail over conditions	• Max 10 Cisco 1040s per instance • Secondary or tertiary instance for fail over conditions

- Applications like Operations Manager and/or CiscoWorks RME can be used to help locate phones
- Cisco 1040s must attach to switch that supports IEEE 802.3af Power over Ethernet (PoE)
- Use Cisco 1040 sensors with sites having Cisco CallManager Express (CME) in absence of CVTQ

Planning

Dean's first activity is to select the best tool to meet the monitoring requirements. Dean's task is to monitor active calls for both current quality issues, and conformance to SLAs. This is the exact problem set addressed by Cisco Unified Service Monitor.

Now that Dean has his tool of choice, he must still do his homework to determine how to best deploy it.

The requirements of Dean's task have a direct correlation to the configuration of Service Monitor – Dean will need to both look for current voice concerns (MOS violation threshold) and make sure he archives the call metrics for every call to help him determine if the SLAs are being met. Since Dean wants to see real-time quality concerns, the MOS violations must be forwarded to a trap receiver. Dean chooses Operations Manager as his trap receiver of choice since Company XYZ will also being deploying it for its rich set of Unified Communications management functionality. Dean will then later create his own spreadsheet program for analyzing the call metrics files generated by the archiving feature of Service Monitor.

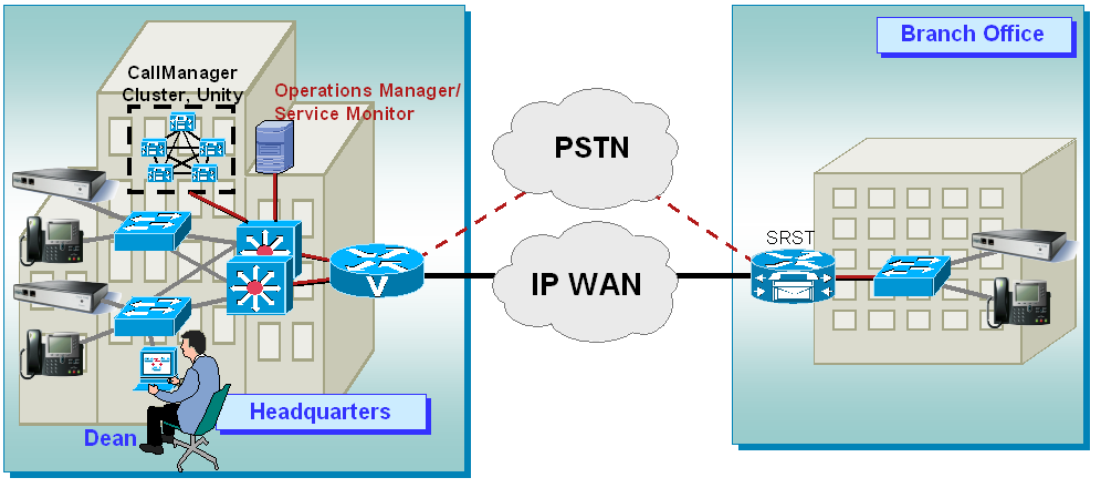
Perhaps the biggest issue in the planning of the Service Monitor deployment is how many, and where to put the Cisco 1040 sensors used for real-time monitoring. Dean has also chosen to use the CVTQ algorithm found in IP phones and some gateways, which will provide MOS values for the entire call. The CVTQ values are available from Dean's CallManagers, but he will need sensors at the CME sites, critical locations, and real-time troubleshooting. Many factors must be weighed including, but not limited to:

- Monitoring requirements (continuous or strategic)
- Busy hour call completion (BHCC) per switch (each 1040 can only monitor 80 RTP streams at one time)
- Budget

Dean must also take into account the fact that the Cisco 1040s get there power from the switch, therefore, the Cisco 1040s can only be connected to switches that support the IEEE 802.3af PoE standard (see note below). Further, the Cisco 1040s get the data for monitoring via a SPAN session configured on a switch; therefore, an available SPAN port must be available on the hosting switch. If the hosting switch does not support the IEEE 802.3af PoE standard, either purchase an additional daughter card for the switch if there is an available slot or upgrade the current card.

Finally, Dean must be cognizant of the fact that each instance of the Service Monitor software can support up to 10 Cisco 1040s. If more than 10 Cisco 1040s are to be deployed, multiple instances of SM must be deployed.

Planning
Deployment of Cisco 1040 Sensors



- Placement of Cisco 1040 sensors can support both SLA verification monitoring or Real-Time Alerting
- Place Cisco 1040 sensors near phones and in CME sites (absence of CVTQ)
- SPAN incoming traffic on phone ports to Cisco 1040 sensor
- Combination of real-time voice quality measurement using Cisco 1040 sensors with system-wide voice quality measurement using CVTQ (phone based) provides complete voice quality view

Deployment of Cisco 1040 Sensors

Currently, Company XYZ is a small firm and Dean will only need 3 Cisco 1040 sensors to give him complete coverage at the access layer. Two Cisco 1040 sensors will handle all the phones in the building at the corporate headquarters, and another Cisco 1040 sensor will be deployed to handle the phones at the remote branch facility.

Dean will use the Cisco 1040 Sensors for real-time monitoring and also use the CVTQ data stored in the Cisco CallManager for service quality reporting on completed calls.

Since the current deployment is small (less than a 1000 phones), Dean will have the Cisco Unified Operations Manager (OM) and Cisco Unified Service Monitor (SM), resident on the same Windows server. (Refer to Chapter 4 for server requirements.)

If the SM software is installed standalone, the directories for the sensor configuration and image files and the directory for the call metrics archives can be specified. However, in this scenario, SM and OM are co-resident; thus, Service Monitor defaults these directories to *$NMSROOT*/data/ProbeFiles and *$NMSROOT*/data/CallMetrics respectively.

Before actually connecting the Cisco 1040 sensors, Dean will first setup Service Monitor and use it to create the configuration files for the sensors and establish connections with the Cisco CallManager to obtain the CVTQ data.

Deployment of Cisco 1040 Sensors, (Cont.)

Note(s):

- This scenario provided a brief overlook at the planning for deployment of the Service Monitor product. Every situation is different and many factors that may not be addressed here can factor into the planning process. Also refer to Chapter 5 for a link to the *Service Monitor Deployment Guide*.
- It is recommended, if possible, to place the Cisco 1040 closest to the switches supporting IP phones. If budget concerns prevent this, the network administrator may try to create a separate network connected to the SPAN ports of multiple switches and a single Cisco 1040.
- Other CiscoWorks applications such as Operations Manager and LMS Resource Manager Essentials (RME) User Tracking can be used to determine the location of phones. Also, RME can be used to determine the hardware versions of switches to help determine if they meet the necessary requirements for Power over Ethernet (PoE).
- Placement of sensors in different locations can allow the network manager to monitor different portions of the network with respect to the enterprise or WAN. For instance, a sensor placed on the switch connected to the phones will provide overall voice quality for the incoming voice stream (It makes no sense in this type of deployment to monitor outgoing calls since they will not have degraded yet). A sensor placed near the demarcation point will provide quality of incoming calls with respect to the WAN or service provider portion of the network and the local network portion of the outgoing calls.

Planning
Server / Client Requirements

	SM Server Requirements *	Client Requirements
Processor	IBM PC-compatible system > 2 GHz	IBM PC-compatible system > 500 MHZ
Memory	2 GB	512 MB
Swap	4 GB	1 GB
Disk Space (NTFS Format)	20 GB Minimum	No application software installed
System Software	Windows Server 2003 Standard or Enterprise Edition	• Windows XP with SPK1 or 2 • Windows 2000/2003 Server or Professional with SPK3 or 4
Web Brower	Not required unless accessing Service Monitor from console	• Microsoft Internet Explorer 6.0.28 • Mozilla 1.75

* Having Operations Manager on same server would require additional server resources and is limited based on the number of IP Phones managed (refer to Operations Manager Tutorial.

* Windows Terminal Services is supported in Remote Administration mode only

SM Server / Client Requirements

The chart above details the sizing requirements for a stand-alone Cisco Unified Service Monitor server supporting up to 10 Cisco 1040 sensors. If Service Monitor is to reside on the same server as Cisco Unified Operations Manager, then additional resources will be required to support both applications.

The chart above also details the sizing requirements for a remote client workstation that will be used to access the Service Monitor application across the network. The Service Monitor application can also be accessed directly from the server if a web browser is installed on the server.

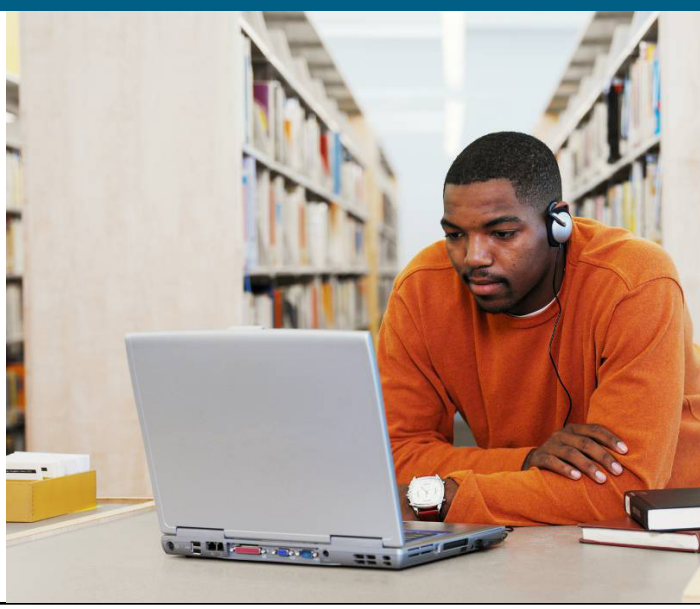
Additional configuration notes for the web browser are available in Chapter 4, System Administration, of this tutorial.

It is always a good idea to check the latest Release Notes for up-to-date information regarding system requirements.

<Intentionally Left Blank>

Scenario 2: Getting Started

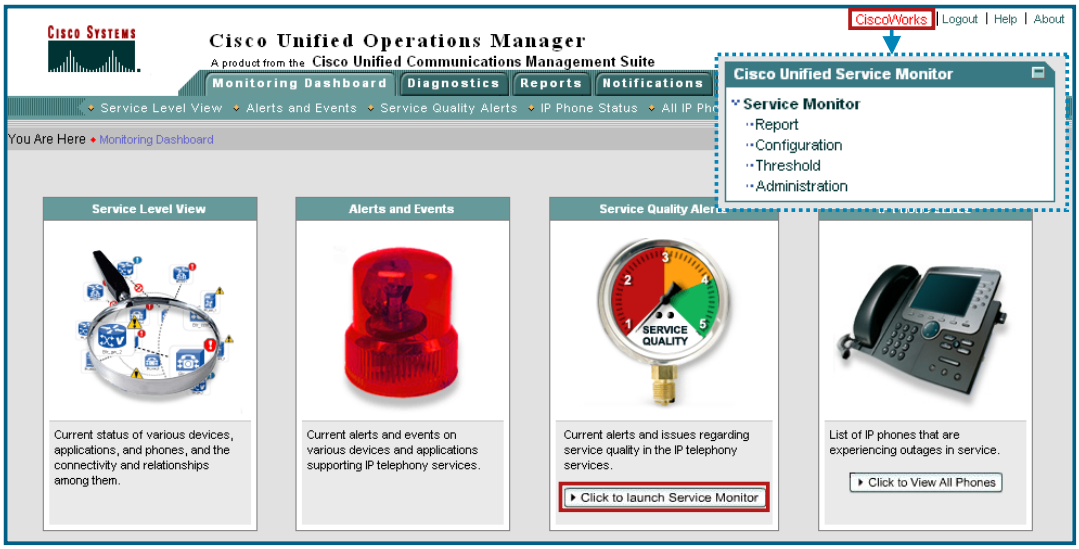
- Planning
- **Getting Started**
- Monitoring Active Calls



Getting Started – Workflow

Dean has outline various tasks associated with installing and configuring the Service Monitor application, Cisco 1040 sensors, and the Cisco CallManagers. These tasks are illustrated above and the rest of this scenario follows this workflow. Therefore, each of these tasks will be discussed in this scenario.

Getting Started
Launch Point for Service Monitor



Getting Started – Launch Point for Service Monitor

Service Monitor is a component application of the Cisco Unified Communications management suite and thus like Operations Manager also makes use of service provided by Common Services. In fact, a copy of Service Monitor is installed on the same server as Operations Manager during the install procedure, making access to Service Monitor readily available.

One way to access Service Monitor from Operations Manager use the following steps:

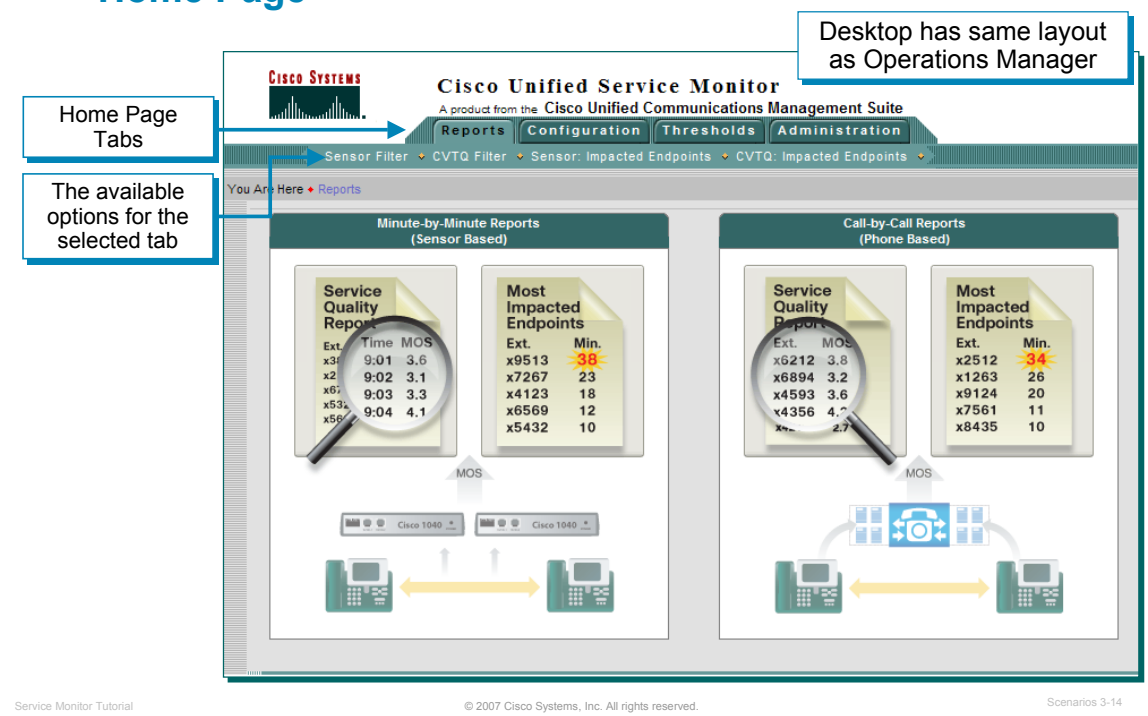
- From the Operations Manager Monitoring Dashboard desktop, click the **Click to Launch Service Monitor** button near the Service Quality Alerts icon.

Another way to access Service Monitor from Operations Manager use the following steps:

- From The Operations Manager desktop click the **CiscoWorks** link in the upper right-hand corner. The CiscoWorks homepage will display in a new window.
- The homepage displays all applications on the server registered to Common Services. Click on the **Cisco Unified Service Monitor** heading or expand the Service Monitor element and click on Service Monitor to launch the Service Monitor desktop.

Note(s):

- Service Monitor use requires a separate license
- If Service Monitor is a stand-alone copy, then enter http://<SM DNS or IP Address>:1741, login and you will be directed to the Service Monitor desktop.



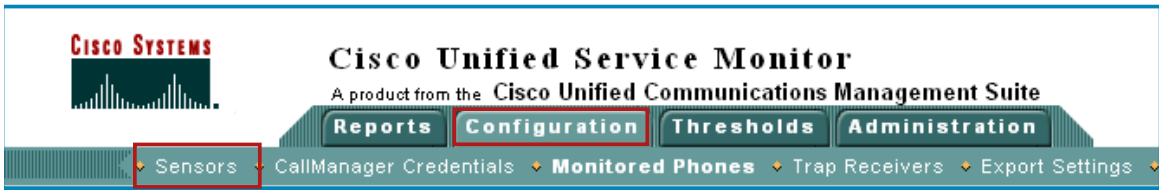
Getting Started – Home Page

The Service Monitor desktop shares the same layout and navigation as Operations Manager. In fact, all Cisco management applications, which use Common Services, employ this desktop layout.

The Service Monitor desktop is straightforward. It contains several main tabs or tasks categories:

- Reports
- Configuration
- Thresholds
- Administration

Working with Cisco 1040s
Overview



- Setup sensors with the following settings:
  - Enable and disable the archival of call-metrics (syslog)
  - Configure global primary and secondary Service Monitors
  - Configure the name of the global sensor image file
  - Configure trap throttling - This is done by suppressing traps for a configurable number of minutes, per endpoint.
- Configure the TFTP server IP addresses to push sensor images and configuration files
- Define new sensors, and edit/ reset registered sensors managed by this Service Monitor

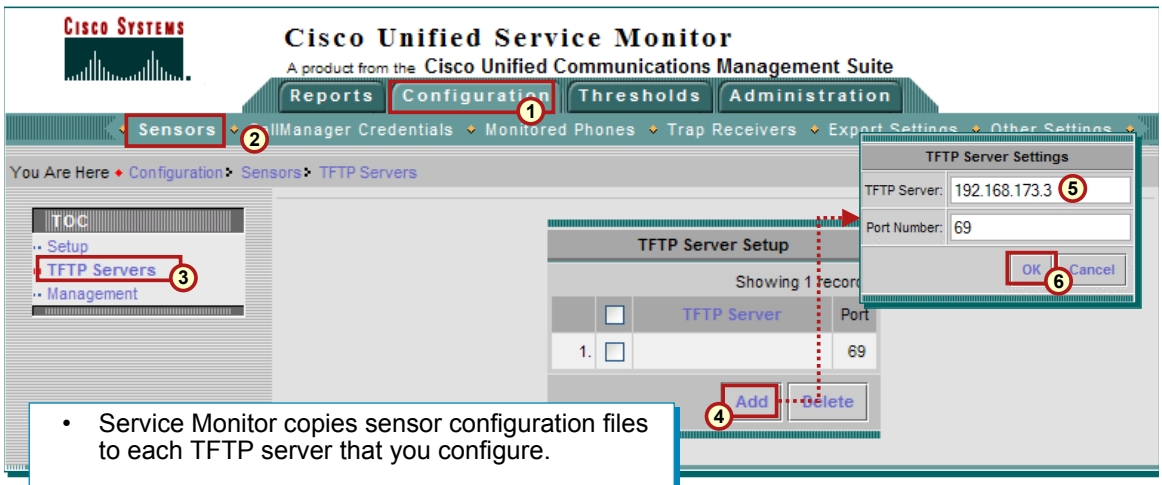
Working with Cisco 1040s – Overview

The Service Monitor software component only has a few tasks from the **Configuration>Sensors** tab: Setup, TFTP Servers, and Management.

So, the first place Dean starts when setting up his Cisco 1040 sensors is the **Configuration> Sensors** tabs. This is where Dean can perform the following tasks:

- Setup sensors with the following settings:
  - Default for specific configuration file
  - Enable and disable the archival of call-metrics (syslog)
  - Configure global primary and secondary Service Monitors
  - Configure the name of the global sensor image file
  - Configure trap throttling - This is done by suppressing traps for a configurable number of minutes, per endpoint.
- Configure the TFTP server IP addresses to push sensor images and configuration files
- Define new sensors, and edit/ reset registered sensors managed by this Service Monitor

Working with Cisco 1040s
TFTP Server



- Service Monitor copies sensor configuration files to each TFTP server that you configure.
- When a sensor connects to the network, it downloads a configuration file from a TFTP server before registering to a Service Monitor.

Working with Cisco 1040s – TFTP Server

Dean first defines his TFTP server. Service Monitor uses one or more TFTP servers to provide configuration files and binary image files for sensors. Dean must define at least one TFTP server for Service Monitor to use. He can configure additional TFTP servers either as backup or if he has more than one DHCP scope. Like IP Phones, Cisco 1040 sensors require the use of a TFTP server. Let's look at why.

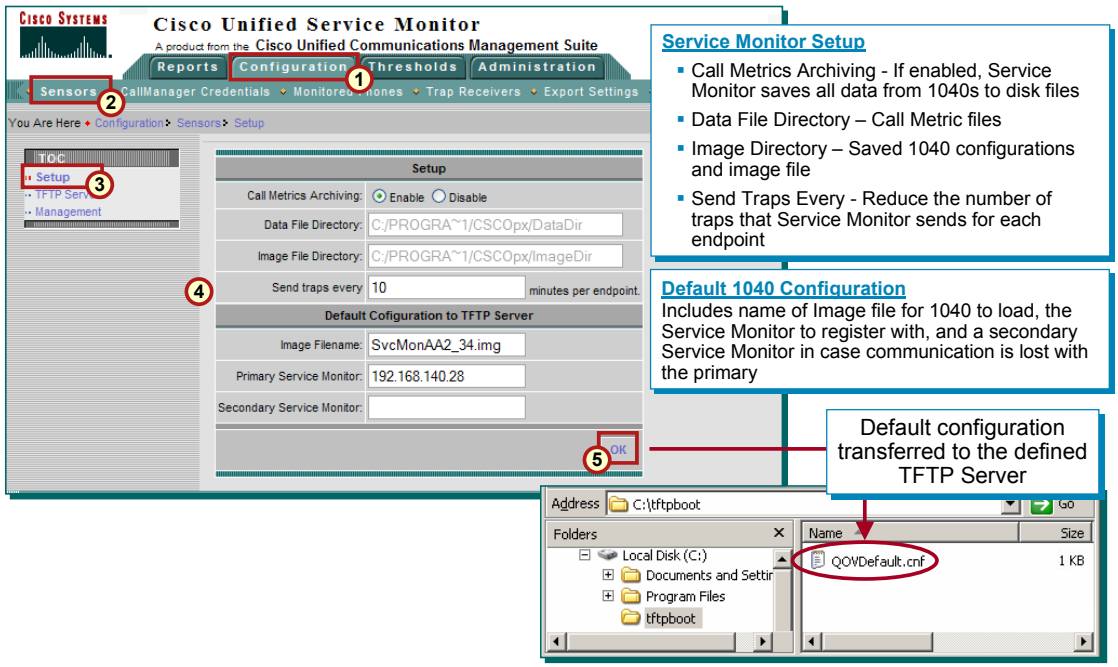
The Cisco 1040s act like IP phones in that they request both their image and configuration files from a TFTP server. This means that all 1040 configuration and image files must be copied from the Service Monitor server to the TFTP server prior to bringing any 1040 on-line.

Service Monitor automatically copies the configuration files to the specified TFTP server. After Dean adds or edits a sensor, Service Monitor updates the configuration file locally, on its server, before copying the configuration file to all known TFTP servers. Keeping copies of the configuration files on each TFTP server enables sensors to fail over efficiently to a secondary Service Monitor. Dean can use the configuration files that Service Monitor keeps on the server to recover if there is a write failure on the TFTP server. In this case, he can manually copy configuration files from Service Monitor to each TFTP server that is configured for Service Monitor.

The image file, however, must be manually copied to the TFTP server (described later in this scenario).

Dean, clicks the **Configuration> Sensors > TFTP Servers** task; then clicks **Add** to define the IP address and port for the TFTP server.

Working with Cisco 1040
Creating Default 1040 Configuration



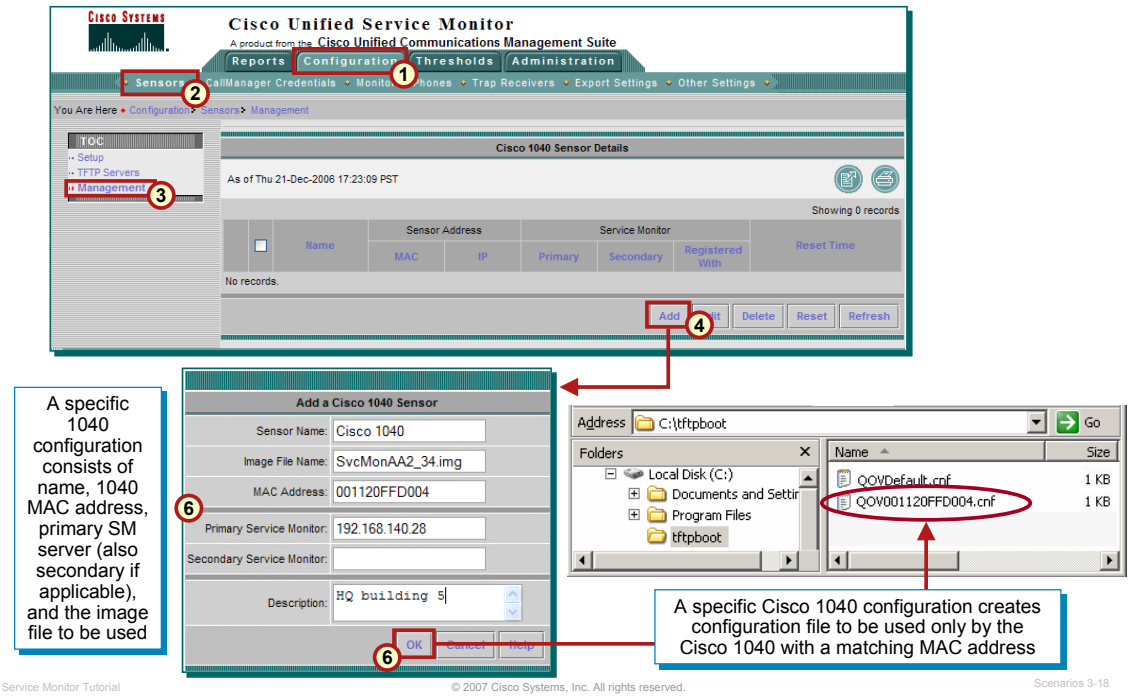
Working with Cisco 1040s – Creating Default 1040 Configuration

The Setup task allows Dean to configure whether the Cisco 1040s will use the default configuration (automatic registration) or must be individually configured in order to register with Service Monitor. The setup task is also used to enable Call Metric archiving, to set the MOS threshold, and to configure the trap receivers that MOS violations will be forwarded to.

Let's look at how Dean creates the default configuration file for the Cisco 1040s.

1. When a Cisco 1040 boots up, it first looks for a specific configuration for itself (based on MAC address) and if one is not available, it uses the default configuration. So let's create the default configuration that can be used by any sensor.
2. Select the **Configuration** tab, the **Sensors** option, and **Setup** from the TOC. The Setup dialog is displayed. Enter the following settings:
   - IP address of the Service Monitor server (where the Cisco 1040 sends MOS values to); Optionally, if so deployed, the IP address of a secondary SM server can be added to the default configuration for fail over operations.
   - Image directory location and name of the 1040 binary image
   - Call Metrics Archiving - If enabled, Service Monitor saves all data from 1040s to files
   - Data directory location for Call Metrics data
   - SNMP trap transmission frequency
3. When the **OK** button is clicked, Service Monitor generates the default configuration and places it in the TFTP server's directory selected during installation (listed by the Setup task). The file has the filename of QOVDefault.cnf.

Working with Cisco 1040s
Creating a Configuration for Specific 1040



Working with Cisco 1040s – Creating a Specific 1040 Configuration

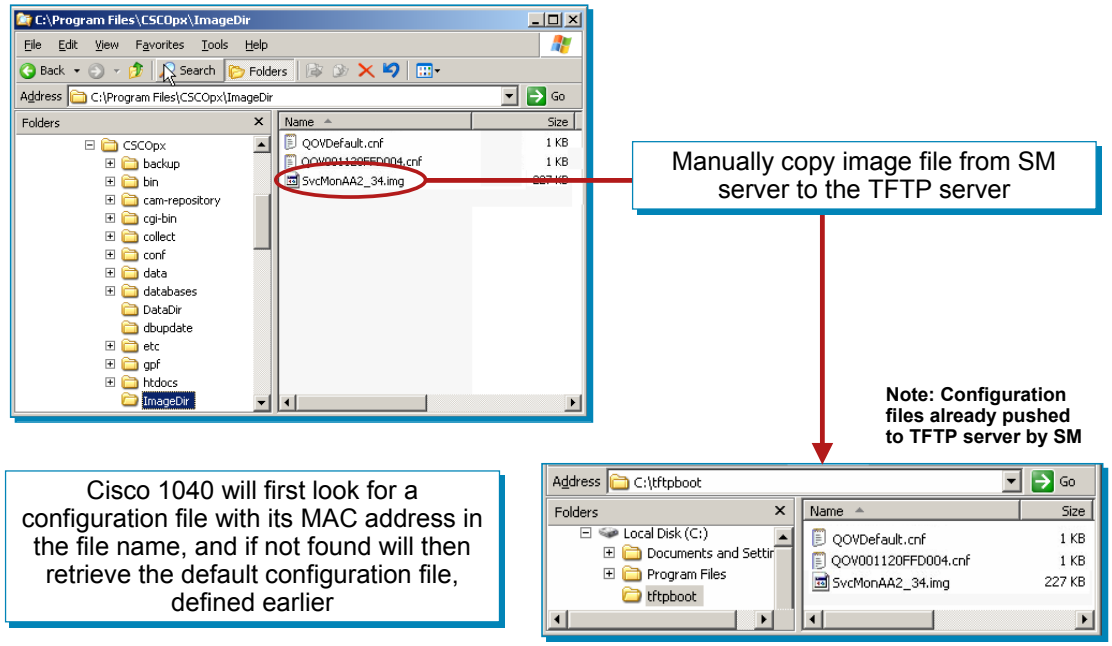
Dean can also create specific configuration files for each individual Cisco 1040. Configuration files contain the image to use and the address of the Service Monitor server, which will receive its MOS values. Dean can also configure and define a secondary Service Monitor server in case the primary server fails.

Dean uses the Management task manage the Cisco 1040s and configure these features. This task can then be used to verify that the configured Cisco 1040s have registered with Service Monitor.

Dean uses the following steps to create a manual configuration file for a specific Cisco 1040 sensor.

1. Select the **Configuration** tab, the **Sensors** option, and **Management** from the TOC.
2. The *Cisco 1040 Details* dialog is displayed showing a list of any previously defined or registered Cisco 1040s. Select **Add** to create a specific configuration for a Cisco 1040.
3. The *Add a Cisco 1040* dialog is displayed. Like the default config setup, enter both the IP address of the Service Monitor server and the name of the image file that the sensor will use. For this specific 1040 configuration, Dean must enter the MAC address of the sensor. This is how a sensor will determine that the configuration is for it. If so deployed, a secondary SM server can also be added.
4. When the **OK** button is clicked, Service Monitor generates the specific configuration and places it in the TFTP server's directory defined during installation (listed by the Setup task). The file has the filename of QOV<*1040_mac_address*>.cnf.

Working with Cisco 1040s
Copy 1040 Image File to TFTP Server

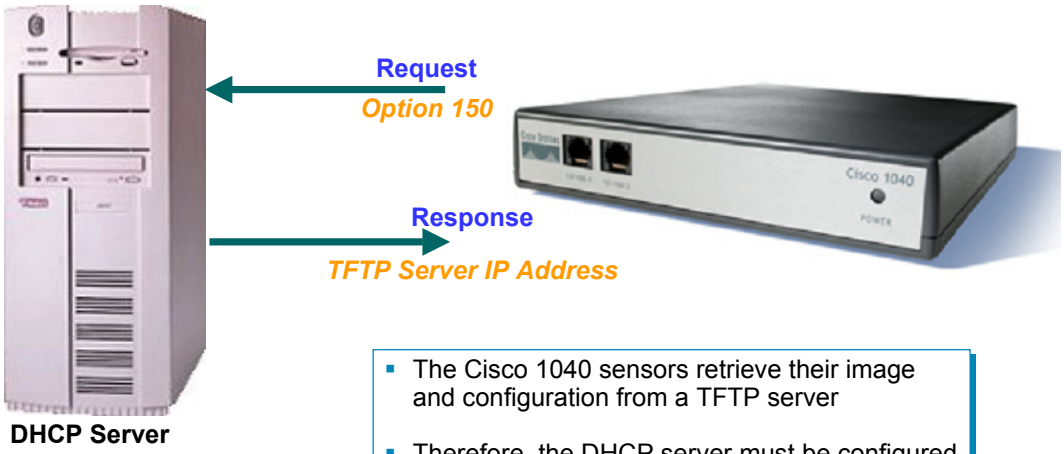


Working with Cisco 1040s – Copy 1040 Image File to TFTP Server

The Cisco 1040s act like IP phones in that they request both their image and configuration files from a TFTP server. This means that all 1040 configuration and image files must be copied from the Service Monitor server to the TFTP server prior to bringing any 1040 on-line.

Service Monitor automatically copies the configuration files to the specified TFTP server. The image file, however, must be manually copied to the TFTP server.

Working with Cisco 1040s
Configure DHCP Server



- The Cisco 1040 sensors retrieve their image and configuration from a TFTP server
- Therefore, the DHCP server must be configured to supply the TFTP IP address (defined in SM) to the Cisco 1040

Working with Cisco 1040s – Configure DHCP Server

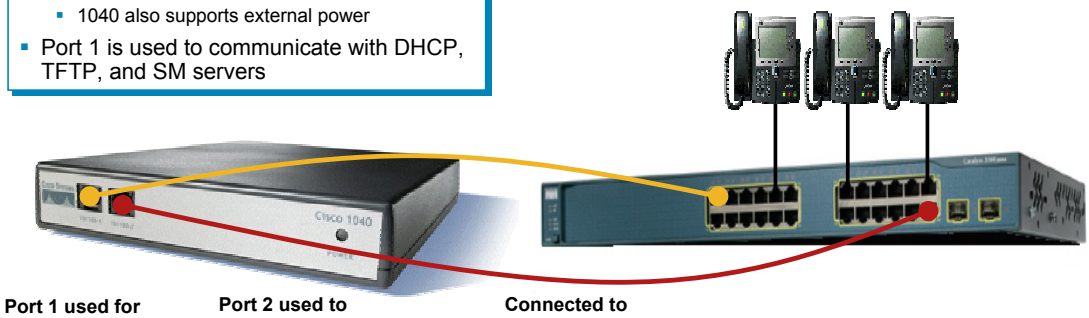
The Cisco 1040 sensors will pull their image and configuration files from the TFTP server, but how do they know which TFTP server has these files for download?

During the boot process, the Cisco 1040 will receive all typical IP communication parameters from the DHCP server. The sensor will also issue an “option 150” request.

Dean must configure the DHCP server to respond to this request and provide the IP address of the TFTP server where the configuration and image files resides.

Working with Cisco 1040s
Install - Connecting Sensor to a Switch

- Cisco 1040 receives power on Port 1 from switch (IEEE 802.3af PoE)
  - 1040 also supports external power
- Port 1 is used to communicate with DHCP, TFTP, and SM servers



Port 1 used for management

Port 2 used to monitor RTP streams

Connected to SPAN port on switch

- Configure switch to copy (SPAN or RSPAN) packets from a VLAN or specified ports that contain voice traffic to a specified port for detailed analysis
- Cisco 1040 (Port 2) is connected to the specified SPAN port and monitors RTP call streams

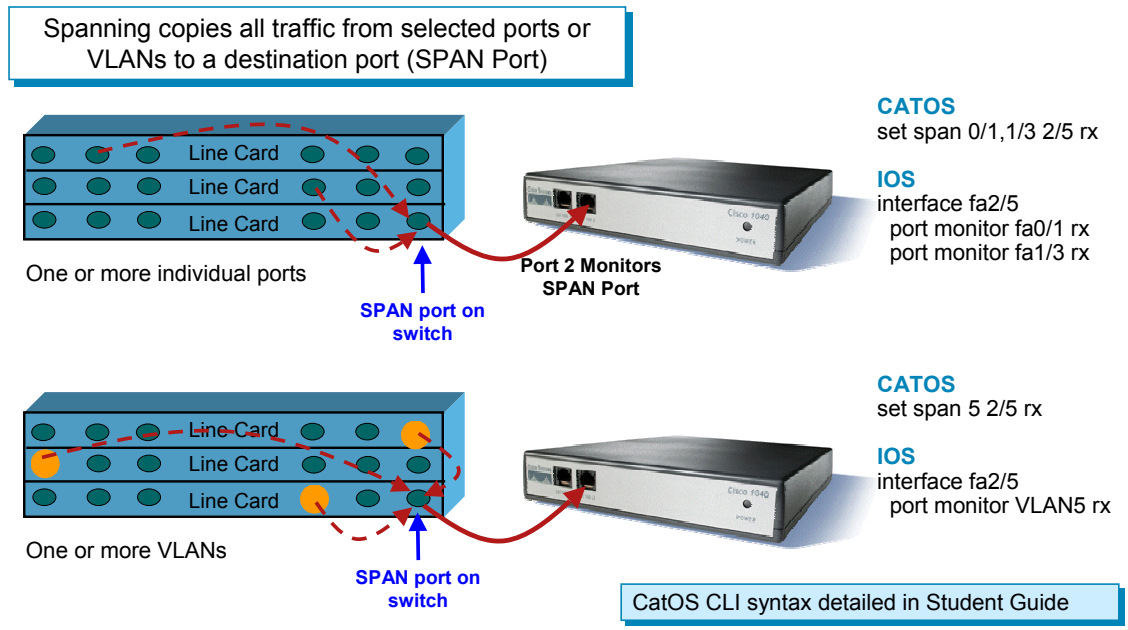
Working with Cisco 1040s – Install – Connecting Sensor to a Switch

Dean must now connect the Cisco 1040 to the network monitor its boot process.

Dean has verified that all configuration and image files have been placed on the TFTP server, each Cisco 1040 can be connected to the network. As soon as it is connected to a switch supporting IEEE 802.3af PoE, the sensor powers up and begin its boot cycle, which includes retrieving its image and configuration from the TFTP server.

Each Cisco 1040 has two Ethernet 10/100 ports. Dean must connect BOTH.

- Port 1 is used for communication with the servers (DHCP, TFTP, and Service Monitor) and is also the port used to receive power from the switch.
- Port 2 is used for monitoring call streams. Typically it is connected to a SPAN port on a switch.



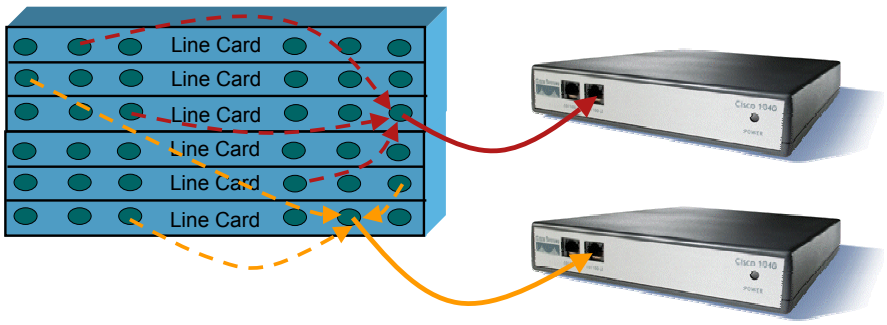
Working with Cisco 1040s – Install – Configuring Switch SPAN Port

SPAN (Switch Port Analyzer) ports are used to mirror traffic from ports in order to allow for some form of analysis. Because the Cisco 1040 analysis is performed on RTP voice streams, Dean needs to mirror the traffic from ports containing this type of traffic to the SPAN port connected to the Cisco 1040. SPAN allows Dean to forward one or more ports or VLANs to the SPAN port and can even specify the direction (Rx/TX/Both).

Note(s):

- Dean must be carefully when using SPAN that they do not send more traffic than the SPAN port speed can handle.
- Typically, only SPAN the TX direction since the received direction is from the local phone and the short hop will not have experienced any call degradation.
- The administrator can also use the RSPAN feature (Remote SPAN) to SPAN traffic from remote switches to the switch configured with the SPAN port, however, they must be cognizant of the additional traffic that is put on the various interconnection links.
- Spanning voice traffic from multiple switches to ports connected to a hub and a sensor is one way to limited the number of sensors needed and keep analysis traffic off the production network.
- SPAN command syntax varies depending on the device type and OS in use. For additional details about the SPAN command see the appropriate documentation for your device and OS.

Working with Cisco 1040s
Install - Alternative SPAN Configurations



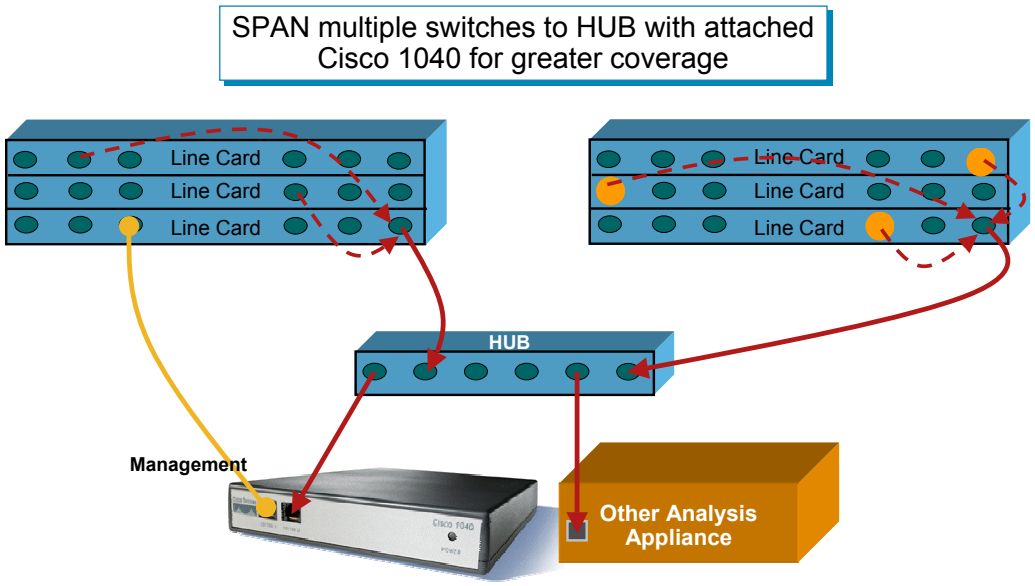
For large switches, with a BHCC exceeding the capacity of one Cisco 1040, use multiple SPAN ports and Cisco 1040s

Working with Cisco 1040s – Install – Alternative SPAN Configurations

In the case of large switches with many phones, and a Busy Hour Call Completions (BHCC) exceeding the capability of a single Cisco 1040 (100 active RTP streams per minute), Dean could configure the switch with more than one SPAN port and attach a Cisco 1040 sensor to each configured SPAN port.

Each call is potentially two RTP streams (one in each direction). Typically, you only want to monitor the incoming (from the remote end) direction of the call, since the local or outgoing stream will more than likely not have had any time to degrade.

Working with Cisco 1040s
Install - Alternative SPAN Configurations



Working with Cisco 1040s - Install – Alternative SPAN Configurations

In the case of an environment having many small switches with low BHCC, Dean may opt to connect a SPAN port on each switch to a hub where a Cisco 1040 is connected. This both saves money, and allows Dean to use a single Cisco 1040 to its fullest potential. This connection strategy would also allow for an additional network analysis appliance (i.e. Sniffer) to monitor the same voice streams.

Working with Cisco 1040s
Install - Boot Process

Boot Sequence

1. Initial State (status light – Solid Orange)
2. Obtained power from switch. Requests communication information from DHCP server (IP Address, netmask, default gateway, and TFTP server address) (status light – Flashing Yellow)
3. Access TFTP server and first asks for specific configuration file (QOV<1040_mac_ address>.cnf. If not available retrieves default configuration file (QOVDefault). (status light - Flashing Yellow)
4. Configuration file retrieved has name of image file. Cisco 1040 retrieves image file from TFTP server and completes boot process (status light - Flashing Yellow)
5. Registers with Service Monitor (status light - Solid Yellow)
6. Successful registration to primary SM (status light –Solid Green). Successful registration to secondary SM (status light - Flashing Green)

Cisco 1040 gets TFTP server IP address from DHCP server (DHCP option 150)

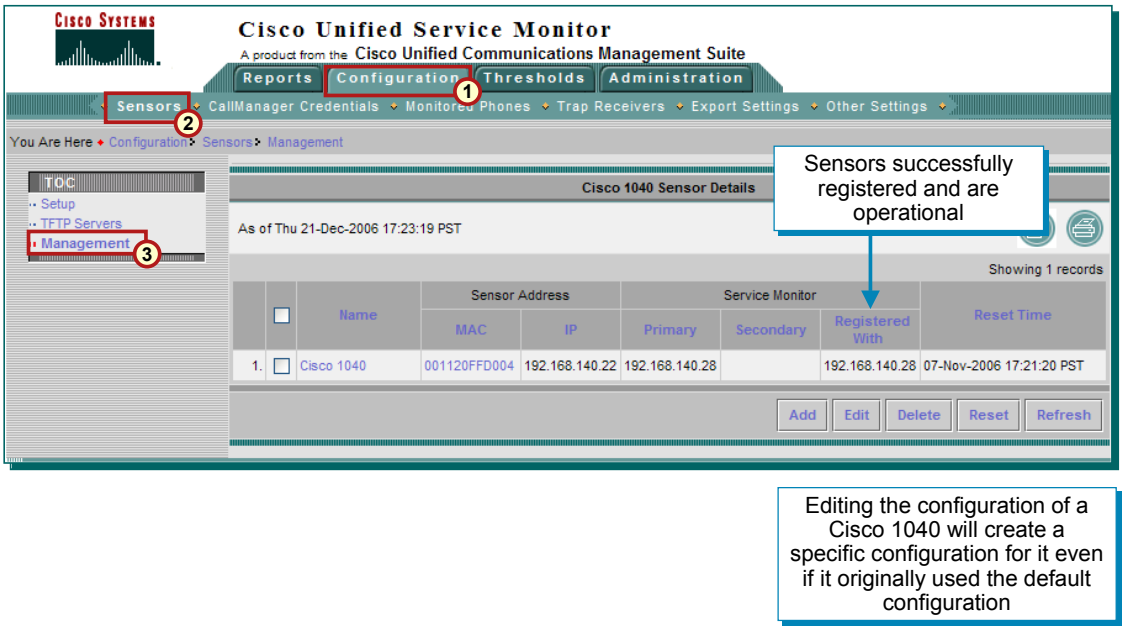
Cisco 1040 gets configuration and binary image from TFTP server

Working with Cisco 1040s - Install

Dean monitors the Cisco 1040 boot process.

- Once Port 1 is connected to a switch port, the Cisco 1040 receives power and begins its boot process. Like many network devices, the Cisco 1040 first sends out a DHCP request to get its IP communication parameters. The Cisco 1040 will then send an option 150 request to the DHCP server and in return will receive the IP address for the TFTP server hosting its image and configuration files.
- Next, the Cisco 1040 contacts the TFTP server and attempts to pull a specific configuration by requesting file QOV<*1040_MAC_address*>.cnf. If this fails, the Cisco 1040 next tries to retrieve the default configuration by asking for file QOVDefault.cnf.
- Once the configuration file is retrieved, the Cisco 1040 looks in the configuration file to get the name of the image it is to use, and then pulls it from the TFTP server. Once received, the Cisco 1040 loads the image.
- During the above procedures, the status light on the Cisco 1040 is a flashing amber color.
- Once the image is loaded, the Cisco 1040 looks in the configuration file for the IP address of the primary Service Monitor server and attempts to register with it. (If not available, the Cisco 1040 will try to register with the secondary server; if the registration process fails, the boot process starts all over again). During the registration process, the status light is a solid yellow color.
- When registration is completed, the status light will be a green color. If registration was successful to the primary SM server, the status light will be a solid green color. The status light will be a flashing green color, if registration was successful to an alternative SM server, the secondary server.

Working with Cisco 1040s
Verify Registration with Service Monitor



Working with Cisco 1040s – Verify Registration with Service Monitor

Dean now needs to verify that the Cisco 1040 sensor(s) properly registered with the Service Monitor server specified in their configuration and are ready to begin monitoring active calls for quality of voice

Dean checks with the Service Monitor server to make sure the Cisco 1040s are registered correctly and sets the time on them to ensure consistent time-stamping for the reported MOS values.

Dean uses the **Configuration> Sensors> Management** task to see a list of the 1040s that are reporting to this Service Monitor and their current status. As can be seen in the figure above, all three Cisco 1040s have properly registered with SM.

Note that the status field could also be **Failover** (if this Service Monitor was the secondary server for a Cisco 1040) or Unregistered if the Cisco 1040 was no longer communicating with this Service Monitor (perhaps if failed over to a secondary server).

Dean can also use Cisco 1040 Management dialog to edit/ view configurations and reset or delete a 1040.

Working with Cisco Unified CallManagers
Overview

Necessary to configure CallManagers, in order for Service Monitor to receive voice quality data.

- CallManager Service Parameters
  - CDR Enable flag to True
  - Call Diagnostics Enabled to True
- CallManager Enterprise Parameters
  - CDR File Time Interval (min) - Set to 1
  - CDR Format (CM 3.3 and CM 4.x) - Select CDRs will be inserted into database
- CM 3.3 and CM 4.x
  - Enable Mixed Authentication on SQL Server
  - Create SQL User
  - Service Monitor pulls the data from the CallManager Call Detail Record (CDR)/Call Management Record (CMR) tables
- CM 5.x
  - Create Billing Server, add Service Monitor
  - CallManager pushes the CDR/CMR records to Service Monitor
  - There can be a maximum of 3 Billing Servers for 5.x CallManager

Working with Cisco Unified CallManagers

In order for Service Monitor to receive voice quality data from the Cisco Unified CallManagers, Dean needs to make a few configuration changes to them, as indicated here.

CallManager Service Parameters

- CDR Enable flag to True
- Call Diagnostics Enabled to True

CallManager Enterprise Parameters

- CDR File Time Interval (min) - Set to 1
- CDR Format (CM 3.3 and CM 4.x) - Select CDRs will be inserted into database
- CM 3.3 and CM 4.x
- Enable Mixed Authentication on SQL Server
- Create SQL User
- Service Monitor pulls the data from the CallManager Call Detail Record (CDR)/Call Management Record (CMR) tables

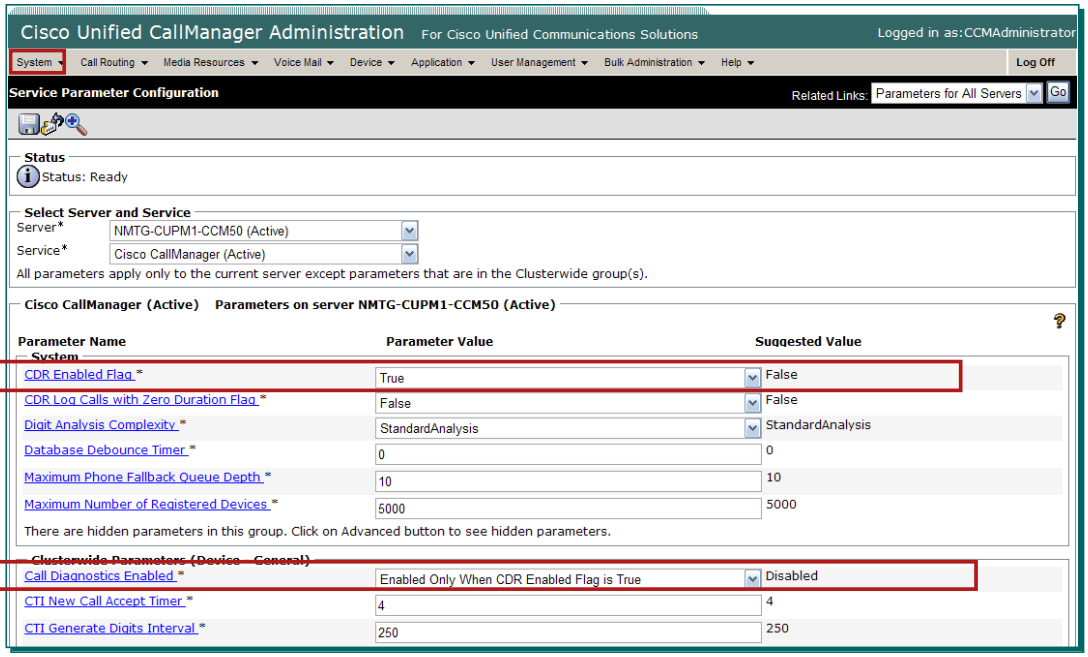
CM 5.x

- Create Billing Server, add Service Monitor
- CallManager pushes the CDR/CMR records to Service Monitor
- There can be a maximum of 3 Billing Servers for 5.x CallManager

CCM3.3/CCM4.1

- Needs to be configured even though it doesn't support CVTQ
- SM collects CCM3.3 /CCM4.x/CCM5.x CDR/CMR to populate the fields for Sensor Reports.

Working with Cisco Unified CallManagers
Service Parameters (CM 5.x Example)

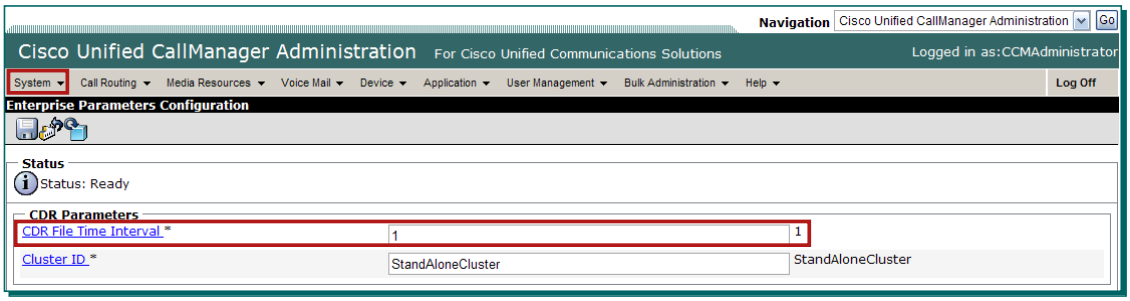


Working with Cisco Unified CallManagers – Service Parameters

Here's an example of how to set the Service Parameters on a Cisco Unified CallManager v5.x. Set these parameters on each Cisco Unified CallManager in a cluster.

1. Log in to Cisco Unified CallManager Administration utility.
2. Go to the Service Parameters Configuration page as follows:
   - For Cisco Unified CallManager 3.3 and 4.x, select **Service > Service Parameters**.
   - For Cisco Unified CallManager 5.x, select **System > Service Parameters**.
3. From the Service Parameters Configuration page, select the server and the service:
   - Select the name of the Cisco Unified CallManager server. This is a Cisco Unified CallManager from which Service Monitor will gather data.
   - Select the Cisco CallManager service.
4. Set these parameters for Cisco Unified CallManager versions 3.3.x and 4.x:
   - **CDR Enabled Flag**--Scroll down to System. Set to True.
   - **Call Diagnostics Enabled**--Scroll down to Clusterwide Parameters (Device - General). Set to True.
5. Set these parameters for Cisco Unified CallManager 5.x:
   - **CDR Enabled Flag**--Scroll down to System. Set to True.
   - **Call Diagnostics Enabled**--Scroll down to Clusterwide Parameters (Device - General). Set to Enable Only When CDR Enabled Flag is True.
6. Click Update.

Working with Cisco Unified CallManagers
Enterprise Parameters (CM 5.x Example)

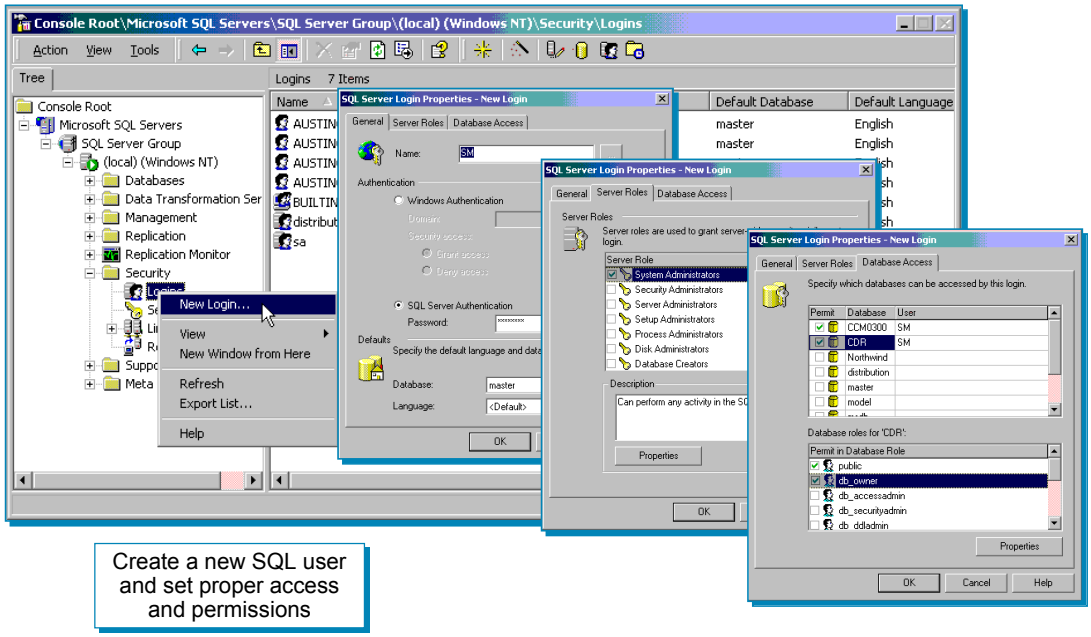


Working with Cisco Unified CallManagers – Enterprise Parameters

Perform this procedure for Cisco Unified CallManager versions 3.3, 4.x, and 5.x.

1. Log in to Cisco Unified CallManager Administration utility.
2. Select **System > Enterprise Parameters**. The Enterprise Parameters Configuration page appears.
3. Scroll down to **CDR Parameters** and set these parameters:
4. For Cisco Unified CallManager 3.3 and 4.x:
    - **CDR File Time Interval (min)**--Set to 1.
    - **CDR Format--**Select CDRs will be inserted into database.
5. For Cisco Unified CallManager 5.x:
    - **CDR File Time Interval (min)**—Set to 1.
6. Click **Update**.

Working with Cisco Unified CallManagers
CCM 4.x – Creating SQL User Example



Create a new SQL user and set proper access and permissions

Working with Cisco Unified CallManagers – Create SQL User

Service Monitor needs a Microsoft SQLServer user account to access local databases on the system with Cisco Unified CallManager. Use this procedure to add user accounts on any of these Cisco Unified CallManager versions:

- 4.x--Add an account to enable Service Monitor to access the CDR database.
- 3.3.x--Add an account to enable Service Monitor to access the CDR database and the device database, named CCM030n; for example, CCM0300. Alternatively, add two accounts: one for the CDR database and another for the CCM030*n* database.

Here is how to create an SQL user account, using CCM v4.x as an illustrated example.

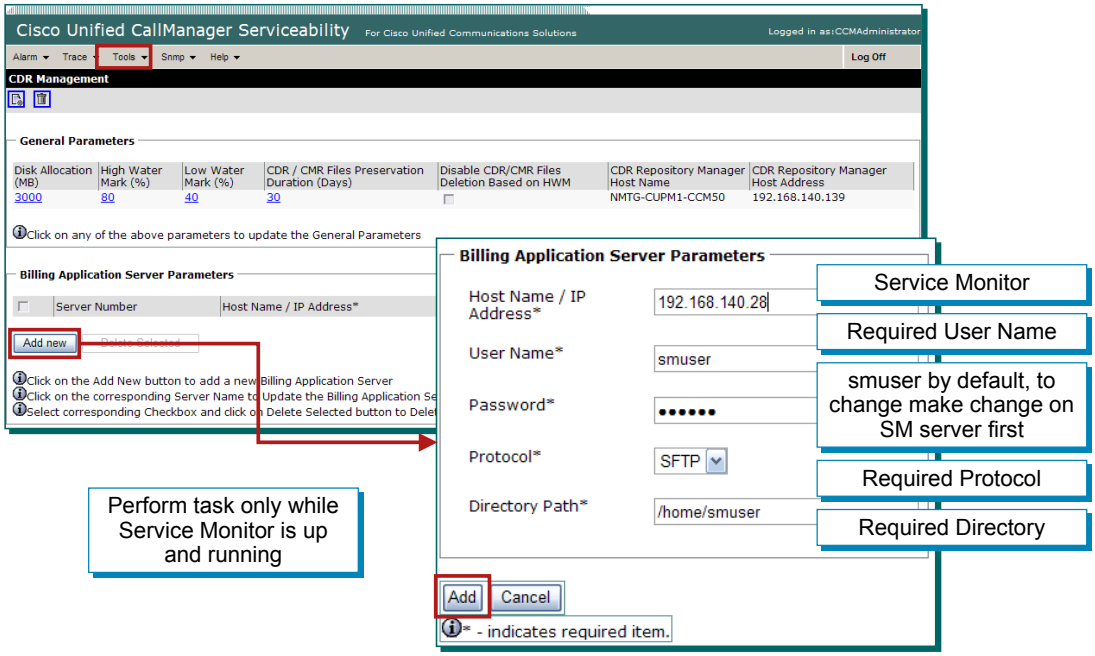
1. Log on to the server where Cisco Unified CallManager is installed. Select **Start > Programs > Microsoft SQL Server Enterprise Manager > Security**.
2. Right-click **Logins** and select **New Login**.
3. On the **General** tab: Enter a username. Select SQL Authentication and enter a password. Make sure that SQL Authentication is selected and *not* Windows Authentication, which can sometimes be selected by default.
4. Select the **Server Roles** tab and select the **System Administrators** role.

(continue…)

Working with Cisco Unified CallManagers – Create SQL User, (Cont.)

5. Select the **Database Access** tab.
    - Select databases as follows:
        - For Cisco Unified CallManager version 4.x, check the **Permit** column for the CDR database.
        - For Cisco Unified CallManager version 3.3.x, check the **Permit** column for the CDR database and for the device database, named CCM030n; for example, CCM0300. Alternatively, select only one database, CDR or the device database, and continue creating the account. After creating one account, repeat the procedure to create another account for the other database.
        - Note: Each time you upgrade Cisco Unified CallManager, the *n* in CCM030*n* is increased by 1 and a new device database is created. If there are multiple device databases, choose the most recent one, the one with the highest number; for example, CCM0302. If you upgrade Cisco Unified CallManager 3.3 after you complete this step, you must return to this procedure and repeat this step.
        - Note: Alternatively, select only one database, CDR or the device database, and continue creating the account. After creating one account, repeat the procedure to create another account for the other database.
    - At the bottom of the window, database roles for the selected databases are displayed; public is checked by default.
    - Check the **db_owner** role (so that public and db_owner are checked).
6. Click **OK**. A confirmation dialog box appears. Confirm the password by entering it again in the dialog box.

Working with Cisco Unified CallManagers
CCM 5.x – Create Billing Server



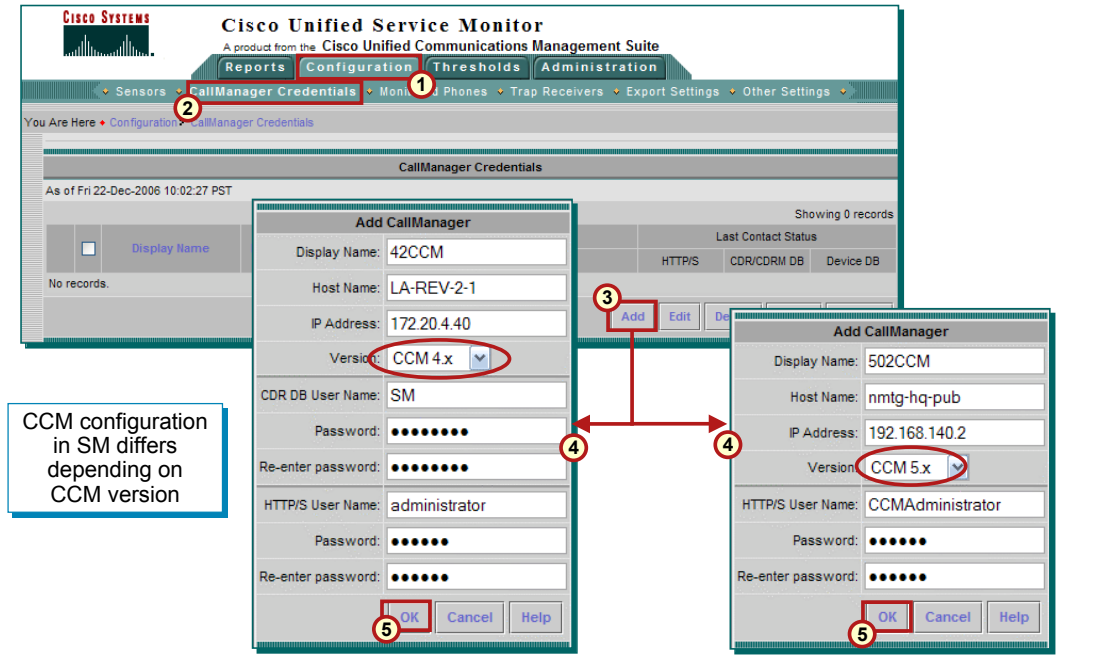
Working with CU CallManagers – Create Billing Server (CCM 5.x only)

Another task to have SM work with Cisco CallManagers 5.x is to add Service Monitor to Cisco Unified CallManager 5.x as a Billing Server. Here's how to configure this.

1. Launch **Cisco Unified CallManager Serviceability**.
2. Select **Tools > CDR Manageability**.
3. Scroll down to **Billing Applications Server Parameters** and click **Add New**. Enter the following:
    - Host Name / IP Address--IP address of Cisco Unified Service Monitor.
    - User Name--Enter smuser. Note: Do not enter any username other than smuser.
    - Password--Enter a password. The default password is smuser. To change this password:
        - Change it in Service Monitor first.
        - Enter the same password that you entered for smuser while configuring other settings in Service Monitor.
        - Note: If you changed the password in Service Monitor and Cisco Unified CallManager does not immediately accept the new password, wait one minute and enter the new password again.
    - Select SFTP Protocol.
    - Directory Path--Enter /home/smuser/. Note: Do not change.
4. Click **Add**.

- In some cases, for CDR/CMR files to be delivered to a newly added billing server, it is necessary to first restart the CDR Repository Service. From Cisco Unified CallManager Serviceability, select Tools > Control Center - Network Services. Then select publisher > stop / start or restart Cisco CDR Repository Manager.
- Perform this task on Cisco Unified CallManager version 5.x only.
- Perform this task only while Service Monitor is up and running.

Working with Cisco Unified CallManagers
Add CCM Credentials to Service Monitor



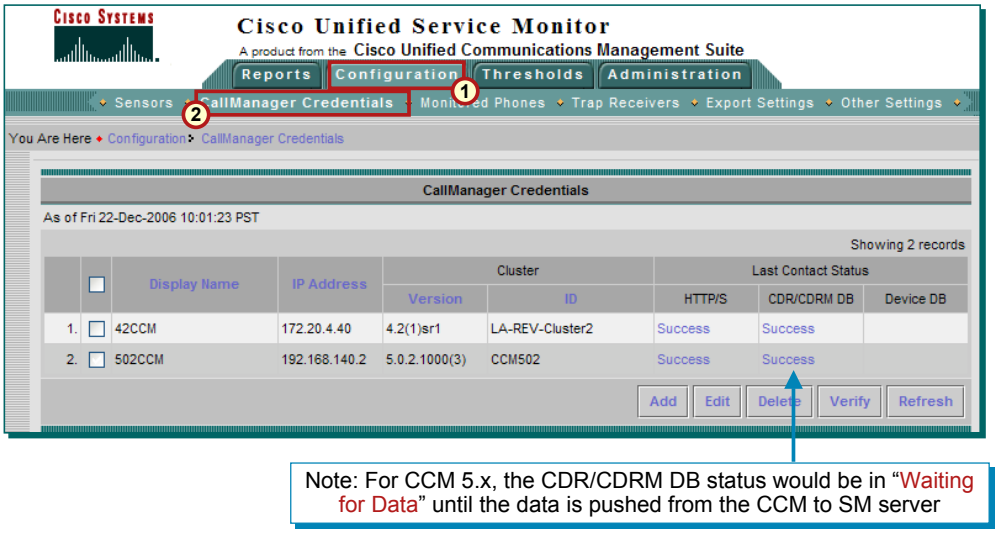
Working with Cisco Unified CallManagers – Add CCM Credentials to SM

Service Monitor can obtain and analyze voice data from supported versions of Cisco Unified CallManager. For Service Monitor to do this, Dean must:

- Perform configuration tasks (just described in the previous slides) either using Cisco Unified CallManager or logged in to the system where Cisco Unified CallManager is installed.
- Add Cisco Unified CallManager credentials to Service Monitor using the following procedure.

1. Select **Configuration > CallManager Credentials**. The CallManager Credentials page displays existing CallManager information.
2. Click **Add** to add a new CCM. The Add CallManager dialog box appears, which differs per CCM version. Enter the data:
   - Enter a display name--up to 20 characters--to describe the cluster.
   - Host Name - (Optional) - Enter the host name for the server where Cisco Unified CallManager is installed. Note, you must enter the host name of the Cisco Unified CallManager if the Service Monitor server cannot resolve the Cisco Unified CallManager host name to an IP address.
   - IP Address - Enter the IP address for appropriate node in the cluster; for this software version: For 3.3.x or 4.x --Enter the IP address for the publisher; for 5.x--Enter the IP address for a publisher or a subscriber
   - Version - Select the software version running on the cluster. These versions are supported: 3.3.x, 4.x, and 5.x.
   - Enter usernames and passwords. The usernames and passwords that are required vary by Cisco Unified CallManager version. Refer to on-line help for more details.

Working with Cisco Unified CallManagers
CCM Access Status



Working with Cisco Unified CallManagers – CCM Access Status

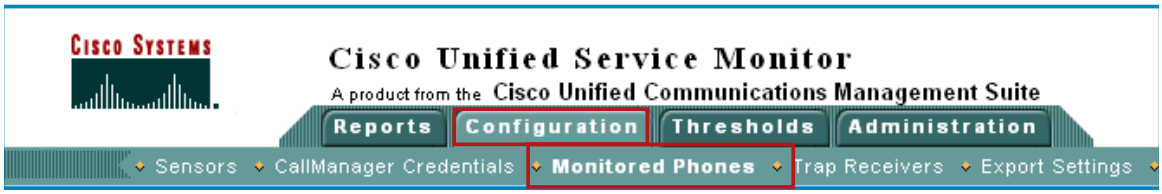
Service Monitor needs one or more credentials to obtain Cisco Unified CallManager data successfully. The CallManager Credentials page displays the status of the last contact between Service Monitor and Cisco Unified CallManagers.

In a few cases, you might need to correct credentials on the Cisco Unified CallManager and then verify the credentials from Service Monitor:

- When the last contact status is Successful, in some cases, Service Monitor might not be receiving data, but simply waiting to receive data. To see when the last successful contact occurred, click the status link. If the last contact was not recent, correct any problem with credentials on the Cisco Unified CallManager and verify the credentials from Service Monitor.
- Credentials that Service Monitor relies upon might change on the Cisco Unified CallManager platform. If this happens, check with your Cisco Unified CallManager administrator to obtain the correct credentials. If necessary, update the credentials in Service Monitor. Otherwise, verify the credentials.

To verify access credentials, select the Cisco Unified CallManager for which you want to verify credentials. Then, click Verify.

Working with Clusters/Sensors
Monitored Phones



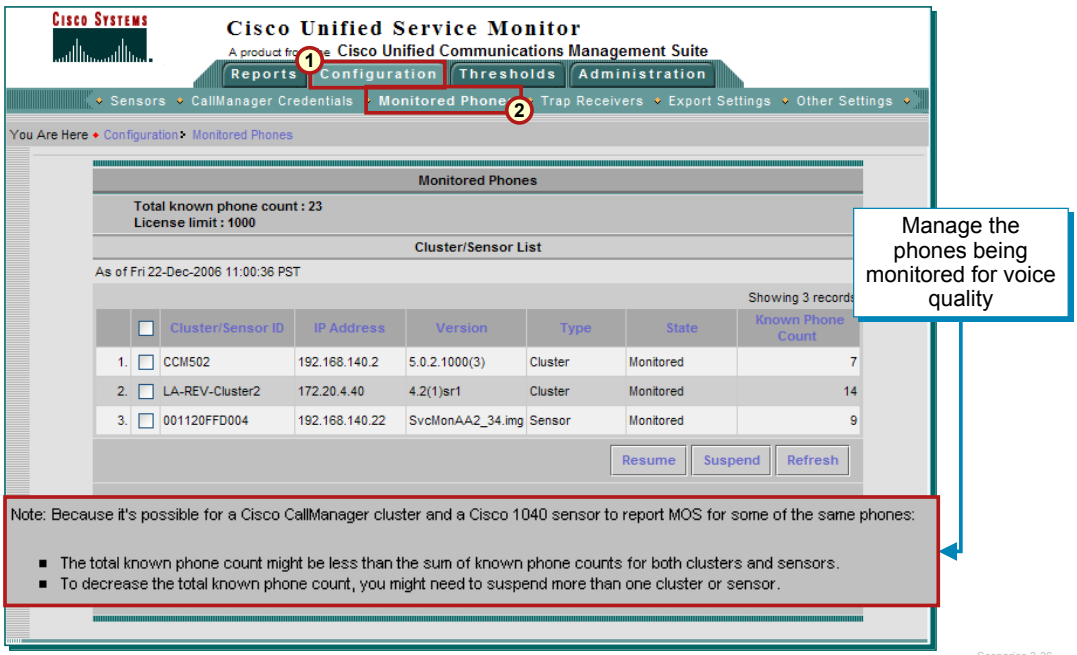
- Displays phone count for each cluster and sensor that is managed with this Service Monitor
- Displays total phone count and licensed limits
- Suspending and resuming the monitoring of a sensor or cluster resets the phone count, allowing new clusters and sensors to be added or sensors to be relocated
- Records are not processed for an entity that is Suspended

Working with Clusters / Sensors

Service Monitor starts to monitor a cluster when it learns of the cluster. Service Monitor learns of a cluster when you add Cisco Unified CallManager credentials to Service Monitor (previous slide). Service Monitor learns of a Cisco 1040 sensor when the sensor registers.

If Dean wants to suspend a cluster or a sensor from monitoring--for example, to enable him to monitor phones from a different cluster or sensor--Dean can do so using the **Monitored Phones** task, described next.

Working with Clusters/Sensors
Monitored Phones, (Cont.)



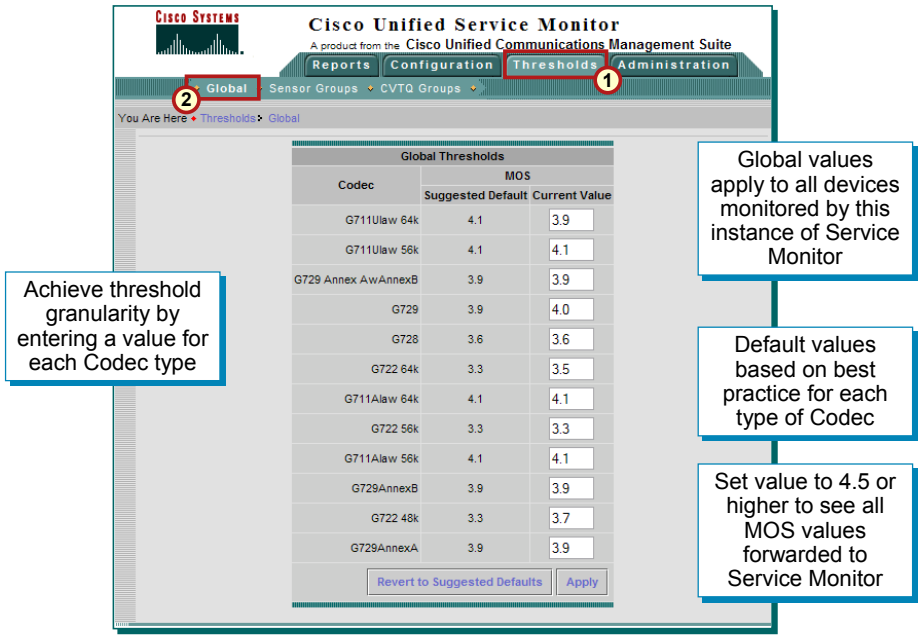
Working with Clusters / Sensors

On the **Monitored Phones** page, Dean can view the total number of phones that Service Monitor is monitoring. He can also view the names of all sensors and Cisco Unified CallManager clusters known to Service Monitor, see whether each is monitored, and, if so, see the number of phones that Service Monitor manages in the cluster or for the sensor.

Note that because it is possible for a Cisco Unified CallManager cluster and a sensor to report MOS for some of the same phones:

- The total known phone count displayed on the Monitored Phones page might be less than the sum of known phone counts for clusters/sensors.
- To decrease the total known phone count, you might need to suspend more than one cluster or sensor.

Defining Thresholds
Global



Defining Thresholds – Global

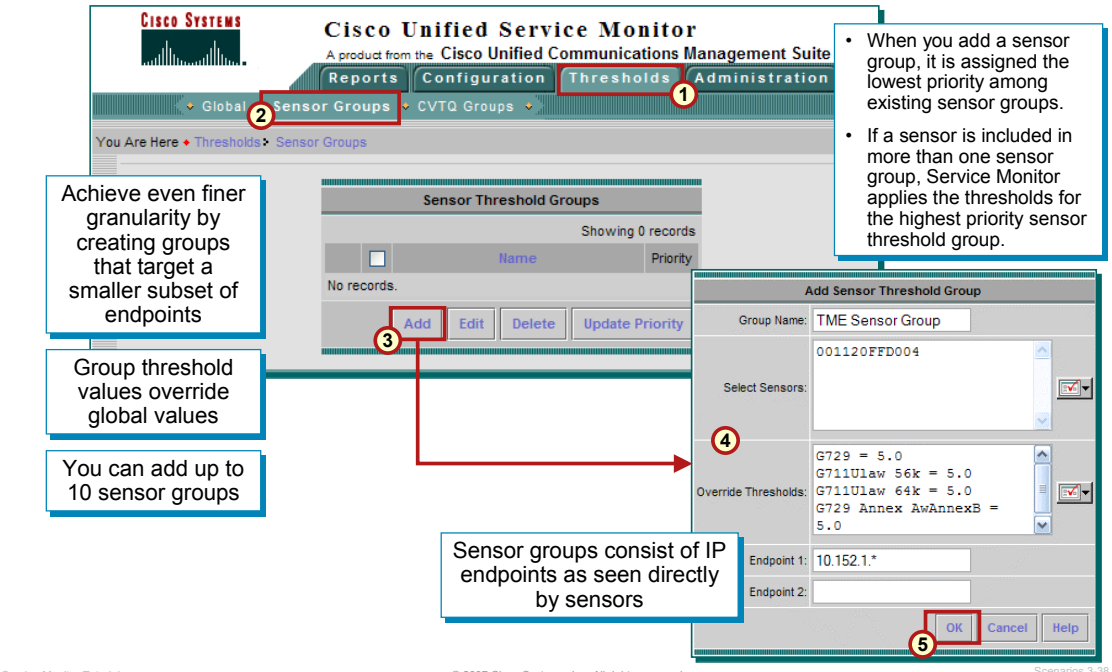
Service Monitor uses thresholds to determine when a MOS value--reported from a sensor or included in CDRs from a Cisco Unified CallManager cluster--has fallen to an unacceptable level. When MOS falls below a threshold, Service Monitor sends a QoVMOSViolation trap to up to four trap receivers. Dean plans on using the Cisco Unified Operations Manager as a trap receiver.

Service Monitor supplies global thresholds and provides default values for them. Service Monitor can use global thresholds to compare against MOS values reported from sensors or clusters. Since the MOS threshold values might vary depending upon the codec being used in a call, global thresholds include separate values for commonly used Codecs, as illustrated above.

Dean can update the global threshold default values to reflect MOS values below the average MOS seen in his system. By monitoring Service Monitor reports, he can determine average MOS values and then adjust global thresholds accordingly. Dean can also easily restore global thresholds to the default values that Service Monitor supplies.

If Dean would like to use different threshold values for particular sensors, clusters, or groups of endpoints reported on by either sensors or clusters, he can override global thresholds by adding these threshold groups: **Sensor Groups** and **CVTQ Groups**. These are discussed next.

Defining Thresholds
Sensor Groups



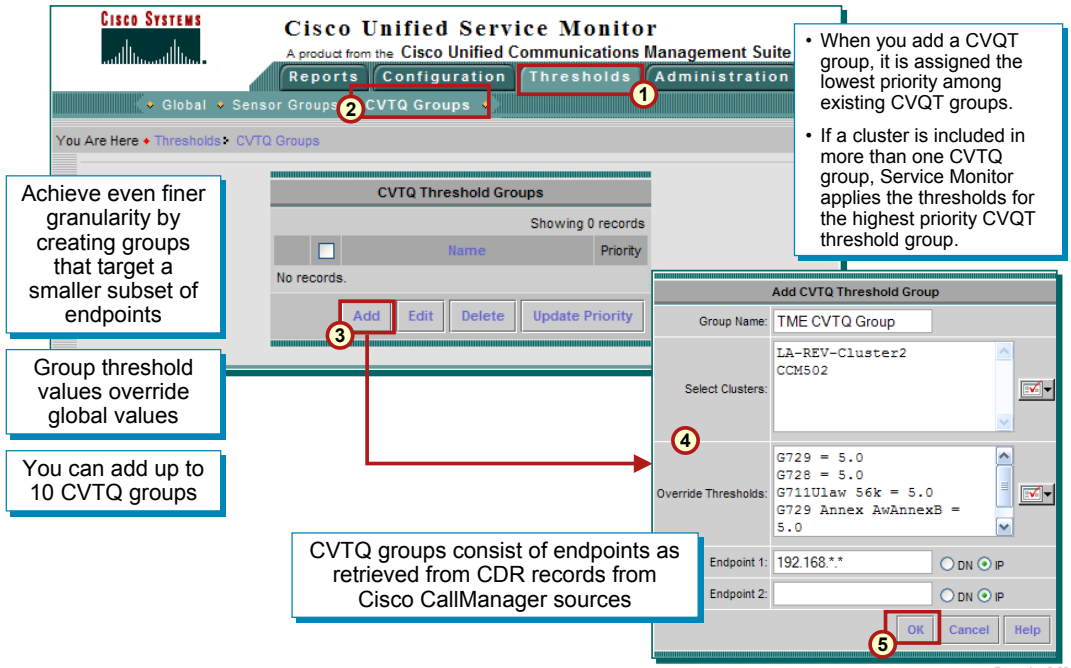
Defining Thresholds – Sensor Groups

A sensor group includes one or more sensors, two sets of endpoints, and one or more threshold values for commonly used Codecs.

If Dean would like to use different threshold values for particular sensors, clusters, or groups of endpoints reported on by sensors, he can override global thresholds by adding a sensor threshold groups.

Dean can create up to 10 sensor groups. Sensor groups are prioritized from highest (one) to lowest (ten). In cases where an endpoint is included in more than one sensor group, Service Monitor compares MOS for the endpoint against the highest priority group that it belongs to.

Defining Thresholds
CVTQ Groups



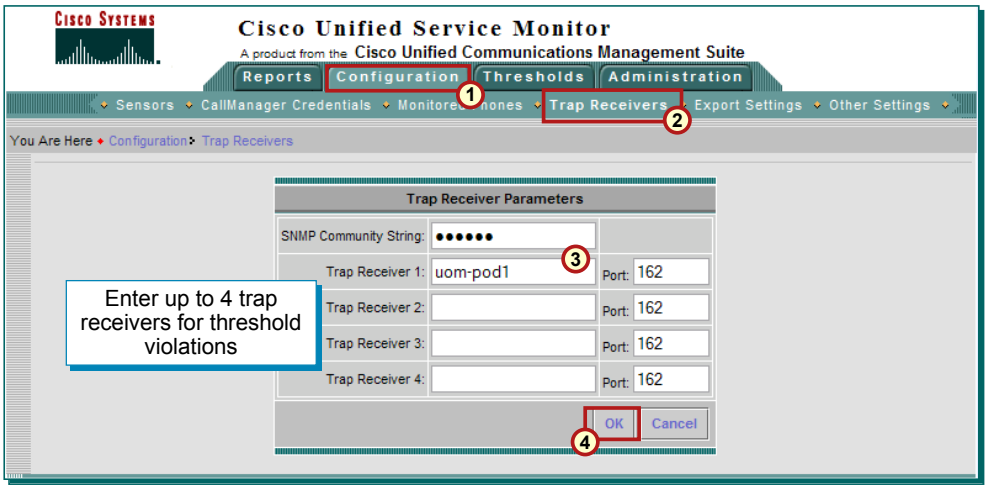
Defining Thresholds – CVTQ Groups

A CVTQ group includes one or more clusters, two sets of endpoints, and one or more threshold values for commonly used Codecs.

If Dean would like to use different threshold values for particular sensors, clusters, or groups of endpoints reported on by clusters, he can override global thresholds by adding a CVTQ threshold groups.

Dean can create up to 10 CVTQ groups. CVTQ groups are prioritized from highest (one) to lowest (ten). In cases where an endpoint is included in more than one CVTQ group, Service Monitor compares MOS for the endpoint against the highest priority group that it belongs to.

Defining Thresholds
Define Where to Send Threshold Violations



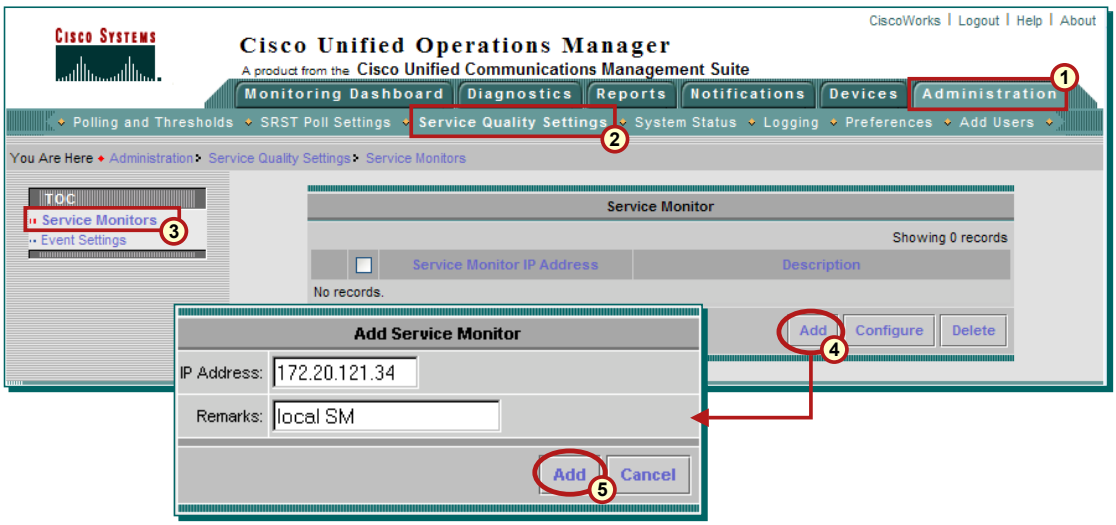
Note: Typically one of the trap receivers is Operations Manager which can display threshold violations on the Service Quality dashboard

Defining Thresholds – Trap Destination

Service Monitor can send a QoVMOSViolation trap to up to four trap receivers. Use the **Configuration> Trap Receivers** task to define these SNMP trap receivers.

Dean plans on using the Cisco Unified Operations Manager as a trap receiver. This will allow him to view threshold violations on the Service Quality dashboard.

Integrating with Operations Manager
Register Service Monitor



To display Service Monitor (SM) MOS violations on the Operations Manager (OM) Service Quality Dashboard, all SM servers must be registered with OM

Integrating with Operations Manager – Register SM

Dean had just used the **Setup** task of Service Monitor to forward any MOS violations as SNMP traps to Operations Manager. He must now configure Operations Manager to accept traps from Service Monitor.

Use the following steps to configure Operations Manager to accept traps from Service Monitor:

1. From the Operations Manager desktop, select the **Administration** tab.
2. Select the **Service Quality Settings** option found on the bar underneath the folder tabs.
3. A Table of Contents (TOC) menu is displayed on the left side of the OM desktop; select the **Service Monitors** task. The *Service Monitor* dialog is displayed listing any currently configured Service Monitor servers.
4. Click the **Add** button to add the local instance of Service Monitor.
5. The *Add Service Monitor* dialog is displayed. The OM/SM server IP address should be listed. If not, enter it in the IP Address field, enter any *Remarks*, and click Add.

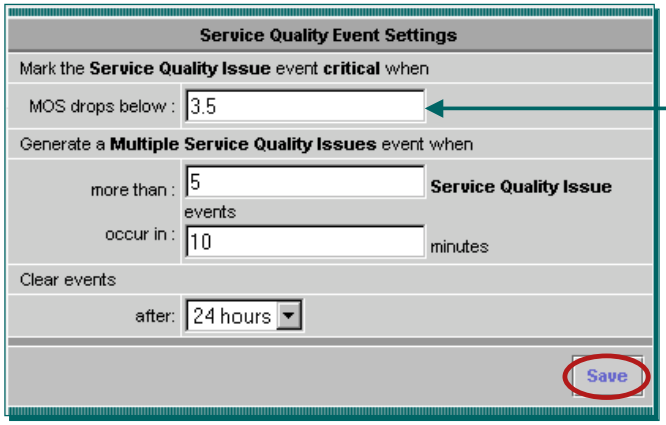
Operations Manager is now configured to have the received SNMP traps from Service Monitor, analyzed and displayed on the Service Quality Alert dashboard.

TIP: From the list of Service Monitors, select one and click **Configure** to launch the desktop for that instance of SM.

Integrating with Operations Manager
Event Display Settings

Define which MOS violations received by Operations Manager should be marked critical; all others will be set to warning

Operations Manager > Administration > Service Quality Settings > Event Settings



MOS violations at or below will be displayed as Critical Events

All other MOS violations will be displayed as Warning Events

Integrating with Operations Manager – Event Display Settings

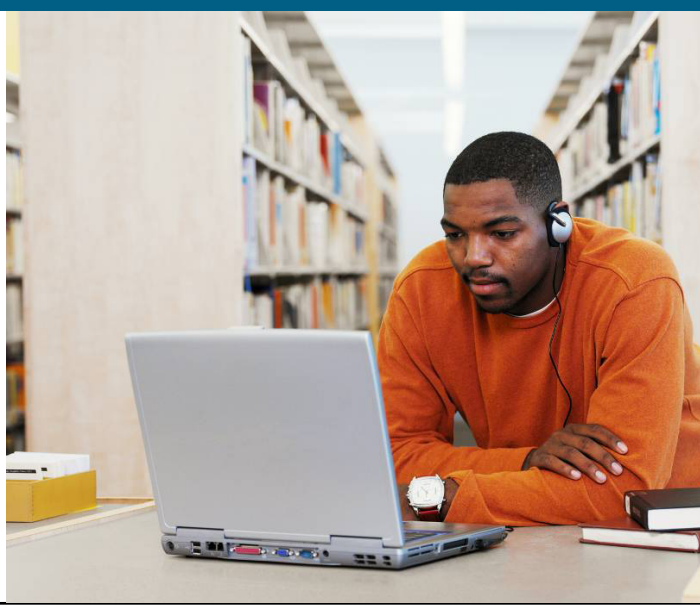
There is one final configuration step to make before Dean can look at the results and that is to define which MOS violations received by Operations Manager should be marked as critical in the dashboard and when a Multiple Service Quality Issues event should be generated.

Dean can configure Operations Manager to display different MOS values with different levels of severity icons. Earlier, he configured Service Monitor to send a MOS violation trap for certain MOS values (lets say 4.0 or lower). He can have Operations Manager display any MOS value of 3.5 or lower as a *Critical* alert and then any alert between 3.6 and 4.0 to be marked as a *Warning*. To achieve this, use the **Event Settings** task located in the Service Quality Settings.

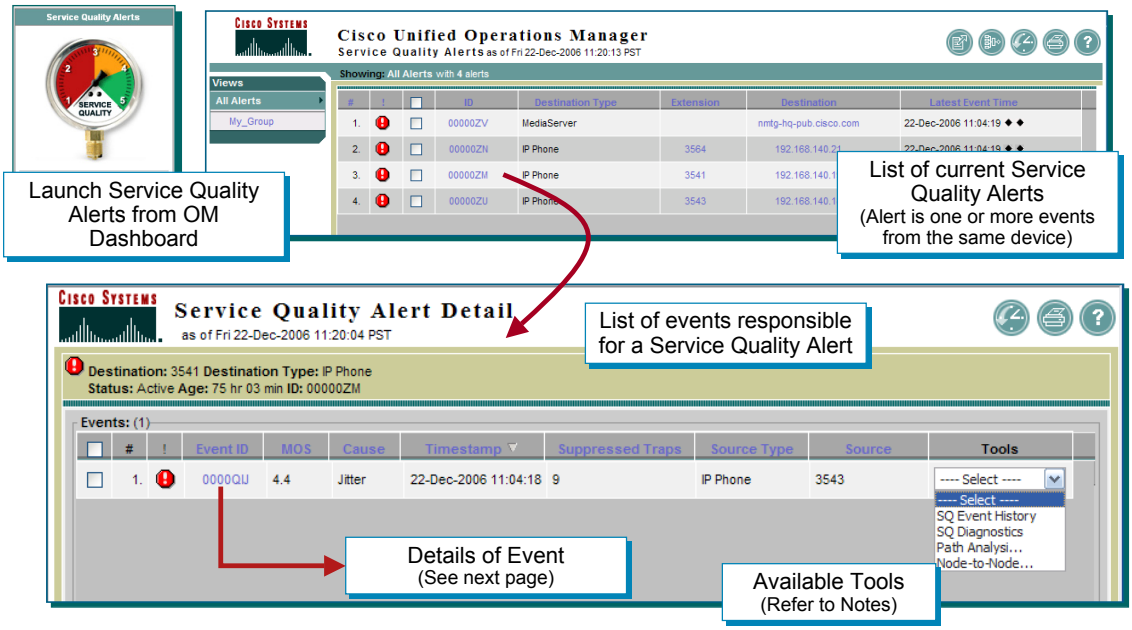
1. From the Operations Manager desktop select the **Event Settings** task from the TOC displayed after selecting **Administration > Service Quality Settings**. (This TOC should still be displayed after the previous task performed.)
2. The *Service Quality Event Settings* dialog is displayed. Set the "*MOS drops below"* field to a value that represents a critical condition, such as 3.5. This dialog is also used to tell Operations Manager when to generate a Multiple Service Quality Issues event, and a time frame for clearing the events.
3. Click **Save** to have these parameters take effect.

Scenario 3: Monitoring Active Calls

- Planning
- Getting Started
- **Monitoring Active Calls**



View Service Quality Alerts
Service Quality Alerts Dashboard



View Service Quality Alerts

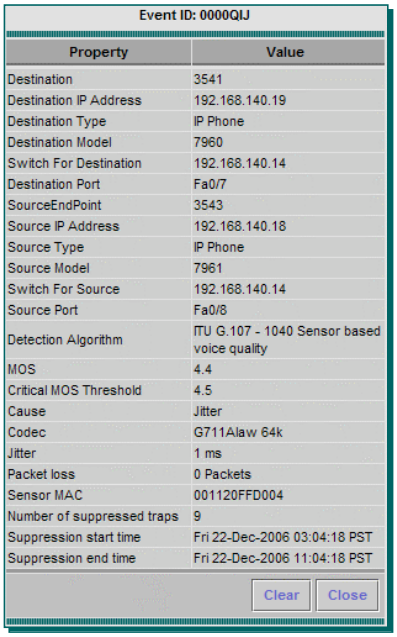
After completing the previous scenario, voice quality monitoring should be fully configured and operational. Let's take a look at the results when Service Monitor is integrated with Operations Manager.

The Service Quality Alerts Dashboard displays the alerts sent by Service Monitor using a SNMP trap. Service Monitor analyzes the incoming MOS values (coming from the Cisco 1040s and the Cisco CallManagers) against the user-defined threshold and forwards any violations to Operations Manager (as configured in the Setup task).

To view any MOS violation, use the following steps:

1. From the Operations Manager desktop select the **Monitoring Dashboard** tab.
2. The content area of the Operations Manager desktop displays four icons for four different types of dashboards. Clicks the third one – **Service Quality Alerts**.
3. The Service Quality Alerts dashboard is displayed in a new window listing the service quality alerts received (one entry per device reporting a service quality issue – an alert is one or more events). Each alert displays the type of device, extension number and address, the time of the last event, and the severity level of the highest individual event. To see details about an alert (individual events), click on the **Alert ID**.
4. The Service Quality Alerts Details table is displayed in a new window listing the individual service quality events that caused the alert. You can now see more information including the MOS value and primary cause for that MOS value. You can also launch several Operations Manager tools to help in troubleshooting efforts. The severity icons allow you to quickly see the MOS values below 3.5 because they are displayed as critical events as defined in the **Event Settings** task.
5. Click on an individual **Event ID** to see its details (next page).

View Service Quality Alerts
Service Quality Event Details



Event ID: 0000QIJ

Property	Value
Destination	3541
Destination IP Address	192.168.140.19
Destination Type	IP Phone
Destination Model	7960
Switch For Destination	192.168.140.14
Destination Port	Fa0/7
SourceEndPoint	3543
Source IP Address	192.168.140.18
Source Type	IP Phone
Source Model	7961
Switch For Source	192.168.140.14
Source Port	Fa0/8
Detection Algorithm	ITU G.107 - 1040 Sensor based voice quality
MOS	4.4
Critical MOS Threshold	4.5
Cause	Jitter
Codec	G711Alaw 64k
Jitter	1 ms
Packet loss	0 Packets
Sensor MAC	001120FFD004
Number of suppressed traps	9
Suppression start time	Fri 22-Dec-2006 03:04:18 PST
Suppression end time	Fri 22-Dec-2006 11:04:18 PST

Clear Close

Service Quality Event Details

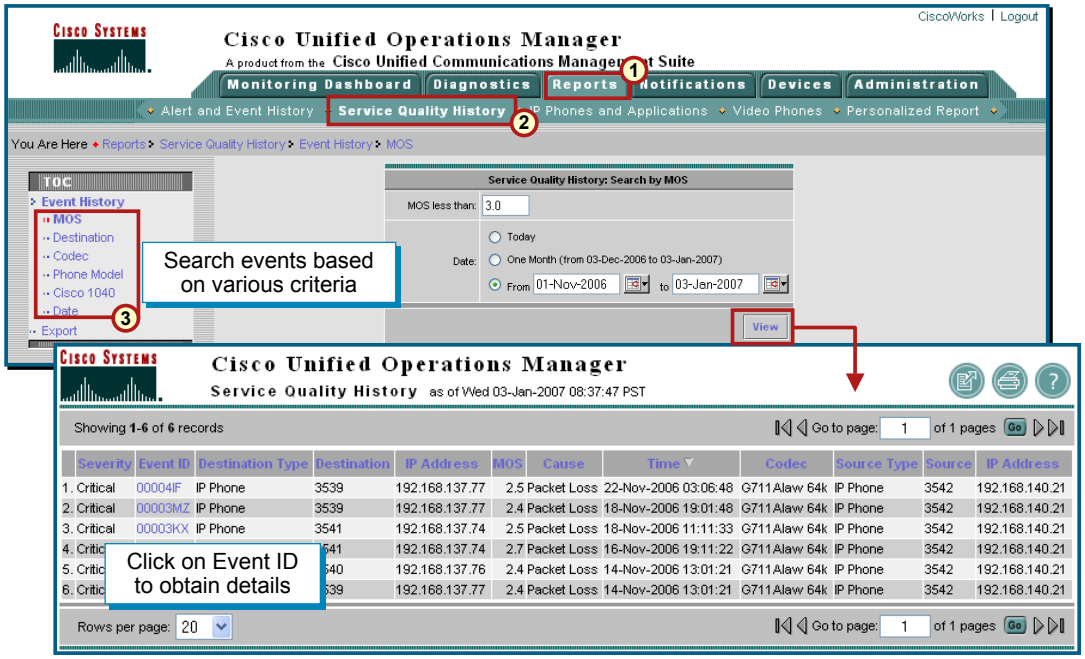
- Call information
  - Devices
  - Phone Numbers
  - Ports
  - addresses
- MOS Values
  - Reported
  - Threshold
- Detection algorithm: CVTQ-based or Cisco 1040 Sensor-based
- Main Cause for low MOS
  - Can be either *Packet Loss* or *Jitter*
- Codec used
- Actual Jitter and packet loss for the reported 60 second period
- Probe ID of the reporting Cisco 1040

View Service Quality Alerts – Event Details

The *Event Details* will open in a new window. The *Event Details* includes information about the endpoints (phone numbers, IP address, switch and port connectivity), as well as information about the nature of the violation (reported MOS, user-defined MOS threshold, primary cause for low MOS, Codec used for call, actual jitter and packet loss values this violation represents).

This particular violation was detected by a Cisco 1040 sensor (detection algorithm displayed); the reported MOS was 4.4, which is lower than the Service Monitor's user-defined threshold of 4.5; and the primary cause of the MOS was jitter, which was reported at 1 msec for the 60-second reporting period.

View Service Quality Alerts
Service Quality History Reports



View Service Quality Alerts – Service Quality History

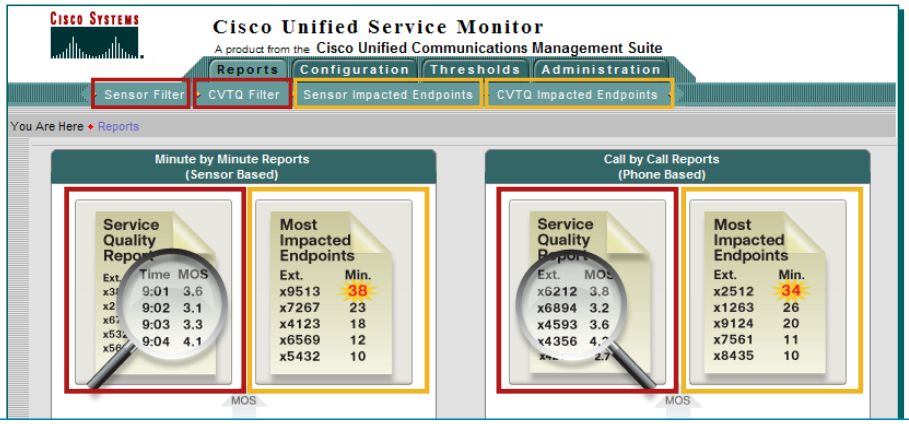
The Service Quality History Report lets Dean view stored information on past service quality events.

This information is stored in the Service Quality History database. The searches can be tailored according to what Dean is looking for, or he can set up Operations Manager to automatically save them to a file on the server using the **Export** feature.

Operations Manager allows Dean to search the database and generate a report based on events that have a mean opinion score (MOS) value less than a specified value, occurred on specific destination endpoints, have a specific Codec, occurred on specific phone models, associated with specific Cisco 1040 IDs, or have occurred within a specific date range.

The Export feature allows Dean to configure Operations Manager to automatically generate 24-hour and 7-day Service Quality reports daily and store them in CSV and PDF formats, with an email notification option.

Reporting
Overview



- Service Monitor reports enable you to examine voice transmission quality in the parts of your network that Service Monitor has monitored during the last 30 days.
- Service Monitor reports show the times when MOS have been low, the Codec in use on the call, and the endpoints on which the violations have occurred.
- Filter Reports - Enables you to specify what you want to report on and generate a report that contains as little as one day of data or as much as 30 days of data
- Most Impacted Endpoints Reports - Provides details of the end points experiencing the most severe voice quality issues for the previous day

Reporting – Overview

Service Monitor reports enables Dean to examine voice transmission quality in the parts of your network that Service Monitor has monitored during the last 30 days. Service Monitor reports show the times when MOS has been below configured thresholds, the codec in use, and the endpoints on which the violations have occurred. Data for the reports is obtained from Cisco 1040 sensors and Cisco Unified CallManager clusters in your network.

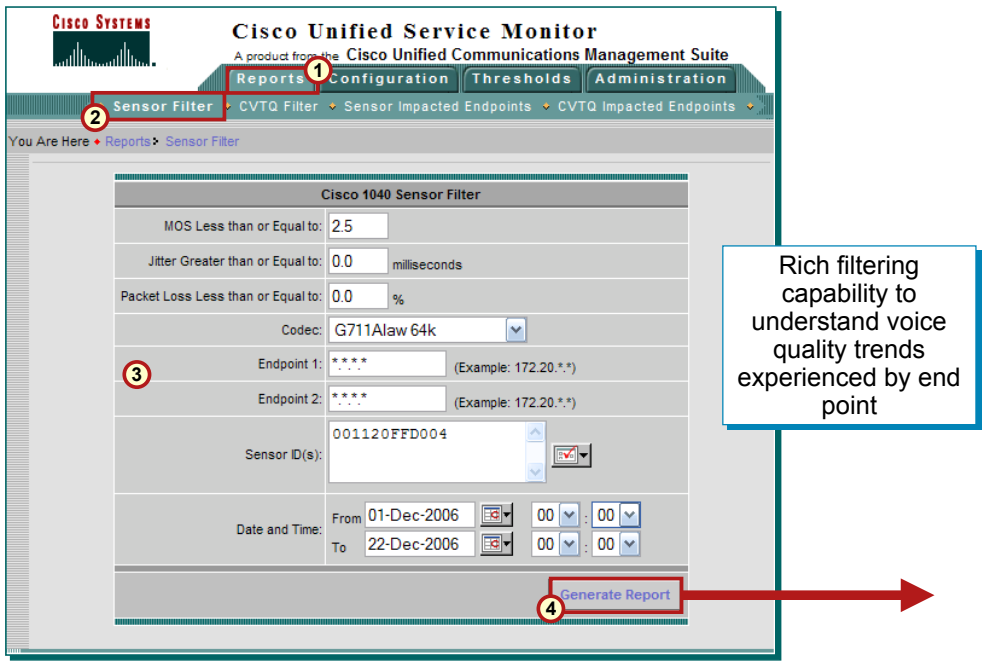
Service Monitor stores the data that it collects from sensors and Cisco Unified CallManagers in the Service Monitor database for 30 days. Service Monitor purges its database every day, retaining only the data for the last 30 days.

Service Monitor supplies separate reports for data obtained from:

- **Sensors**--Sensors send data to Service Monitor every 60 seconds, providing minute-by-minute assessments of MOS.
- **Cisco Unified CallManager Clusters**--Service Monitor obtains CVTQ data from clusters every 60 seconds. However, data for a given call becomes available only after it completes. Service Monitor therefore can assess MOS, send traps, and provide information in reports after the call has occurred.

Within sensor reports and CVTQ reports, there are two types of reports: Diagnostic reports and Most-Impacted Endpoint reports. These reports are discussed next.

Reporting
Configuring Sensor Report



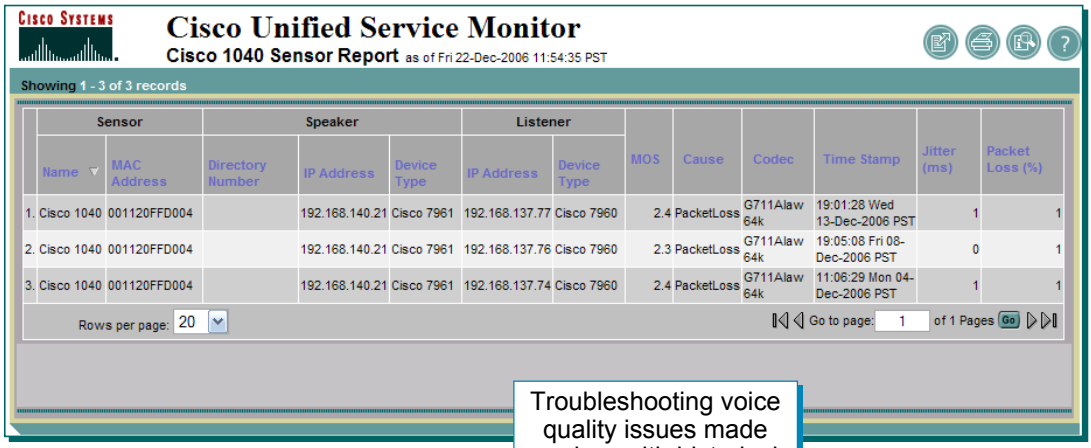
Reporting – Configuring Sensor Report

After Cisco 1040 sensors in the network register to a Service Monitor, they send data to that Service Monitor every 60 seconds for every call underway. Service Monitor retains the data in its database for up to 30 days.

Using sensor report filters, Dean can generate reports that include data for all calls that have been monitored by the sensors or reports that include a subset of data, such as:

- Where MOS was less than a specific value
- When reported from specific sensors
- Where particular Codecs were used
- A set of endpoints
- All sensors or a subset of sensors
- Any given time period--from one minute to 30 days--during the last 30 days

Reporting
Cisco 1040 Sensor Report

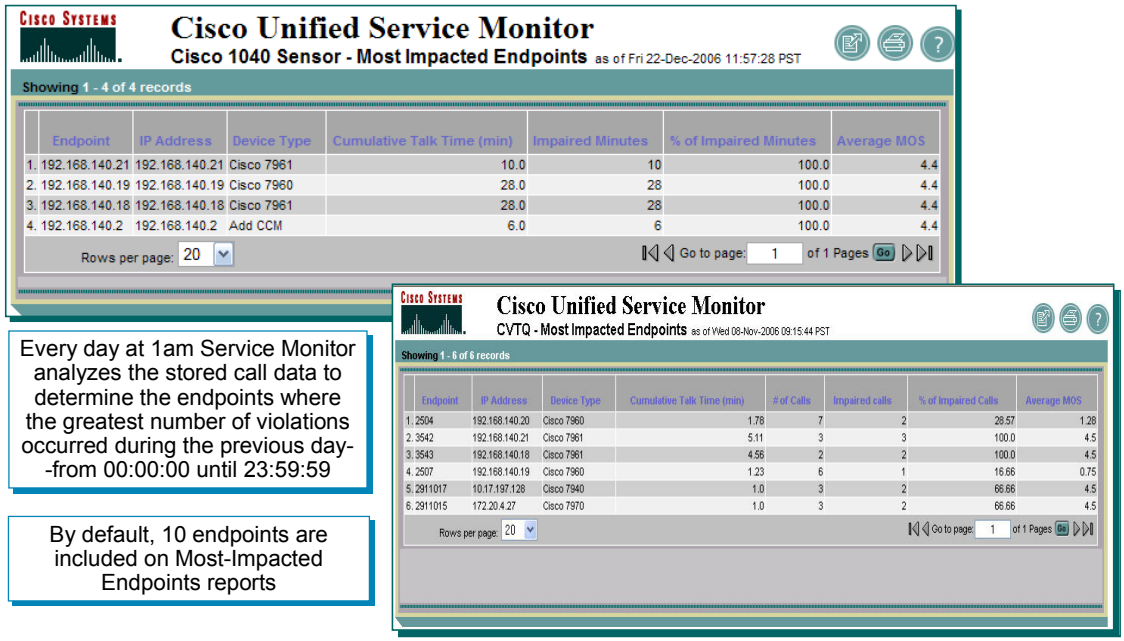


Troubleshooting voice quality issues made easier, with historical information

Reporting – Cisco 1040 Sensor Report

Illustrated above is a report that Dean generated. Reports like these will help Dean troubleshoot voice quality issues easier with historical information.

Reporting
Most Impacted Endpoints



Every day at 1am Service Monitor analyzes the stored call data to determine the endpoints where the greatest number of violations occurred during the previous day--from 00:00:00 until 23:59:59

By default, 10 endpoints are included on Most-Impacted Endpoints reports

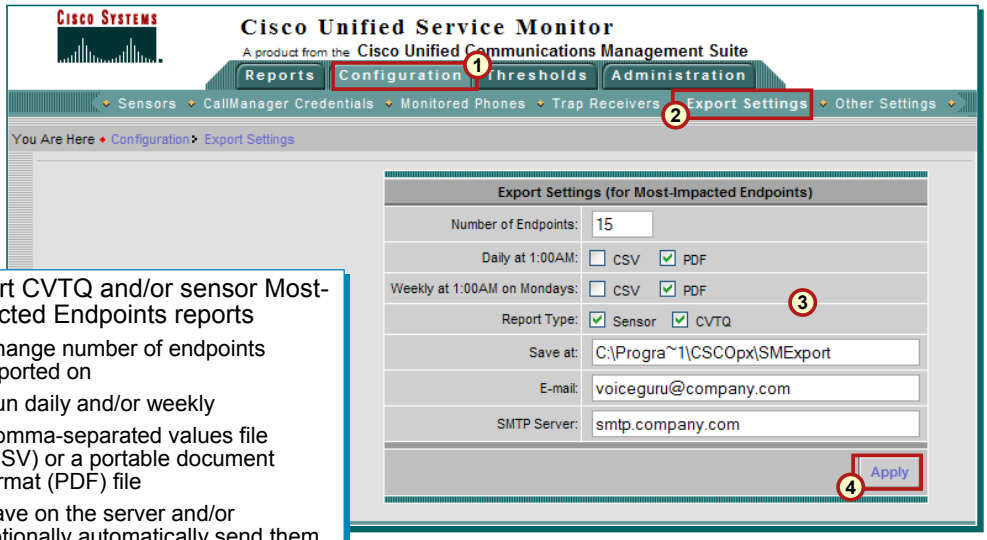
Reporting – Most Impacted Endpoints

The Most-Impacted Endpoint reports list the endpoints that have had the most violations reported in the last 24 hours. Dean can also schedule this report to run automatically; exported reports are then created for the last 24 hours and for the last 7 days.

Every day at 1am Service Monitor analyzes the stored call data to determine the endpoints where the greatest number of violations occurred during the previous day--from 00:00:00 until 23:59:59:999. Service Monitor stores the result of this analysis in the database for display in most-impacted endpoints reports. Subsequent to the analysis, Service Monitor optionally exports daily and weekly (on Monday) most-impacted endpoints reports, storing them on the server.

By default, Service Monitor determines the 10 most-impacted endpoints and does not export the most-impacted endpoints reports. To change the number of most-impacted endpoints that Service Monitor reports on and to configure automatic export, use the **Configuration > Export Settings** task, discussed next.

Reporting
Export Settings



Export CVTQ and/or sensor Most-Impacted Endpoints reports

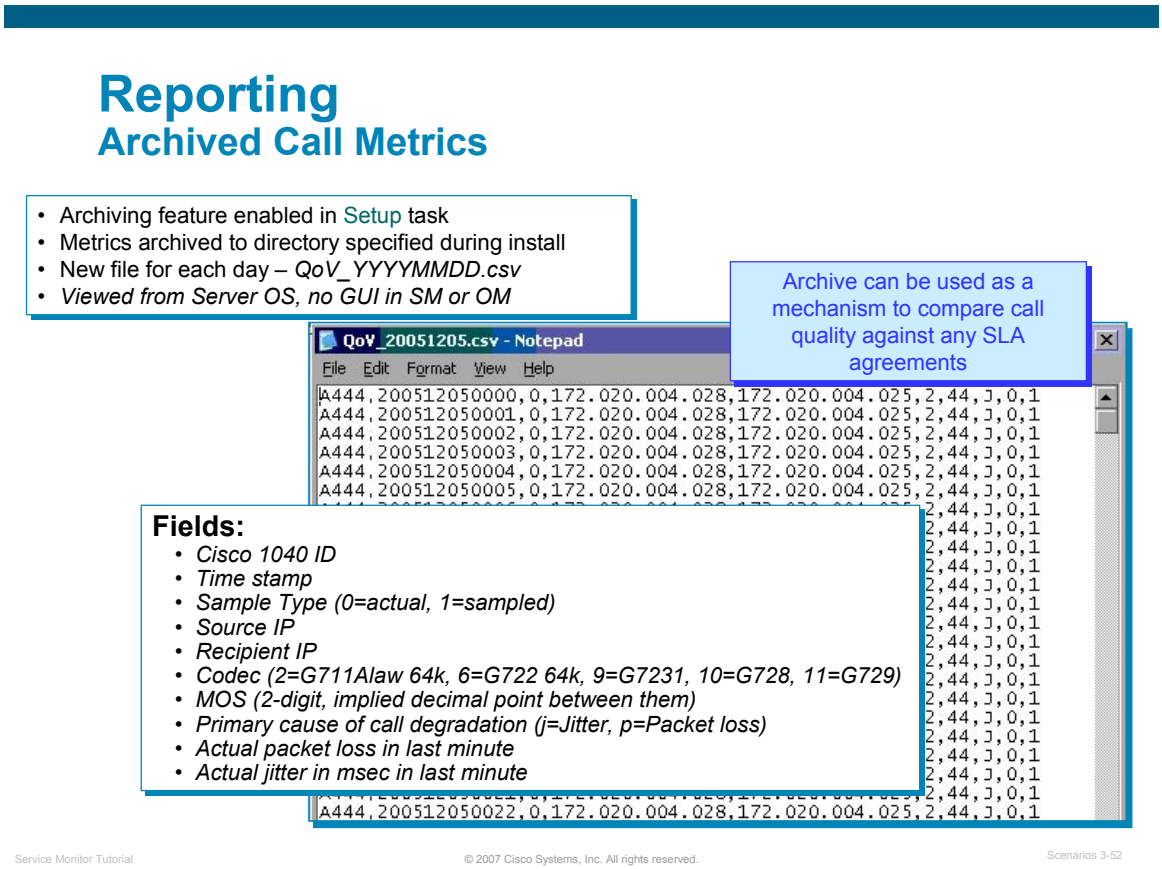
- Change number of endpoints reported on
- Run daily and/or weekly
- Comma-separated values file (CSV) or a portable document format (PDF) file
- Save on the server and/or optionally automatically send them through e-mail

Reporting – Export Settings

The CVTQ and sensor Most Impacted Endpoints reports can be exported to a CSV or PDF file.

Dean can use the **Configuration > Export Settings** task, to configure:

- The number of endpoints to be included in CVTQ and sensor most-impacted endpoint reports no matter when they run--daily, weekly, or on demand.
- The most-impacted endpoints reports to export--CVTQ or sensor or both. Most-impacted endpoint reports can run daily and weekly, exporting the results to a comma-separated values file (CSV) or a portable document format (PDF) file. You can save the reports on the server and, optionally, automatically send them through e-mail.



Reporting – Archived Call Metrics

The call metrics received from the Cisco 1040 sensors can be archived on the Service Monitor server for further analysis.

During the Service Monitor **Setup** task, Dean could enable **Call Metrics Archiving**, which would archive all incoming call metrics from the Cisco 1040 sensors to a flat file. This file can then be analyzed to help verify conformance to service level agreements (SLAs) in place with Service Providers.

A new call metric archive file is created each day and can be found in the directory defined during installation. Each entry in the file represents a 60 second sample for a single call (one direction). The fields include:

- Reporting Cisco 1040
- Time Stamp
- Sample Type (actual/sampled) – this will always be actual
- Source IP
- Recipient IP
- Codec –number representing Codec used (2 = G711Alaw 64k, 6 = G722 64k, 9 = G7231, 10 = G728, and 11 = G729)
- MOS – Mean Opinion Score is 2 digit number with an implied decimal point between them that represents the quality of the call
- Primary cause of call degradation – either jitter or packet loss
- Actual packet loss in the last minute
- Actual jitter in milliseconds in the last minute

These files can be accessed using the file system on the server. Also note that these files are not backed up as part of the CiscoWorks data backup process.

Dean can now rest easier and work smarter with Cisco Unified Service Monitor in place!

Thank You!

Continue on to Chapter 4 to learn about some of the System Administrative tasks not yet discussed.

Cisco Systems

<Intentionally Left Blank>

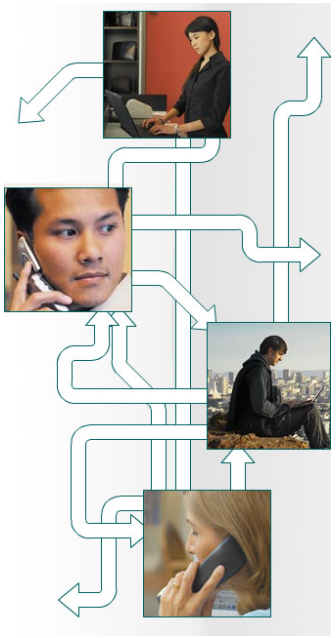
Cisco Unified Service Monitor

System Administration

Chapter 4

Chapter 4 Outline

- Requirements
  - Server
  - Client
- Installation Guidelines
  - Licensing
- User Security Administration
- Periodic Maintenance
- Helpful Troubleshooting Tips



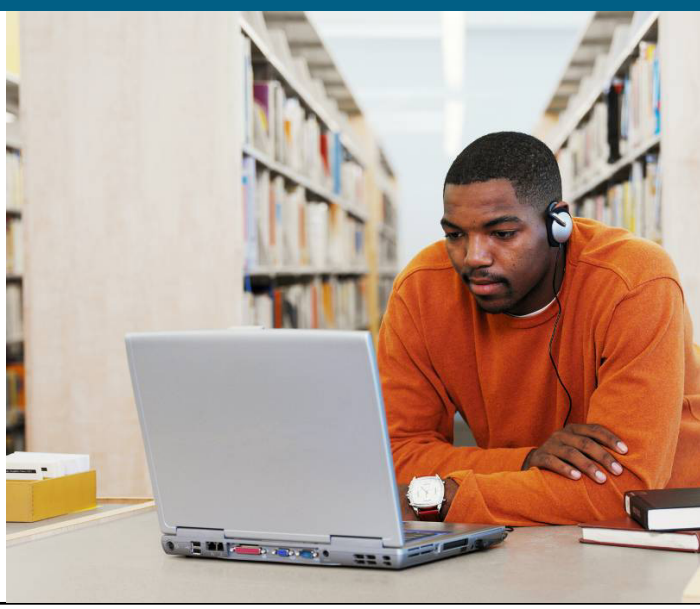
Chapter 4 Outline

This chapter starts out by covering some basic requirements for both the Service Monitor (SM) server and client used to access the server. Following that are sections that briefly covers some installation guidelines, periodic maintenance tasks, and some helpful troubleshooting tips.

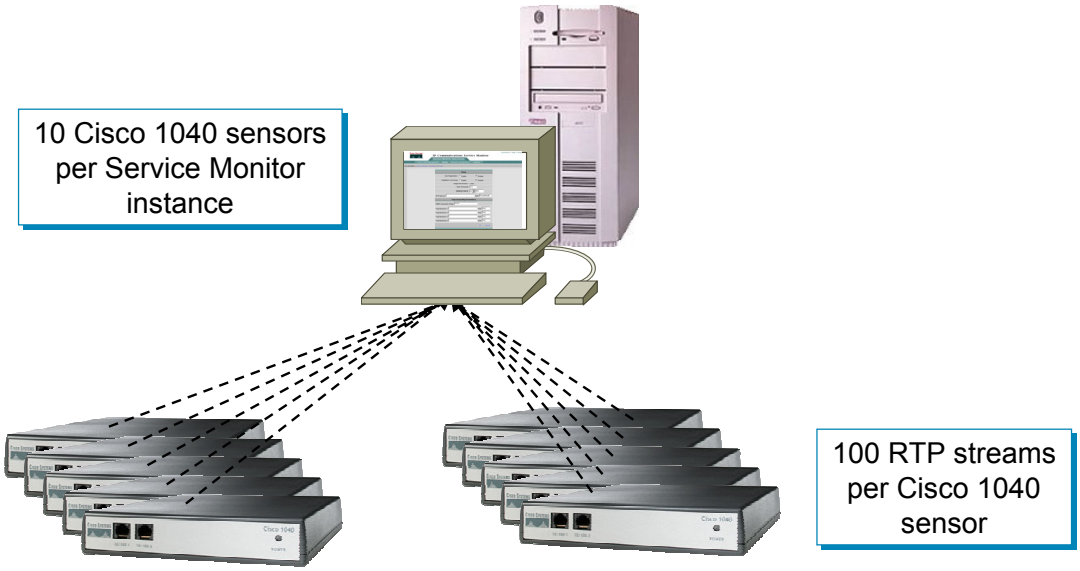
For detailed installation steps, refer to the Installation and Setup Guide for Service Monitor. Links to these reference guides can be found in Chapter 5.

Requirements

- **Requirements**
- Installation Guidelines
- User Security Administration
- Periodic Maintenance
- Helpful Troubleshooting Tips



Requirements
Number of Service Monitor Servers



Number of Service Monitor Servers

Each instance of an Service Monitor server can support up to 10 Cisco 1040s. This limit is primarily due to the large amount of I/O generated. This limit will dictate the minimum number of Service Monitor servers necessary to support the deployment of Cisco 1040s. Of course, multiple server instances can be deployed that do not support a full compliment of 10 Cisco 1040s. This would allow for growth, as well as, regional placement.

Requirements
Stand-Alone SM Server

Server Requirements	
Processor	Pentium IV > 2Ghz
Memory	2 GB
Swap	4 GB
Disk Space (NTFS Format)	60 GB Minimum
Operating System	• Windows Server 2003, Standard or Enterprise • SPK1 • ODBC Driver 3.5.10

Windows Terminal Services is supported in remote administration mode only

Stand-Alone SM Server Requirements

The chart above details the sizing requirements for a stand-alone Service Monitor server supporting up to 10 Cisco 1040s. If Service Monitor is to reside on the same server as Operations Manager, then additional resources will be required.

Note(s):

- It is always a good idea to check the latest release notes for up-to-date information regarding system requirements.

Requirements
Client

Client Requirements (minimum)	
Processor	Pentium IV > 1Ghz
Memory	1 GB
Swap	2 GB
Operating System	• Windows XP Home or Professional with SPK2 • Windows Server 2003, SPK1, Standard or Enterprise without terminal services
Additional Software	• Microsoft Internet Explorer 6.0.2600.0000, IE 6.0.2800.1106, or IE 6.0 (6.0.3790.0, which ships with Windows 2003 Server) • Adobe Macromedia Flash Player 8 or 9

Client Requirements

Access to a Service Monitor server is achieved using a standard web browser. Service Monitor has been tested and certified only on PC compatible systems running either Windows XP or Windows 2000/2003, and using Microsoft Internet Explorer (6.0.28 or 6.0.37) or Mozilla 1.75.

Note(s):

- It is always a good idea to check the latest release notes for up-to-date information regarding system requirements.
- Clients not conforming to the above requirements may also work but have not been tested and certified by Cisco and therefore will not be supported should problems arise.

Requirements
Client Web Browser Configuration

- ✓ Enable Java and Java Script
- ✓ Set browser cache to at least 6 MB
- ✓ Configure your browser to accept all cookies
- ✓ Configure your browser to compare each page with its cached version every time it loads a page
- ✓ Change the default timeout to 20 minute
- ✓ Enable style sheets
- ✓ Change the default font to sans-serif for improved readability
- ✓ Disable any pop up blocker utility installed on client system
- ✓ Add server as a Trusted Internet site for improved screen size

Web Browser Configuration

As discussed in the Client Requirements, Internet Explorer is the only supported web browser to access Service Monitor. The Install and Setup Guide describes the exact steps for configuring each of the above configuration items for each browser type. (Refer to Chapter 5 for a link to the Install Guide.)

Using the ***Tools>Internet Options> Security*** dialog of Internet Explorer, add the Service Monitor server as a Trusted Internet site. In doing so, the status bar on the bottom of the browser will be removed resulting in a better screen size for the SM dashboards and dialogs.

If you have browser problems after configuring your browser, increase your disk cache settings.

After the web browser is installed on the client system, there are no additional disk space requirements.

However, because the browser uses the local disk to store cached information, ensure that you have enough disk space for the amount of cached information you want to store.

Requirements
Preparing Application Services

DHCP Server:

- Configure DHCP server so that option 150 returns the IP address for the TFTP server (The Cisco 1040 will retrieve its binary image and configuration from TFTP server)

TFTP Server:

- Manually copy Cisco 1040 binary image from image directory on SM server (image directory defined during install. Use Service Monitor to generate and transfer Cisco 1040 configuration files to TFTP server.

Preparing Application Services

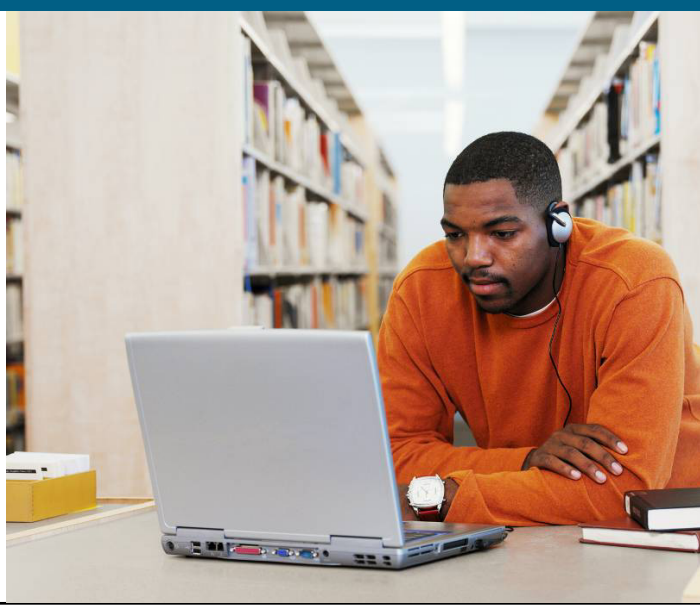
To properly function, Service Monitor requires the configuration of several other servers in the environment.

DHCP Server – because the Cisco 1040s behave like IP phones, they must get there image and configuration from a TFTP server. Therefore, the DHCP server must be configured to respond to option 150 and return the IP address of a TFTP server.

TFTP Server – The TFTP server reported by DHCP option 150 must include the Cisco 1040 binary image, as well as, configurations for each 1040 (either default of specific – see Chapter 3).

Installation Guidelines

- Requirements
- **Installation Guidelines**
- User Security Administration
- Periodic Maintenance
- Helpful Troubleshooting Tips



Installation Guidelines
Options

Standalone Server

- User defined directories
  - Cisco 1040 Images and Configurations
  - Call Metrics Archive

With Operations Manager

- A copy of Service Monitor is installed by default when Operations Manager is installed
- Uses default directories
  - Cisco 1040 Images and Configurations
    - $NMSROOT\data\ProbeFiles
  - Call Metrics Archive
    - $NMSROOT\data\CallMetrics
- Separate license is required to use Service Monitor

Installation Options

A copy of Service Monitor is included with and installed with Operations Manager. In this type of installation the installer is not queried for the directories used to store Cisco 1040 images and configurations or the Call Metrics archive. In this type of installation, these directories can be found under the $NMSROOT\data directory.

The other type of possible installation is a standalone (or sometimes called Remote) installation. In this type of installation the installer is queried for the directory for both the Cisco 1040 files and the Call Metrics archive.

Note(s):

- The Service Monitor installed by default with Operations Manager still requires a separate license for use.

Installation Guidelines

- Use local Administrator account (not cloned account)
- Install on a dedicated platform with static IP Address
- Do not install on:
  - A Primary or Backup Domain Controller
  - A FAT file system
  - An Advanced Server with terminal services enabled in application server mode
  - A system with Internet Information Services (IIS) enabled
  - A system that does not have name lookup
- Verify server requirements and Required and Recommended Service Packs or Patches for operating system are installed (server and client updates exist)

Installation Guidelines

Installation of a standalone Service Monitor should be performed according to the steps detailed in the *Quick Start Guide*. (A link to this guide can be found in Chapter 5 of this tutorial.)

Service Monitor should be installed using the local Administrator (not a cloned account) user account.

If required server patches are missing, the install script prompts whether to continue installation or not. Note that there are required and recommended service packs or patches for clients as well as the server. Remember that client patches are not necessary if the system is used only as a server.

During new installation and upgrade, the user needs to enter the **System Identity Account Password**. System Identity account password has to be the same for all the servers in a multi-server setup. In a multi-server environment, the System Identify Account is used to communicate between the servers for synchronization. (Refer to the CiscoWorks Common Services tutorial for more details.)

The installation script will check for host name resolution. If the host name lookup does not exist, the installation will abort.

If DHCP is enabled on the server, the user is also issued a warning because when the IP address changes, CiscoWorks will no longer work.

If IIS (Microsoft's Internet Information Services) is enabled, the installation will abort due to a port conflict between the Web Server service and IIS. If IIS is disabled, the installation will issue a warning message noting the conflict between the Web Server and IIS.

Installation Guidelines
Continue …

- Verify TCP, UCP ports (listed below) are available for use and not blocked by a firewall
- Refer to Quick Start Guide for IP Communications Service Monitor for installation procedure
  - License file required (refer to next topic for more information on managing licenses)
  - Common Services software will be installed prior to installing Service Monitor (unless it was previously installed with a co-resident Operations Manager)

Installation Guidelines

Refer to the chart below for the ports used by Service Monitor and ensure they are not in use on the server by other applications.

CiscoWorks applications require a license file to be installed. The licensing mechanism is discussed next.

If installing Service Monitor on a standalone server, Common Services will also be installed. Common Services is the foundation software (background services) for all CiscoWorks applications (see Common Services tutorial for more information). If Common Services is already installed from a previously installed CiscoWorks application, ensure that it is the correct version of Common Services required for Service Monitor.

Protocol	Port Number	Service Name
UDP	53	DNS
UDP	67 and 68	DHCP
UDP	69	TFTP—SM uses TFTP to get the config and image files for a given Cisco 1040
UDP	514	Syslog—SM receives Syslog messages from Cisco 1040 sensors
TCP	2000	SCCP—SM uses SCCP to communicate with Cisco 1040 sensors
TCP	43459	Database

Installation Guidelines
Licensing the Service Monitor Software

- Installation ensures a registered and licensed copy of Service Monitor is being installed
- Following license information is shipped with product:
  - Product Identification Number (PIN) – indicates type of install
    - Evaluation Installation – Valid for 90 days
    - Fresh Installation
    - Upgrade Installation
  - Product Authorization Key (PAK) – Used to register product at Cisco.com, a license file is returned.
- Service Monitor will continuously notify the user with a message, once the restricted license limit is reached or exceeded
- Installation procedure will prompt for the location of the license file returned from the registration process.
- If upgrading from evaluation license, enter location of license file at Common Services > Server > Admin > Licensing

Licensing the Service Monitor Software

Service Monitor requires a license to operate. If a license is not installed, Service Monitor operates in Evaluation Mode for 90 days. If the product has not been licensed after the 90 day evaluation period, the product will continue to work, but the user will not have access to key tasks within the product. The user is reminded at each login of the days remaining in the evaluation period.

To obtain a license, the user must register Service Monitor at Cisco.com. Service Monitor is shipped with a Product Identification Number (PIN) indicating the type of install (evaluation, fresh, or upgrade) and a Product Authorization Key (PAK), which is used to register the product at Cisco.com.

The installation will ask you for the location of the license file. To obtain the license file, go to either:

http://www.cisco.com/go/license (registered users) or

http://www.cisco.com/go/license/public (non-registered users)

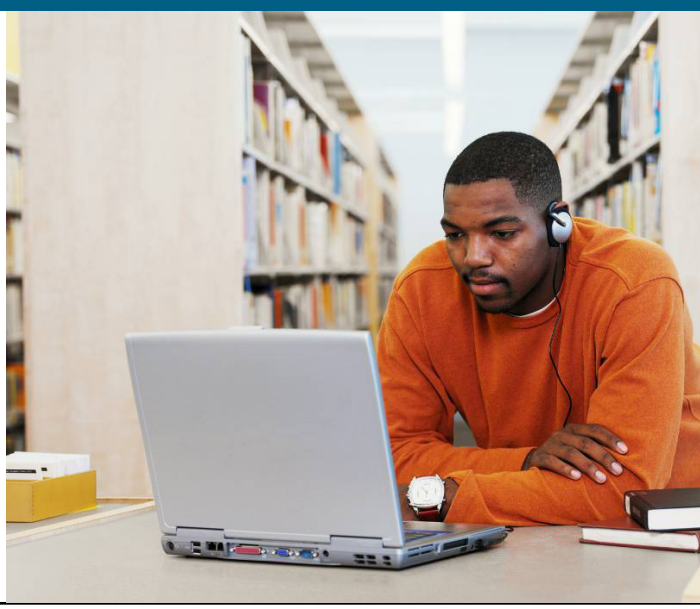
Use the PAK to register the product and download the license file to the server. (Users who are not registered users of Cisco.com can be mailed the license file.

To apply the license after installation (upgrade), secure the license file and go to ***Common Services > Server > Admin > Licensing*** and enter the location of the license file.

<Intentionally Left Blank>

User Security Administration

- Requirements
- Installation Guidelines
- **User Security Administration**
- Periodic Maintenance
- Helpful Troubleshooting Tips



User Security Administration
Login Modes

	Non ACS		ACS
	Common Services	External Module	
Authentication	Common Services	External Module	• ACS • External database integrated with ACS
Authorization	Common Services	Common Services	ACS
User Roles	5 pre-defined static roles	5 pre-defined static roles	• **5 pre-defined roles per application which can be modified** • **Can create new user roles per application**
User Assignment	• One or more per user • Same for all applications	• One or more per user • Same for all applications	• **One per application per user or user group** • **One per Network Device Group per user or user group**

ACS adds increased security and flexibility!

Login Mode

One of the services provided by Common Services is security. Common Services supports two methods for AAA services: Non-ACS and ACS. In the non-ACS mode, several mechanisms are available for user authentication. By default, Common Services performs the authentication check using user accounts added to its local database. The login module can also be set to a number of different external mechanisms (listed in the figure above) to perform the authentication service. Regardless of the mechanism used to perform the authentication service, authorization, or task permission, is always handled by the local accounts in Common Services in the non-ACS mode.

The ACS mode differs from the non-ACS mode in that ACS not only authenticates the user, but also provides the authorization; the local Common Services accounts are not used in this mode. When enabling the ACS mode, the administrator is asked to register the applications with ACS. ACS will now know about the 5 standard user roles (discussed on the next page) and every application and task on the Service Monitor server.

User Security Administration
Pre-defined User Roles

- User roles determine the tasks that can be performed by a user
- User profile defines 1 or more user roles

System Administrator	Server configuration and user accounts
Network Administrator	Device configuration
Network Operator	Backup for most configuration management tasks
Approver	Approve jobs that change device software or configuration
Help Desk	View reports (Default User Role – assigned to all users)

- Tasks displayed on desktop change depending on user's assigned role(s)

Pre-defined User Roles

Service Monitor contains many critical tasks that can modify the behavior of a network, as well as, many totally benign tasks that simply display information. Obviously, it would not be wise to allow all types of users access to the critical functions, but at the same time it would be beneficial to allow all types of users access to the basic information. To allow for proper access to all types of users, Service Monitor employs the concept of User Roles (also known as user privileges or permissions). Use of the various functions or tasks is based upon the "roles" assigned to user accounts. In fact, if a task is not permitted to the user role assigned to the logged in user, then that task will not even be displayed in the navigation tree of the application.

Service Monitor uses five standard User Roles; the five user roles and their basic access ability are:

System Administrator – Can perform Service Monitor system administration tasks

Network Administrator – Can perform all Service Monitor tasks

Network Operator – Can perform all Service Monitor tasks

Approver – Not used in Service Monitor

Help Desk – View only

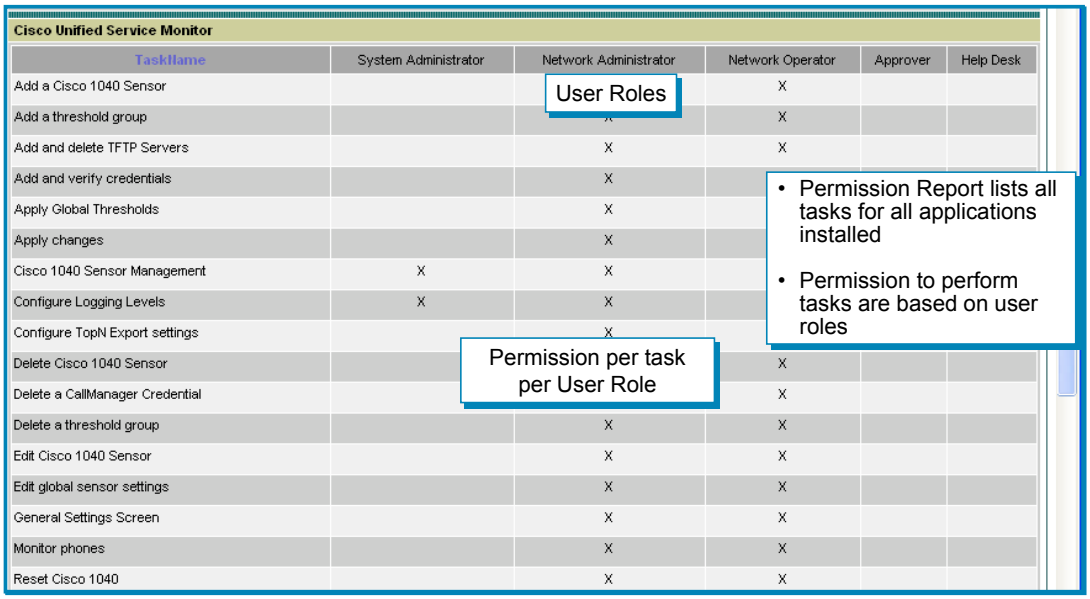
In Non-ACS mode (local server authorization) users can be assigned more than one user role, and all are assigned the basic user role – Help Desk. The roles cannot be modified. See next page for user roles assigned to Service Monitor tasks.

In ACS mode (authorization provided by ACS) users can only be assigned one user role per application (basic configuration), but new user roles can be created. Also for further flexibility, user roles can also be assigned per ACS Network Device Group (NDG) per application.

For more information on Security Services provided by Common Services, see the Common Services tutorial.

User Security Administration
Permission Report

To view report: Common Services > Server > Reports > Permission Report



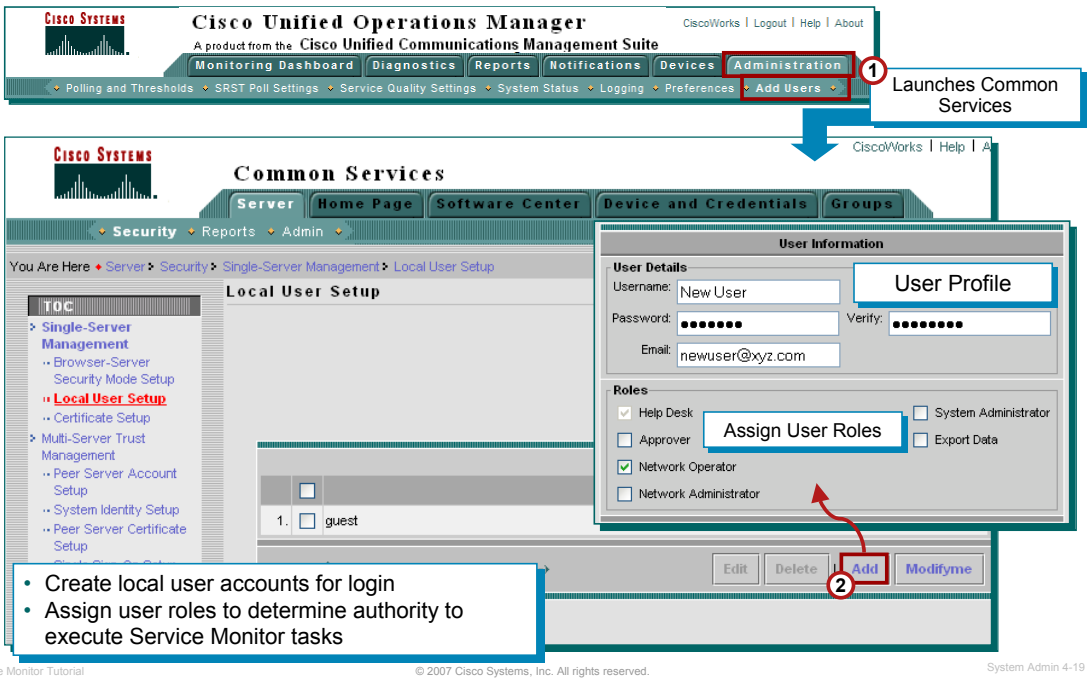
Permission Report

In the Non-ACS mode, the tasks that are executable by a user role are static and cannot be changed. Common Services includes a report that displays every task for every application on the local server and which user roles have permission to execute it.

To view the Permissions Report, select ***Common Services > Server > Reports***, on the dialog displayed select **Permissions Report** and click **Generate**.

The above picture displays the Permission Report for Service Monitor.

User Security Administration
Creating Users (Common Services Authentication)



Creating Users (Common Services Authentication)

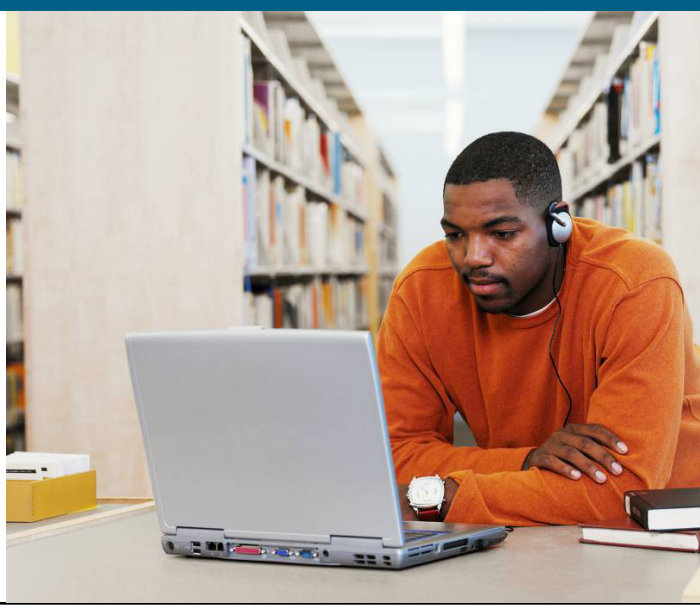
Common Services allows users with the System Administration user role to create user accounts and assign user roles to the account. Creating a new user is simple and straight forward using the ***Common Services > Server > Security > Single-Server Management > Local User Setup*** task. A dialog is displayed listing all the currently defined users, click **Add** to create a new user. Simply enter a name and password for the account and assign the user roles that this user is to have. The E-mail address is optional for all user roles except Approver (E-mail is how some scheduled jobs inform an Approver user of a job to approve – See RME tutorial or User Guide for more information about approving jobs).

All users can view their account using the same task, except selecting **ModifyMe** instead of **Add**. Only the password and e-mail address can be modified by user without the System Administrator user role.

<*Intentionally Blank*>

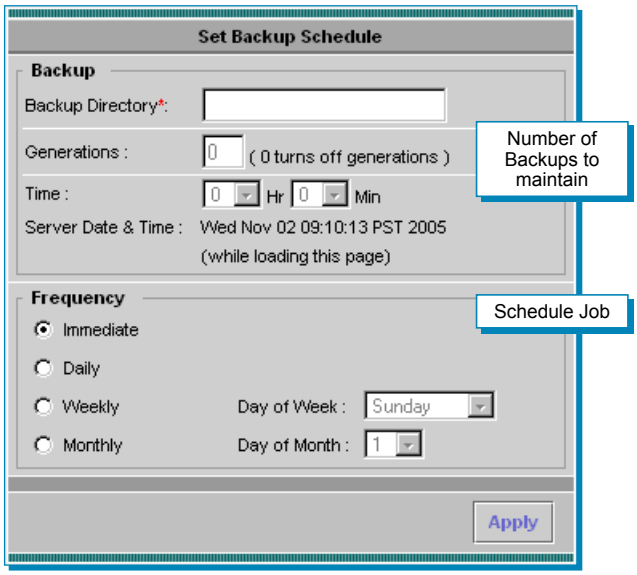
Periodic Maintenance

- Requirements
- Installation Guidelines
- User Security Administration
- **Periodic Maintenance**
- Helpful Troubleshooting Tips



Periodic Maintenance
Database

Common Services > Server > Admin > Backup



- Backup the database on a regular basis
- CLI can also be used to generate backups (see notes for perl script to run)

Database Management

It is important that the Service Monitor database be periodically backed up. The system administrator can schedule immediate, daily, weekly, or monthly automatic database backups. The database should be backed up regularly so that you have a safe copy of the database.

To perform an immediate backup or schedule a new one, follow these steps:

1. Go to ***Common Services > Server > Admin > Backup***. The Set Backup Schedule dialog box appears.
2. Enter the location of the Backup Directory. It is recommend that your target location be on a different partition than where Service Monitor is installed.
3. Enter the number of backup Generations to be stored in the backup directory
4. Enter the Time for the backup to occur. Use a 24-hour format.
5. Enter the Frequency for the backup schedule to be one of the following:
    - *Immediately* - The database is backed up immediately
    - *Daily* - The database is backed up every day at the time specified
    - *Weekly* - The database is backed up once a week on the day and time specified. Select a day from the Day of week list.
    - *Monthly* - The database is backed up once a month on the day and time specified. Select a day from the Day of month list.

Periodically, examine the log file at the following location to verify backup status:

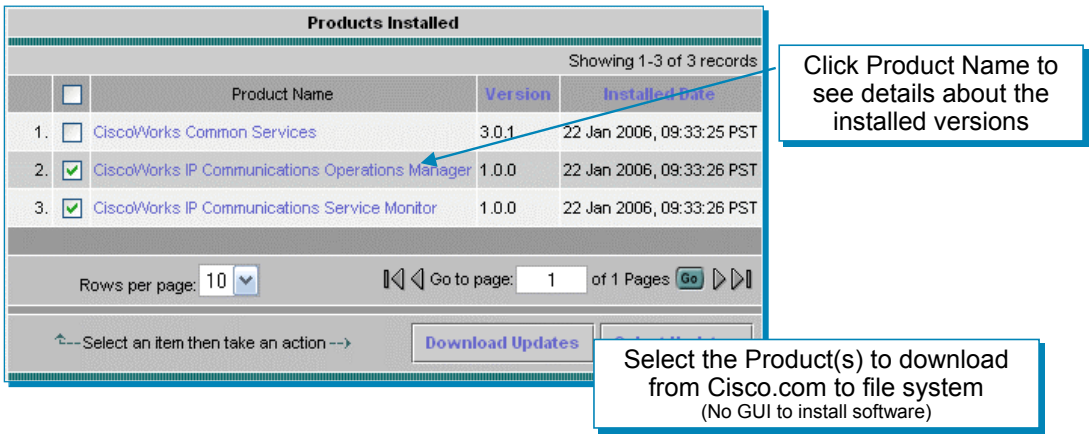
NMSROOT/log/dbbackup.log

Note: You can Backup data using CLI by running the following command:

$NMSROOT/bin/perl $NMSROOT/bin/backup.pl <BackupDirectory> [LogFile] [Num_Generations]

Periodic Maintenance
Software Updates

Common Services > Software Center > Software Update



Software Updates can be found at the following links, then click Download Software:
- http://www.cisco.com/en/US/products/ps6535/index.html (Operations Manager)
- http://www.cisco.com/en/US/products/ps6536/index.html (Service Monitor)

Software Updates

Cisco is continually striving to enhance the software and add support for new devices. Typically, Cisco releases a new service pack on a quarterly basis containing these features. Common Services contains a task that allows the server to check Cisco.com for any updates and download them to the server for subsequent installation.

When accessing the ***Common Services > Software Center > Software Updates*** task a dialog is displayed showing the bundles and individual applications installed. Clicking on an application will give the details about the Applications and Packages installed with a *Product* page that gives the details of the installed applications, patches, and packages of the product.

To download updates for selected applications, select the desired applications and click the **Download Updates** button. The user will then be prompted for a location on the server to download any updates to. If the user wishes to first select which updates to actually download, click the **Select Updates** button which will present a list of available updates for the selected applications.

Note: Each software update is accompanied by a readme file which will provide steps for installation. Software updates are done from a server command line and not the Service Monitor GUI.

Periodic Maintenance
Cisco 1040 Image Updates

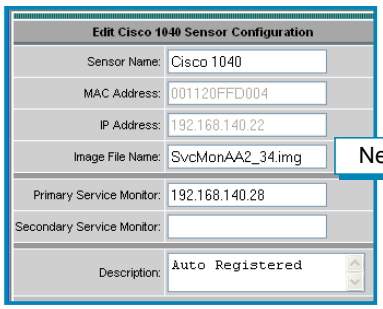
Step 1 - Download new image from Cisco.com

www.cisco.com/support

Step 2 – Update the Cisco 1040 configuration(s)

- Default config
- Individual sensor configs

Default: Service Monitor > Configuration > Sensors > Setup
Individual: Service Monitor > Configuration > Sensors > Management



New image name

Continued on next page

Cisco 1040 Image Updates

Periodically, Cisco may release an update to the binary image of the Cisco 1040 sensors. To use the new image, execute the following 4 steps:

1. **Download New Image from Cisco.com** – The new image can be found by following the downloads link at Cisco.com. Select **Network Management > CiscoWorks downloads** and then navigate to the IP Communications page. The downloaded image should be placed in the image directory of the SM server defined during install.
2. **Update Cisco 1040 Configuration** – The Cisco 1040 configurations needs to be updated to reflect the use of a new image. Depending on how the original configuration was created will dictate which task to use to update the configuration. If all Cisco 1040s use the default configuration, then simply update the *Image Filename* field in the ***IP Communications Service Monitor > Service Monitor Operations > Default Configuration*** task.

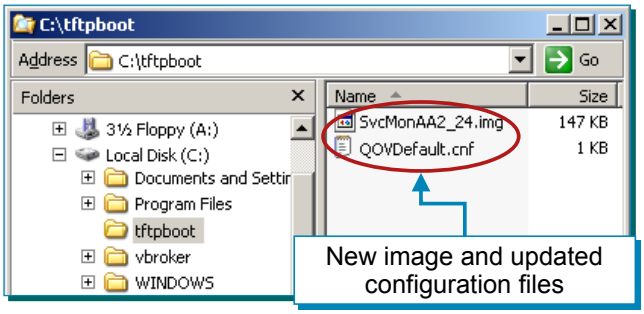
   If a specific configuration was generated for each Cisco 1040 ,then edit their configuration files individually using the ***IP Communications Service Monitor > Service Monitor Operations > Cisco 1040 Management*** task. Select the Cisco 1040 configuration to edit, select **Edit** and update the *Image Filename* field.

Continued on next page…

Periodic Maintenance
Cisco 1040 Image Updates (Continued)

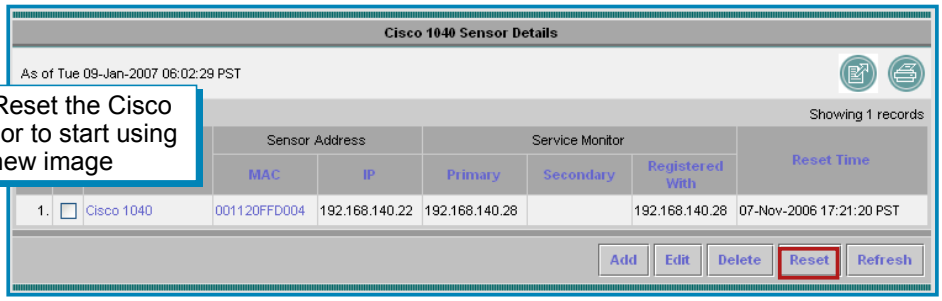
Step 3 - Copy new image file to the TFTP server.

Config file changes are automatically copied to the TFTP server.



Service Monitor > Configuration > Sensors > Management

Step 4 – Reset the Cisco 1040 sensor to start using the new image

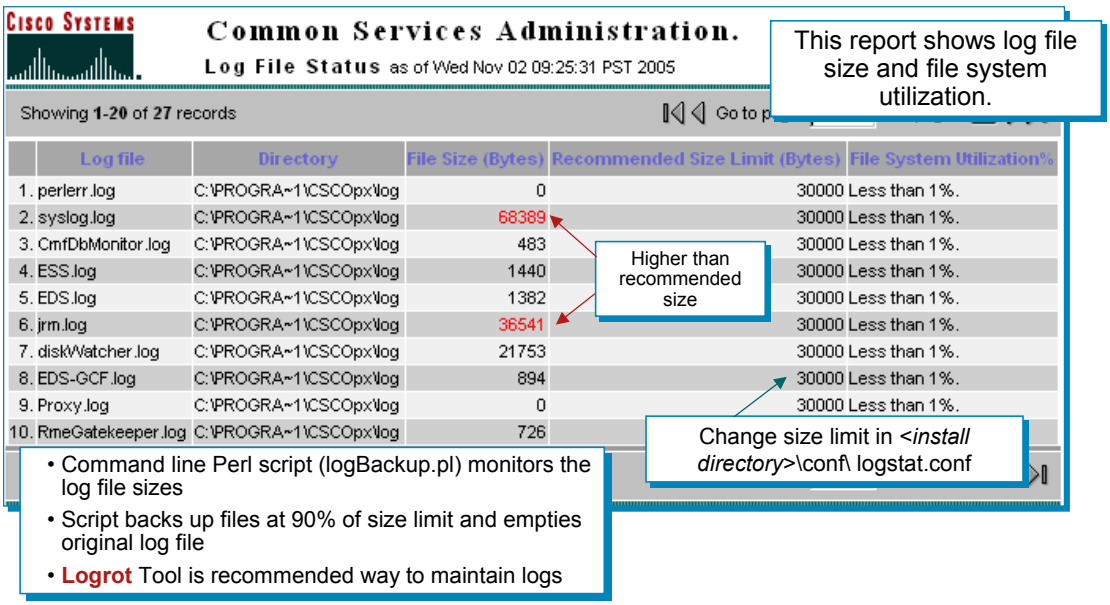


Cisco 1040 Image Updates

3. **Copy Image and Updated Configuration to TFTP Server** – The Cisco 1040 sensors retrieve their image and configuration files from the TFTP server. Therefore, the new image file and updated configuration(s) need to be copied to the TFTP server.
4. **Reset the Cisco 1040** – To have the Cisco 1040 sensors begin using their new image and configuration, they need to be reset to force them to retrieve these items from the TFTP server. To reset a Cisco 1040 use the ***IP Communications Service Monitor > Service Monitor Operations > Cisco 1040 Management*** task. Select the Cisco 1040 to be reset and click the **Reset Cisco 1040** button. After a short amount of time, the *Status* should return to *Registered*.

Periodic Maintenance
Log Files – Common Services

Common Services > Server > Reports > Log File Status



Log File Management – Common Services

Log files can grow and fill up disk space. There are ways to view the logs, their size, and locations, as well as ways to control their growth.

Using the Log File Status task, you can view information on all the log files used by Service Monitor.

File Size displayed in red means the file exceeds its size limit. File System Utilization displayed in red means the file exceeds 90% utilization. You should reduce the size of your log files if your file system utilization is over 90%.

Since log files can grow and fill up disk space, there is a Perl script (logBackup.pl) that enables you to control this growth by backing up the log file and clearing it. Only log files that reach 90% of their size limits are backed up and the original log file is emptied.

Stop all Service Monitor processes first before using the script.

Files maintained by this script include the Daemon Manager and Daemon process log files. Most log files are located in directories in the PX_LOGDIR directory - %NMSROOT% /log.

Logrot Utility

The **logrot utility** helps you manage the log files in a better fashion **and is the recommended approach**. Logrot is a log rotation program that can:

- Rotate log when Service Monitor is running
- Optionally archive and compress rotated logs
- Rotate log only when it has reached a particular size

Logrot helps add new files easily. Logrot should be installed on the same machine where you have installed Common Services. To configure Logrot, refer to the Common Services User Guide, Configuring the Server.

Periodic Maintenance
Syslog File

- If the Syslog file becomes too big, Service Monitor stops processing MoS messages from the 1040s
- To maintain just the Syslog file:

1. Stop the Syslog daemon

   ```
   net stop crmlog
   ```

2. Stop the CiscoWorks daemon manager

   ```
   net stop crmdmgtd
   ```

3. Delete the syslog.log file

   ```
   $NMSROOT\log\syslog.log
   ```

4. Start the Syslog daemon

   ```
   net start crmlog
   ```

5. Start the CiscoWorks daemon manager

   ```
   net start crmdmgtd
   ```


Syslog File

Syslog messages are used by the Cisco 1040s to communicate MOS values for active calls. If the syslog file on the Service Monitor server becomes too large, Service Monitor may stop processing messages. Therefore, it is extremely important to maintain the syslog file. Although the tools described on the previous page could be used, the steps listed below can be used specifically for the syslog file:

1. **Stop the Syslog Daemon**– from a Command Prompt enter ***net stop crmlog*** and wait for the DOS prompt to return
2. **Stop the CiscoWorks Daemon Manager** – from a Command Prompt enter ***net stop crmdmgtd*** and wait for the DOS prompt to return.
3. **Delete the Syslog.log File** – found in the $NMSROOT\log directory. The server will create a new one.
4. **Start the Syslog Daemon**– from a Command Prompt enter ***net start crmlog*** and wait for the DOS prompt to return
5. **Start the CiscoWorks Daemon Manager** – from a Command Prompt enter ***net start crmdmgtd***.

   Note(s):

   - The Command Prompt will return fairly quickly after entering the net start command, but the actual start-up process will take 5-10 minutes. (Use Task Manager to see the resource usage during the start-up process.) Trying to access the server before then will result in an error message.

Periodic Maintenance
History Log File

- The history log file, ServiceMonitorHistory.log, contains records of Cisco 1040 events such as resets, configuration updates, and errors.
- If the History log file becomes too large:

1. Stop the CiscoWorks daemon manager

```
net stop crmdmgtd
```

2. Rename it to enable Service Monitor to start a fresh history log

```
$NMSROOT\log\qovr\ServiceMonitorHistory.log
```

3. Start the CiscoWorks daemon manager

```
net start crmdmgtd
```


History Log File

Log file specific to Service Monitor and its operations can be found in the *$NMSROOT\log\qovr directory*. One log file in this directory that requires periodic maintenance is the ServiceMonitorHistory.log file. This log contains information about the activities of the Cisco 1040s. If this file becomes too large, rename it and the system will create a new one.

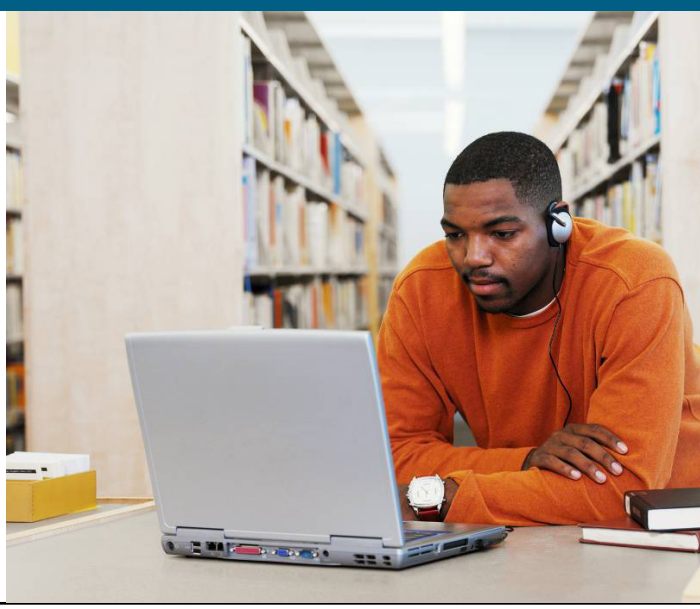
1. **Stop the CiscoWorks Daemon Manager** – from a Command Prompt enter ***net stop crmdmgtd*** and wait for the DOS prompt to return.
2. **Rename the ServiceMonitorHistory.log File** – found in the $NMSROOT\log\qovr directory. The server will create a new one.
3. **Start the CiscoWorks Daemon Manager** – from a Command Prompt enter ***net start crmdmgtd***.

Note(s):

- The Command Prompt will return fairly quickly after entering the net start command, but the actual start-up process will take 5-10 minutes. (Use Task Manager to see the resource usage during the start-up process.) Trying to access the server before then will result in an error message.

Helpful Troubleshooting Tips

- Requirements
- Installation Guidelines
- User Security Administration
- Periodic Maintenance
- **Helpful Troubleshooting Tips**



Helpful Troubleshooting Tips
Cisco 1040 Lights

Amber Flashing – Obtaining information from DHCP, accessing TFTP, retrieving configuration and image files

Yellow – Registration in Progress

Green – Registered to Primary Service Monitor

Green Flashing – Registered to Secondary Service Monitor

Service Monitor Tutorial System Admin 4-30

Cisco 1040 Lights

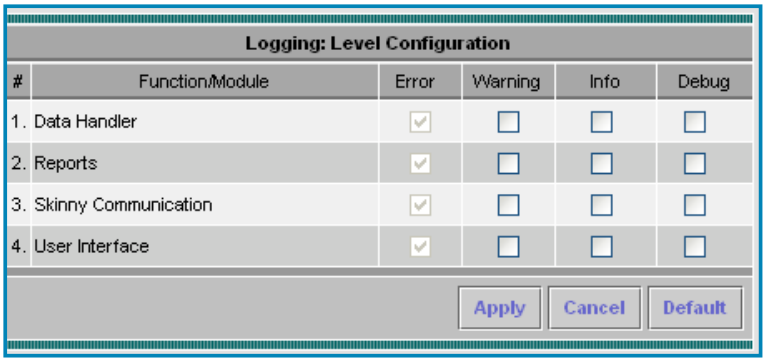
The status indicator light on the front panel of the Cisco 1040 indicates what the Cisco 1040 is currently doing. Knowing the meaning of the lights can help troubleshoot the sensor.

When the Cisco 1040 is first being brought on-line, the status light will be flashing an Amber color. It is during this time that the Cisco 1040 is receiving necessary communication information from the DHCP server, and accessing and retrieving necessary files from the TFTP server.

The next step for the Cisco 1040 is to register with the primary Service Monitor indicated in the configuration file (Status light = yellow). If the primary is not available, the Cisco 1040 will also try the secondary and tertiary Service Monitors, if specified. If the Cisco 1040 is unable to register, it will return to the flashing amber state and attempt to re-retrieve information from the TFTP server. If the Cisco 1040 successfully registers to the primary Service Monitor, the status light will be a solid green. If it registers to a secondary or tertiary Service Monitor, the status light will be a flashing green. When the primary is available again, the Cisco 1040 will register with it and the light will become a solid green.

Helpful Troubleshooting Tips
Log Files – Service Monitor

Service Monitor > Administration > Logging



SM Log File Location:
$NMSROOT/log/qovr

- By default, Service Monitor writes only error and fatal messages to log files.
- Collect more data when needed by increasing the logging level.

Log File Management – Service Monitor

Service Monitor writes application log files for all major functional modules. By default, Service Monitor writes only error and fatal messages to log files. Each module writes to its own folder within the <*NMSROOT*>\log\itemLogs folder. You cannot disable logging. However, you can collect more data when needed by increasing the logging level and return to the default logging level.

To change the logging level, select **Administration > Logging**. Remember, you cannot disable logging. Service Monitor will always write error and fatal messages to application log files. For each Service Monitor functional module, the Error check box is always selected; you cannot deselect it. To change the logging level for individual modules, simply select one (or deselect all) of the following logging levels for each module that you want to change:

- Warning--Log error messages and warning messages
- Info--Log error, warning, and informational messages
- Debug--Log error, warning, informational, and debug message

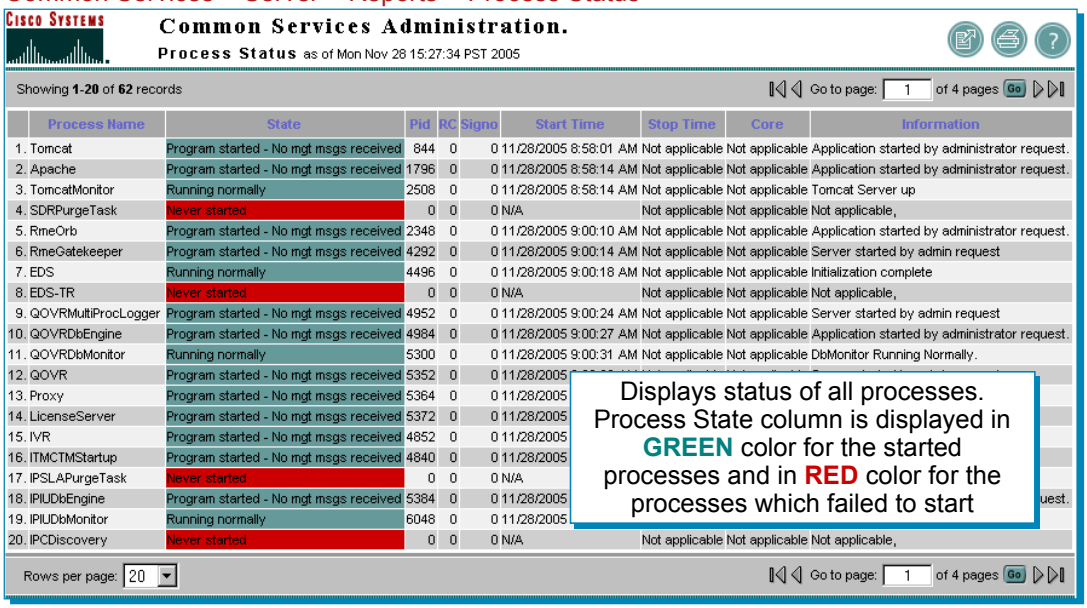
Review your changes. To cancel your changes, click the **Cancel** button. Otherwise, click the **Apply** button. Clicking the **Apply** button starts immediately resetting the changed logging levels for the Service Monitor functional modules.

Notes(s):

- *NMSROOT is the folder where Service Monitor is installed on the server. If you selected the default directory during installation, it is C:\Program Files\CSCOpx.*
- *When a log file reaches a preset maximum size, the module backs up the file and starts writing to a new log file. The maximum size for a log file varies by module. The maximum number of backed up log files that a module keeps also varies.*
- *Service Monitor does not automatically reset the DFMServer log file (DFM.log). To maintain good system performance, back up this file when it grows larger than 30 MB. (Refer to the online help,* ***Maintaining the DFM Log File"*** *for more information on stopping/starting the processes and resetting the file.)*

Helpful Troubleshooting Tips
Process Status

Common Services > Server > Reports > Process Status



* Note: Red state may be normal – see Information column

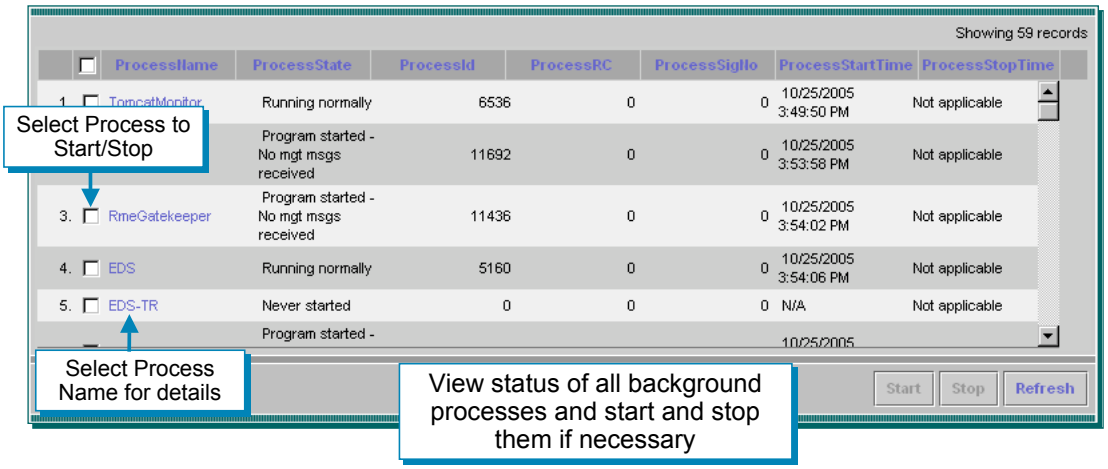
Process Status

Process Status is a Common Services task used to manage all background processes. This report displays the status of all processes. Process State column is displayed in **GREEN** color for the started processes and in **RED** color for the processes which failed to start.

The processes can be viewed by running the ***Common Services > Server > Report > Process Status*** task.

Helpful Troubleshooting Tips
Process Management

Common Services > Server > Admin > Processes



To "restart" all processes – open a Command prompt on the server and enter:
To stop all processes: net stop crmdmgtd
To restart all processes: net start crmdmgtd

Process Management

Process Management is a Common Services task used to monitor and start/stop one or more background processes. In the event something doesn't quite seem right with Service Monitor, the system administrator should first check the processes to ensure that they are running. If not, they can be restarted, or stopped and restarted, in an attempt to fix the problem.

The processes can be viewed by running the ***Common Services > Server > Admin > Processes*** task.

Process Name, State, PID, RC, SigNo.,Start Time and Stop Time are displayed. Core and Information field are not displayed here.

The "Refresh" button is for refreshing the entries in the table.

The Tomcat and Apache processes can not be stopped from this display since communication would be cut between the server and the browser.

To shut down all Service Monitor processes, open a Command Prompt on the server and enter:

net stop crmdmgtd

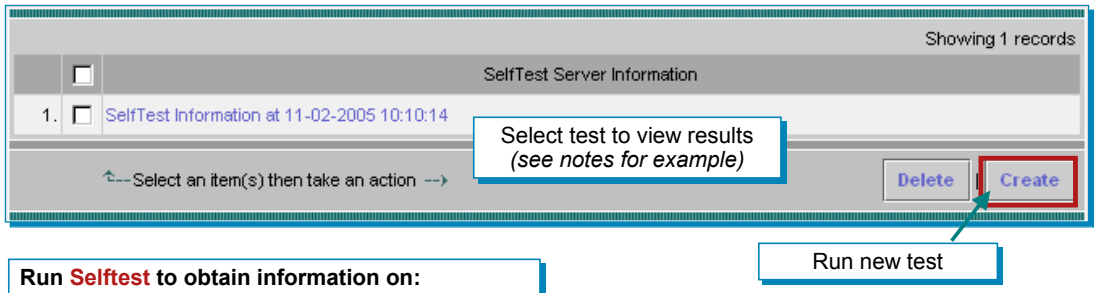
To restart all the Service Monitor processes enter:

net start crmdmgtd

Note: the command prompt will return fairly quickly after entering the net start command, but the actual start-up process will take 5-10 minutes (Use Task Manager to see the resource usage during the start-up process).

Helpful Troubleshooting Tips
Server Self-Test

Common Services > Server > Admin > Selftest



Run Selftest to obtain information on:

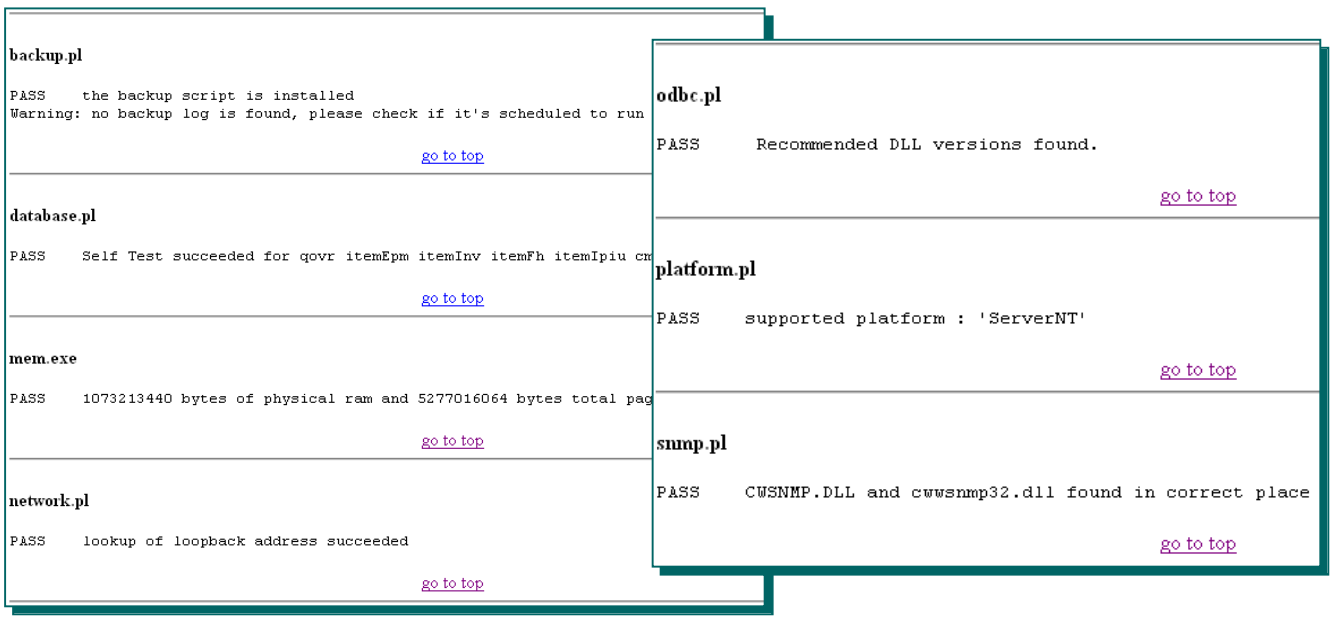
- Backup script available and if scheduled
- Test on database processes
- Check on available memory
- Test of lookback address
- Check on recommended DLL versions
- Check platform type supported
- Check SNMP processes

Server Self-Test

The Selftest option can display and create self-test reports. You can use this option to test the health and integrity of the system. The option executes various Perl scripts and reports whether or not the test passed or failed. Your login and user role determines whether you can use this option.

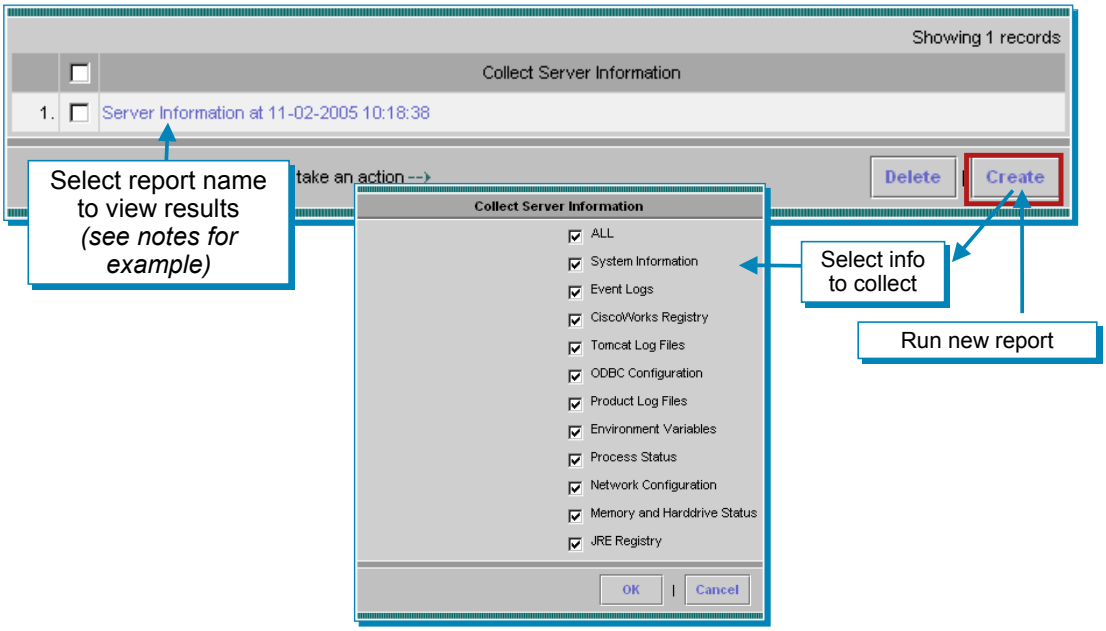
Launch the task by selecting ***Common Services > Server > Admin > Selftest***. To create a new report, click **Create**. To display the new report or a previously generated report, click the report name. Self-test reports indicate whether the tests passed or failed. Reports reflect the server time.

Excerpts from a selftest report are illustrated below.



Helpful Troubleshooting Tips
Collect Server Information

Common Services > Server > Admin > Collect Server Information



Collect Server Information

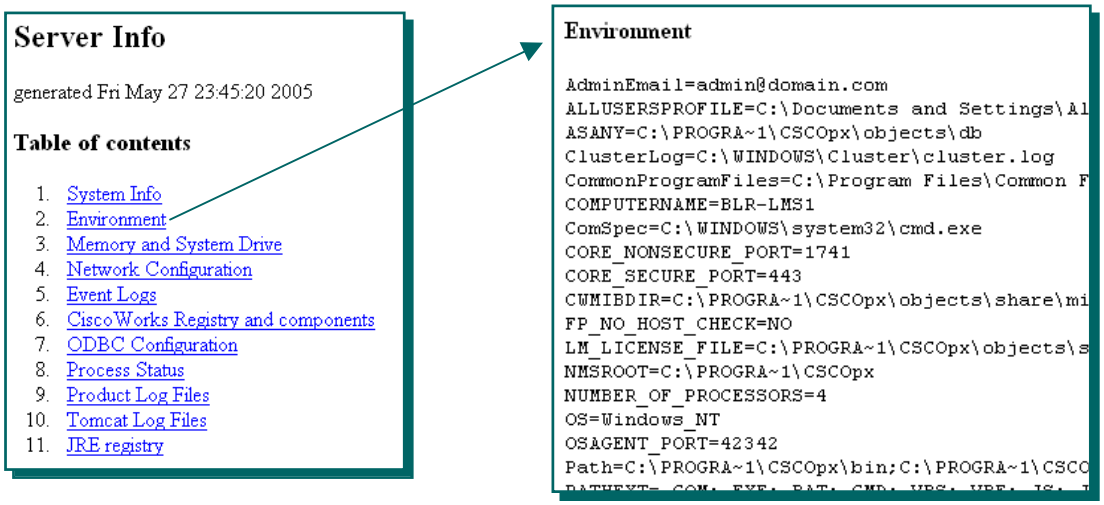
The System Administrator can gather troubleshooting information about the status of the server using this option. (*A command line script is also available at …/CSCOpx/bin/collect.info*). If you collect server information through the user interface, data is stored in …/CSCOpx/htdocs/collect.

The user's login and user roles determines whether you can use this option. (See Permissions Report)

Launch the task by selecting ***Common Services > Server > Admin > Collect Server Information***. To create a new report, click **Create**. A list of report modules and options are displayed. Select the modules you want to include and click **OK**. By default, all the modules are selected.

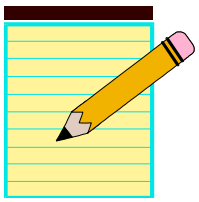
To display a report, click its name in the list of available reports. The report appears with information about the product database, the operating system, disk utilization statistics, Tomcat log files and so on. Reports reflect the server time.

Excerpts from a report are illustrated below.



Helpful Troubleshooting Tips
MDC Support Utility

- MDC provides diagnostics results valuable to a Cisco Technical Assistance Center (TAC) representative
- MDC collects the following information and compresses it into a single file to support the MDCs installed
  - Log Files
  - Configuration Settings
  - Memory Information
  - Complete System Information
  - Process Status
  - Host Environment



MDC Support Utility

The MDC Support utility collects log files, configuration settings, memory info, complete system related info, process status and host environment information. It also collects any other relevant data, into a deliverable tar (compressed form) file to support the MDCs installed.

The MDC Support utility also queries CCR for any other support utilities registered, and runs them. Other MDCs need to register their own support utilities that will collect their relevant data.

Windows:

- Go to: $NMSROOT\MDC\bin\
- Run: MDCSupport.exe

  The utility creates a tar file in $NMSROOT\MDC\etc directory. If \etc directory is full, or if you want to preserve the data collected previously by not over writing the tar file, you may create another directory by running the following command:
- MDCSupport.exe Directory

Before you close the command window, ensure that the MDC Support utility has completed its action. If you close the window prematurely, the subsequent instances of MDCSupport Utility will not function properly. If you happen to close the window, delete the mdcsupporttemp directory from $NMSROOT\MDC\etc directory, for subsequent instances to work properly.

Thank You!

We hope that you have enjoyed using Cisco Unified Service Monitor and have found its features to be an important part of your network-management toolkit.

Cisco Systems

<Intentionally Left Blank>

Cisco Unified Service Monitor

References

Chapter 5

Reference Materials

Many Cisco reference documents have been created to help users understand the use of Cisco Unified Service Monitor (SM). However, finding help and documentation can often be a challenge. This reference chapter has been created to assist you in your pursuit of additional product information. Below are links to documents and Web pages that provide further details on Cisco Unified Service Monitor.

- **Cisco Unified Service Monitor (SM)**

  - **Product Home Page (URL)**

    http://www.cisco.com/en/US/products/ps6536/tsd_products_support_series_home.html

  - **Data Sheet (URL)**
    http://www.cisco.com/en/US/products/ps6536/products_data_sheets_list.html

  - **Install and Upgrade Guides – Cisco 1040 Sensor and SM (URL)**

    http://www.cisco.com/en/US/products/ps6536/prod_installation_guides_list.html

  - **Release Notes (URL)**

    http://www.cisco.com/en/US/products/ps6536/prod_release_notes_list.html

  - **User Guide (URL)**

    http://www.cisco.com/en/US/products/ps6536/products_user_guide_list.html

  - **Frequently Asked Questions (URL)**

    http://www.cisco.com/en/US/products/ps6536/prod_qandas_list.html

  - **Deployment Guide (URL)**

    http://www.cisco.com/en/US/products/ps6535/prod_presentation_list.html

- **Other Related Material**

  - **Cisco Unified Operations Manager (URL)**

    http://www.cisco.com/en/US/products/ps6535/index.html

  - **IP Communications and Voice Solutions (URL)**

    http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/networking_solutions_packages_list.html

  - **IEEE 802.3 Inline Power (URL)**

    http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/networking_solutions_audience_business_benefit09186a0080154647.html

  - **Deployment of QoS in Converged Networks (PDF)**

    http://www.cisco.com/application/pdf/en/us/guest/tech/tk759/c1482/cdccont_0900aecd8019f3e0.pdf

  - **QoS Configuration and Monitoring White Papers (URLs)**

    http://www.cisco.com/en/US/products/ps6558/prod_white_papers_list.html

    http://www.cisco.com/en/US/tech/tk543/tk759/tech_white_papers_list.html

  - **Network Professionals Connection (URL)** <*Select Network Management*>

    http://forums.cisco.com/eforum/servlet/NetProf?page=main

  - **Cisco's SNMP Object Navigator (URL)**

    http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

- **Online Bug Tracker**

  Search for known problems on the Cisco bug tracking system tool, called Bug Toolkit.
  To access Bug Toolkit, perform the following steps:
  - Click on the link above (www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)
  - Login to Cisco.com
  - Click ***Launch Bug Toolkit***.
  - Locate Service Monitor from the list of Cisco Software Products
  - Then click ***Next***.

- **Technical Notes / White Papers**
  - **Network Management Systems: Best Practices White Paper (URL)**

    http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800aea9c.shtml

    The objective of this paper is to provide some deployment guidelines for all areas of network management: Fault, Configuration, Accounting, Performance, and Security (FCAPS).