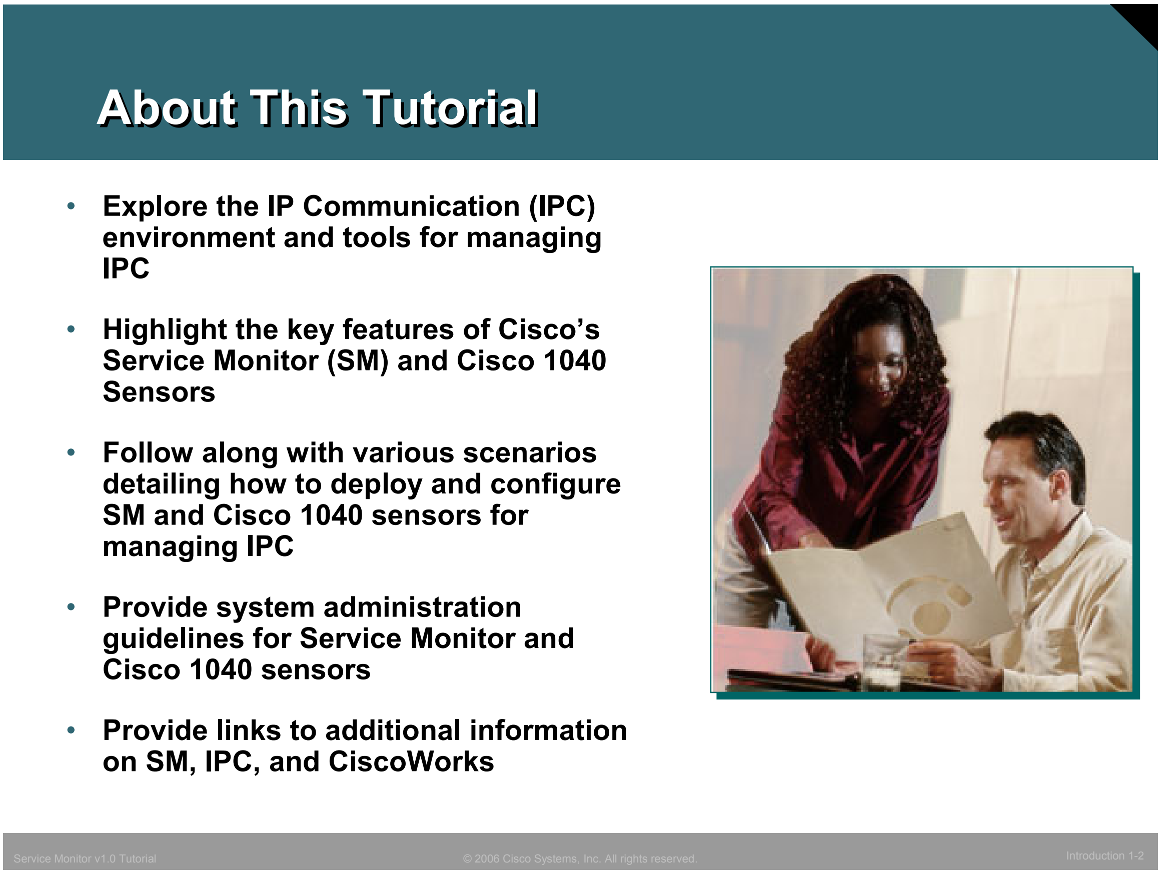
Cisco Systems

Service Monitor

Tutorial

Release 1.0



About This Tutorial

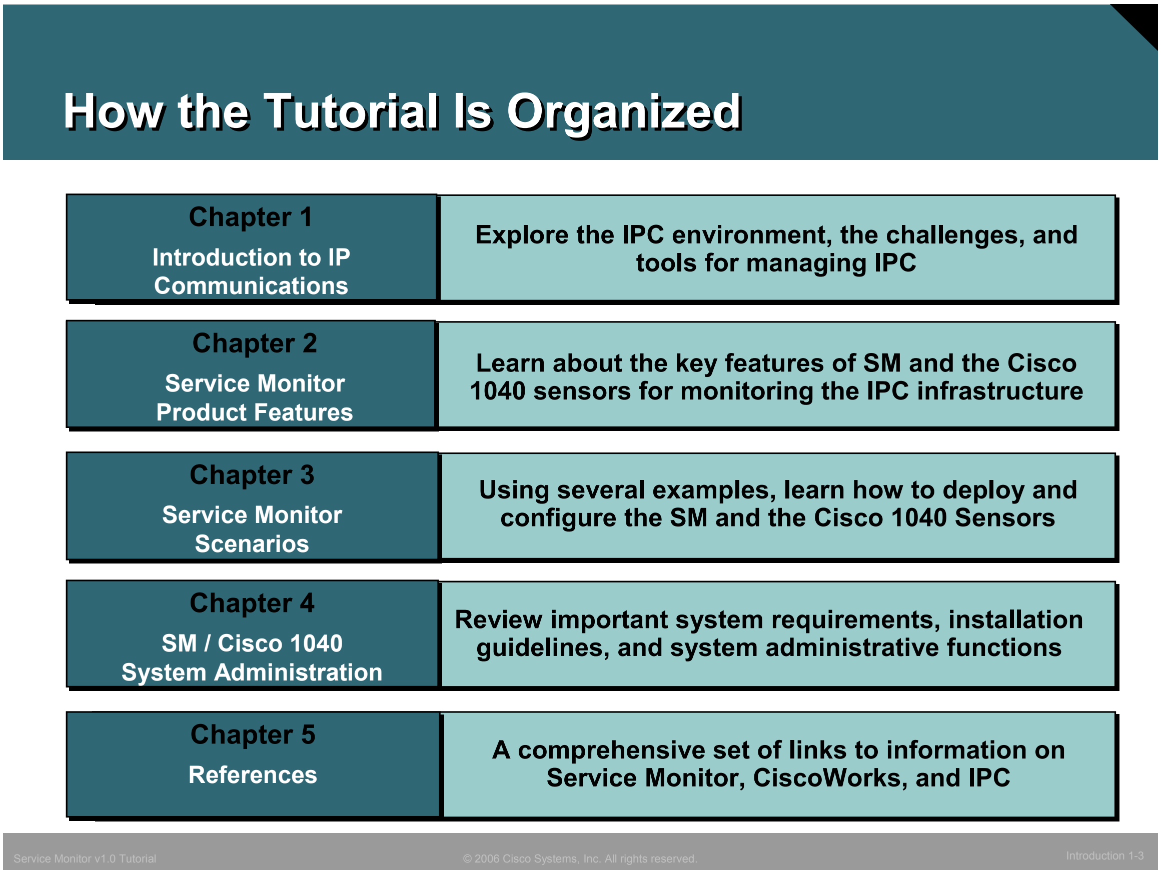
- Explore the IP Communication (IPC) environment and tools for managing IPC
- Highlight the key features of Cisco's Service Monitor (SM) and Cisco 1040 Sensors
- Follow along with various scenarios detailing how to deploy and configure SM and Cisco 1040 sensors for managing IPC
- Provide system administration guidelines for Service Monitor and Cisco 1040 sensors
- Provide links to additional information on SM, IPC, and CiscoWorks

About This Tutorial

Welcome to the Service Monitor (SM) v1.0 tutorial! This tutorial provides self-paced training focused on using the key features of Service Monitor and the Cisco 1040 sensors.

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 to IP Communications	Explore the IPC environment, the challenges, and tools for managing IPC
Chapter 2 Service Monitor Product Features	Learn about the key features of SM and the Cisco 1040 sensors for monitoring the IPC infrastructure
Chapter 3 Service Monitor Scenarios	Using several examples, learn how to deploy and configure the SM and the Cisco 1040 Sensors
Chapter 4 SM / Cisco 1040 System Administration	Review important system requirements, installation guidelines, and system administrative functions
Chapter 5 References	A comprehensive set of links to information on Service Monitor, CiscoWorks, and IPC

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-3

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.

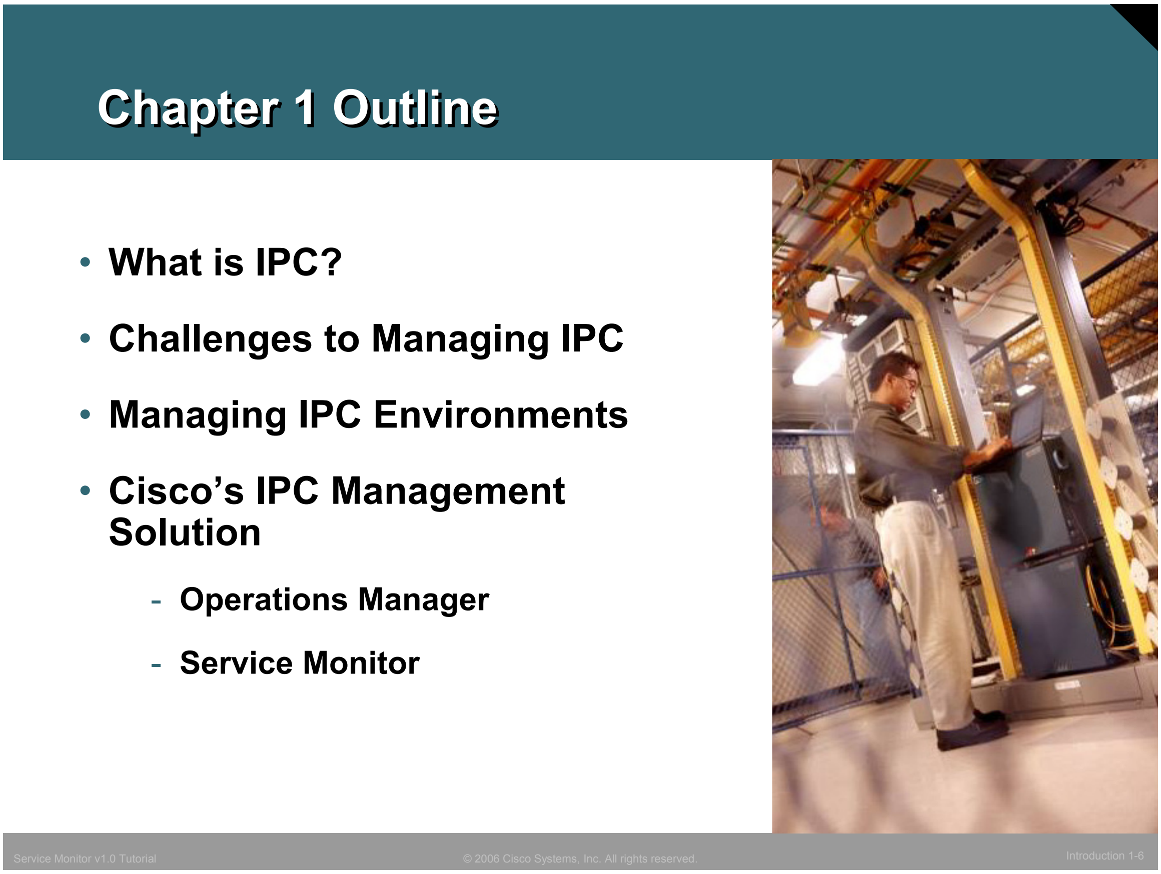
Chapter 5: References

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

<Intentionally Left Blank>

Introduction to IP Communications

Chapter 1



Chapter 1 Outline

- What is IPC?
- Challenges to Managing IPC
- Managing IPC Environments
- Cisco’s IPC Management Solution
  - Operations Manager
  - Service Monitor

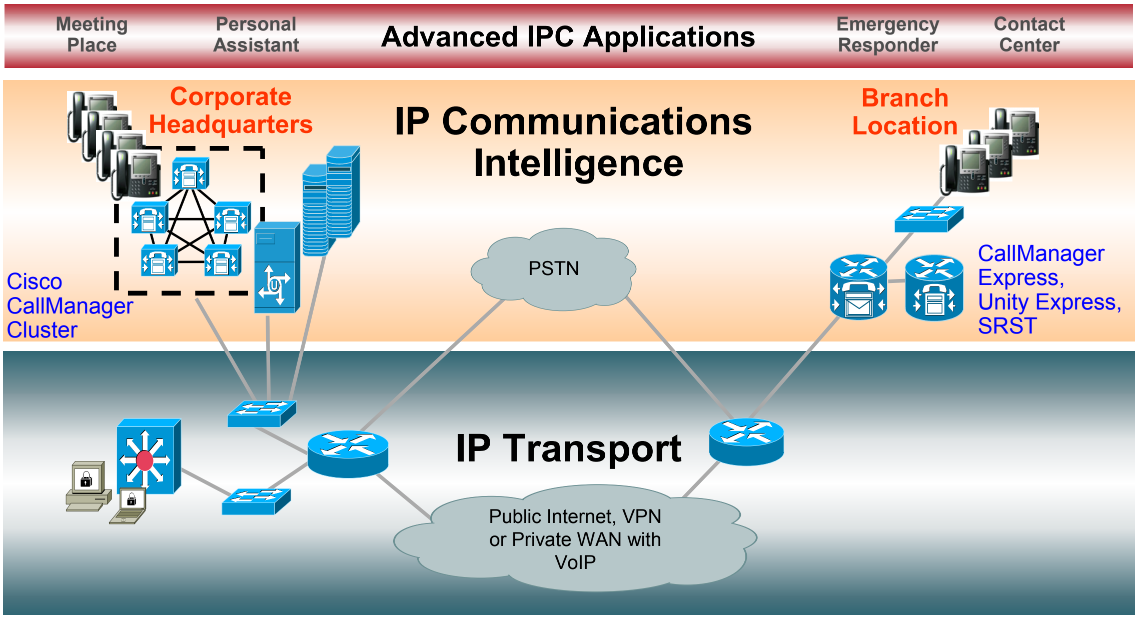
Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-6

Chapter 1 Outline

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

What is IPC?


Meeting Place
Personal Assistant
Advanced IPC Applications
Emergency Responder
Contact Center
Corporate Headquarters
IP Communications Intelligence
Branch Location
Cisco CallManager Cluster
PSTN
CallManager Express, Unity Express, SRST
IP Transport
Public Internet, VPN or Private WAN with VoIP

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-7

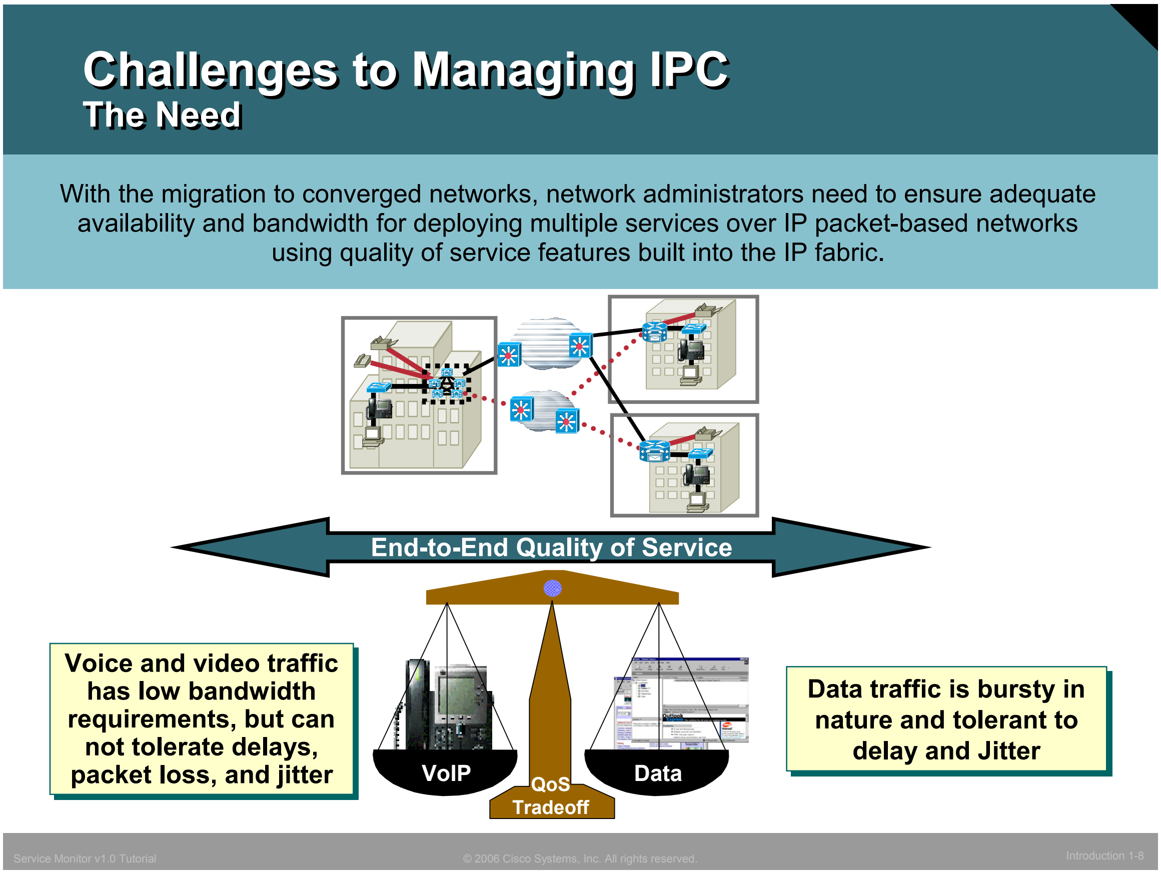
What is IPC?

Not long ago, IP Communications (IPC) was synonymous with IP telephony, and organizations adopted it primarily to save money on phone bills and network support. But today, IPC 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 IPC environment consists of the IP transport devices and the IP communications intelligence built into the IPC application services. IP communications 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 (IPCC) 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, IP 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 IP communications you create a collaborative workforce, increase competitive advantage, and deliver measurable ROI. A smooth operation does not come without obstacles; the IPC environment needs to be managed.



Challenges to Managing IPC
The Need

With the migration to converged networks, network administrators need to ensure adequate availability and bandwidth for deploying multiple services over IP packet-based networks using quality of service features built into the IP fabric.

Voice and video traffic has low bandwidth requirements, but can not tolerate delays, packet loss, and jitter

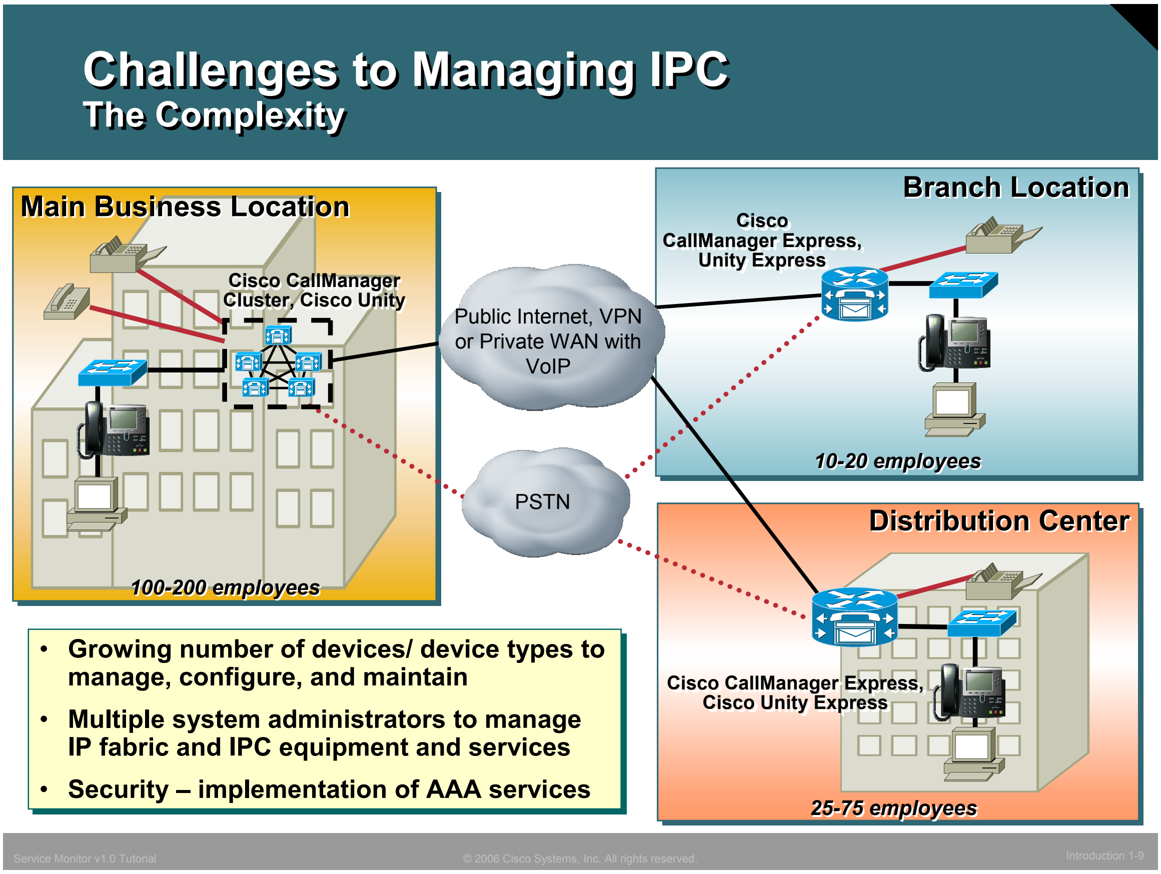
Data traffic is bursty in nature and tolerant to delay and Jitter

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-8

Challenges to Managing IPC

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 present 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.



Challenges to Managing IPC

The Complexity

Main Business Location
Cisco CallManager Cluster, Cisco Unity
100-200 employees
Public Internet, VPN or Private WAN with VoIP
PSTN
Branch Location
Cisco CallManager Express, Unity Express
10-20 employees
Distribution Center
Cisco CallManager Express, Cisco Unity Express
25-75 employees

- **Growing number of devices/ device types to manage, configure, and maintain**
- **Multiple system administrators to manage IP fabric and IPC equipment and services**
- **Security – implementation of AAA services**

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-9

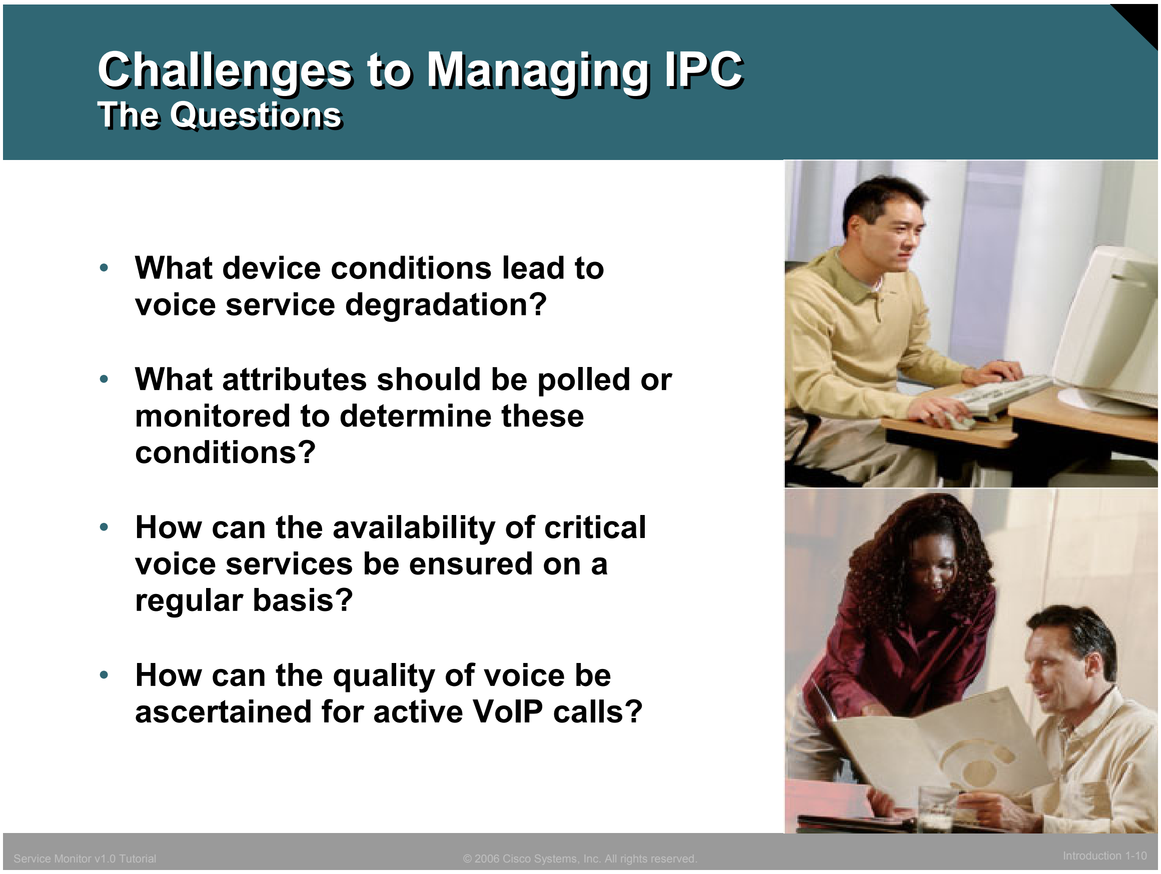
Challenges to Managing IPC

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 IPC 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 IP Communications can be found in Chapter 5 of this tutorial.)



Challenges to Managing IPC
The Questions

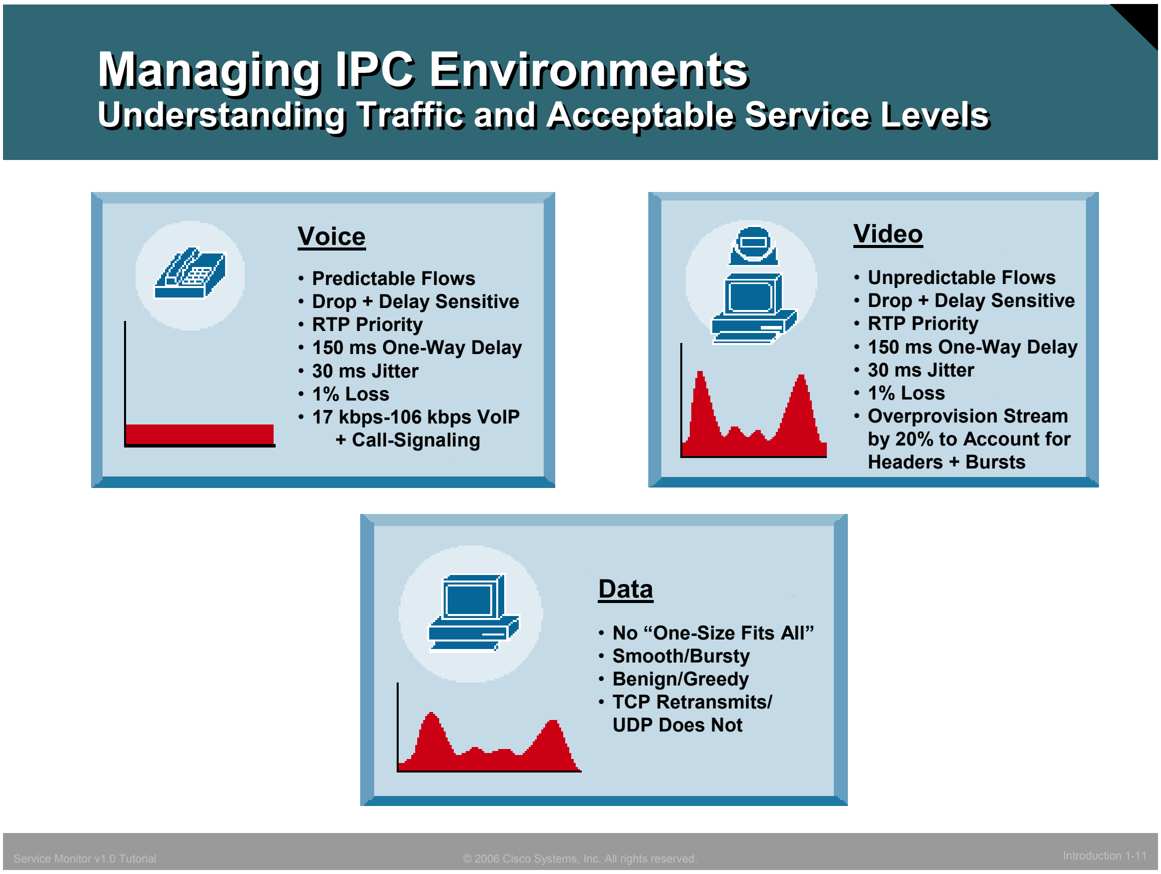
- What device conditions lead to voice service degradation?
- What attributes should be polled or monitored to determine these conditions?
- How can the availability of critical voice services be ensured on a regular basis?
- How can the quality of voice be ascertained for active VoIP calls?

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-10

Challenges to Managing IPC

So the decision was made a long time ago to deploy IP telephony and now that has expanded in 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. Where does one begin to answer some of these questions?

First, understand how you can obtain visibility into the network and its performance; understand how to gather this information, and understand your network and how it can work for you. Cisco’s infrastructure and network management tools is the starting point. Let’s take a look further.



Managing IPC Environments

Understanding Traffic and Acceptable Service Levels

Voice

- Predictable Flows
- Drop + Delay Sensitive
- RTP Priority
- 150 ms One-Way Delay
- 30 ms Jitter
- 1% Loss
- 17 kbps-106 kbps VoIP + Call-Signaling

Video

- Unpredictable Flows
- Drop + Delay Sensitive
- RTP Priority
- 150 ms One-Way Delay
- 30 ms Jitter
- 1% Loss
- Overprovision Stream by 20% to Account for Headers + Bursts

Data

- No “One-Size Fits All”
- Smooth/Bursty
- Benign/Greedy
- TCP Retransmits/ UDP Does Not

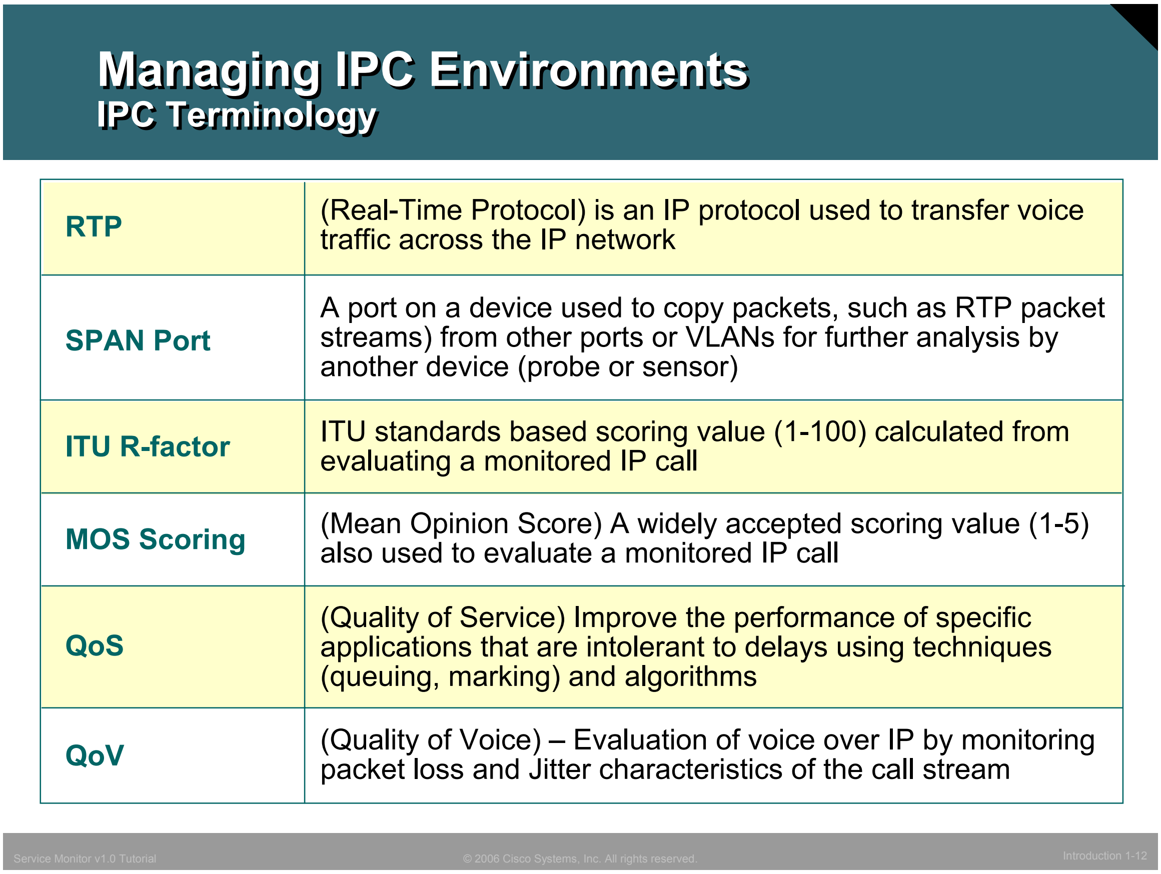
Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-11

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.



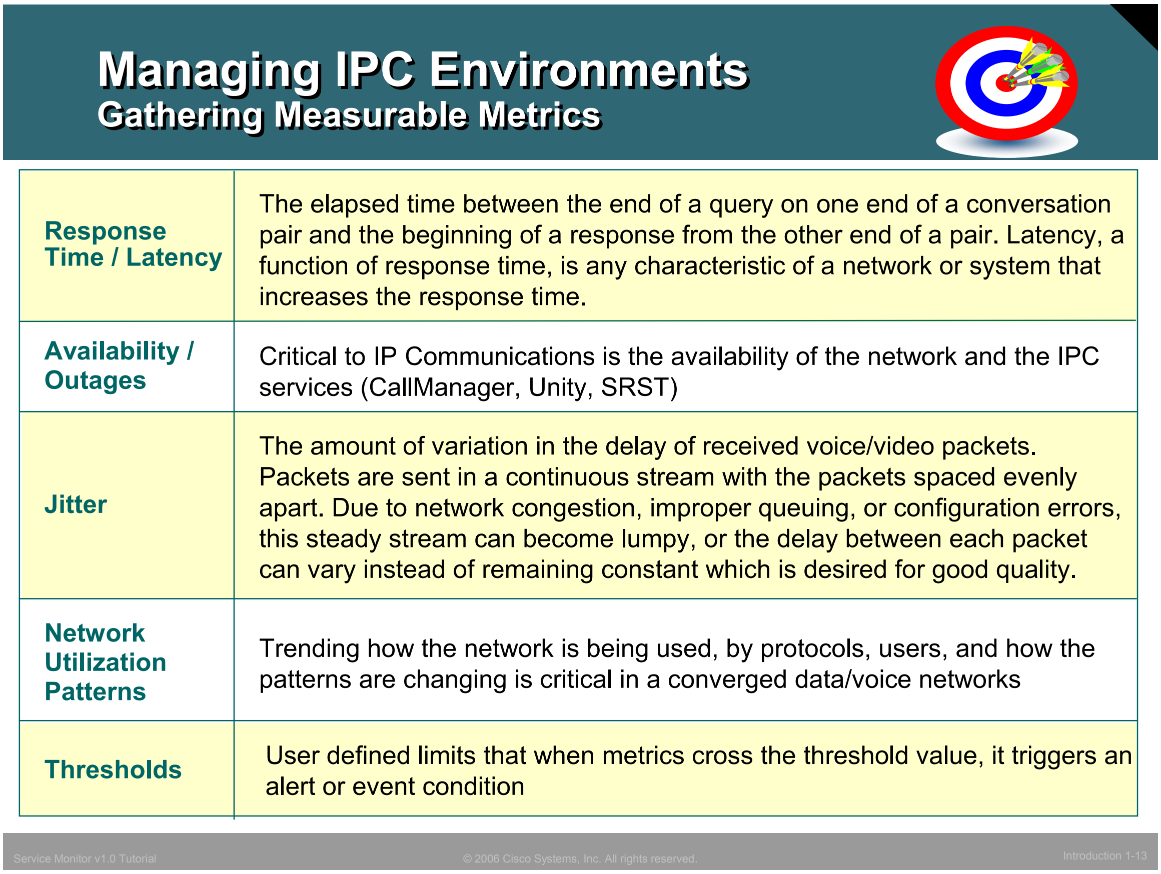
Managing IPC Environments

IPC 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

IPC 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 IPC Environments

Gathering Measurable 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 IPC 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

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-13

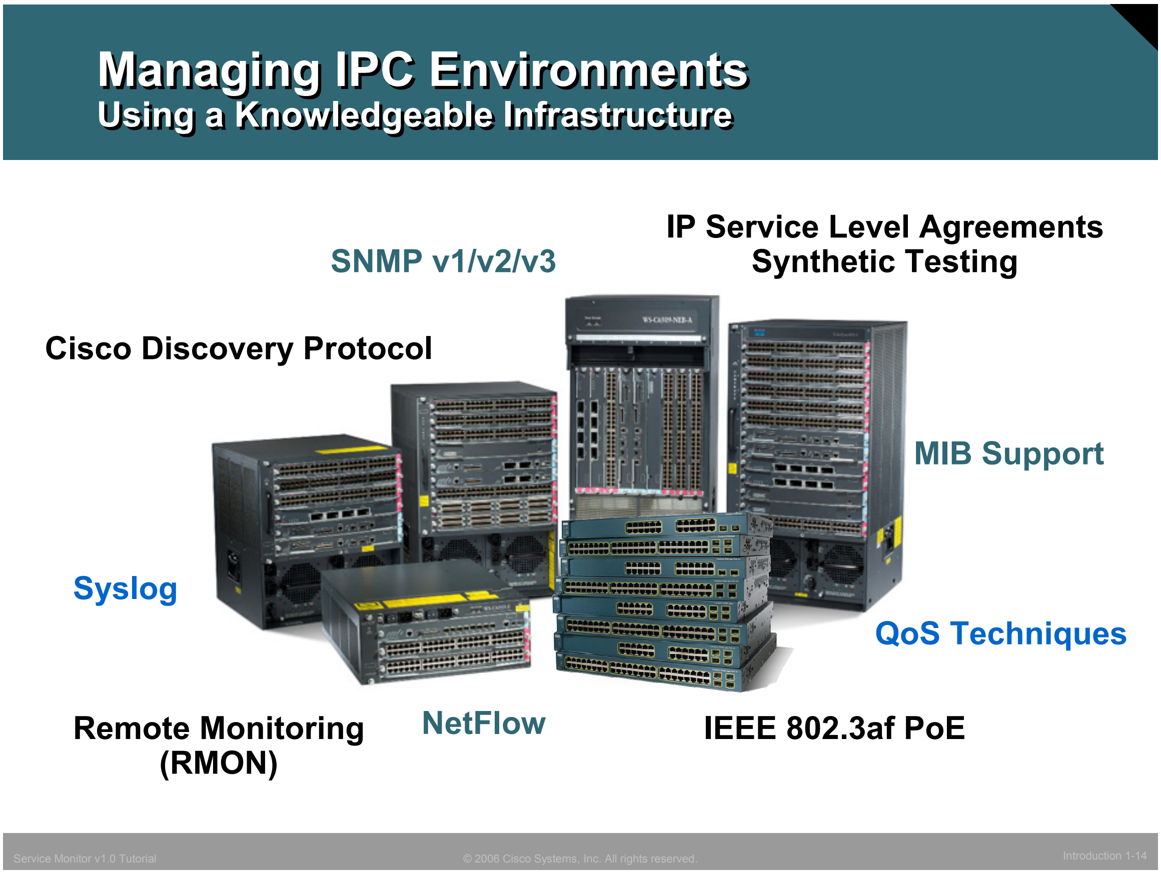
Gathering Measurable Metrics

Network managers look for measurable statistics such as jitter, packet loss, and end-to-end network latency, in order to ensure acceptable service levels. Familiar yourself with these metrics and what they mean in terms or 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 is undesirable for voice networks; a jitter value of zero would be ideal for delay-sensitive networks.*
>
> As depicted earlier, voice and video traffic is recommended to have 30 ms or less of jitter.

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



Managing IPC Environments
Using a Knowledgeable Infrastructure

IP Service Level Agreements
Synthetic Testing

SNMP v1/v2/v3

Cisco Discovery Protocol

MIB Support

Syslog

QoS Techniques

Remote Monitoring
(RMON)

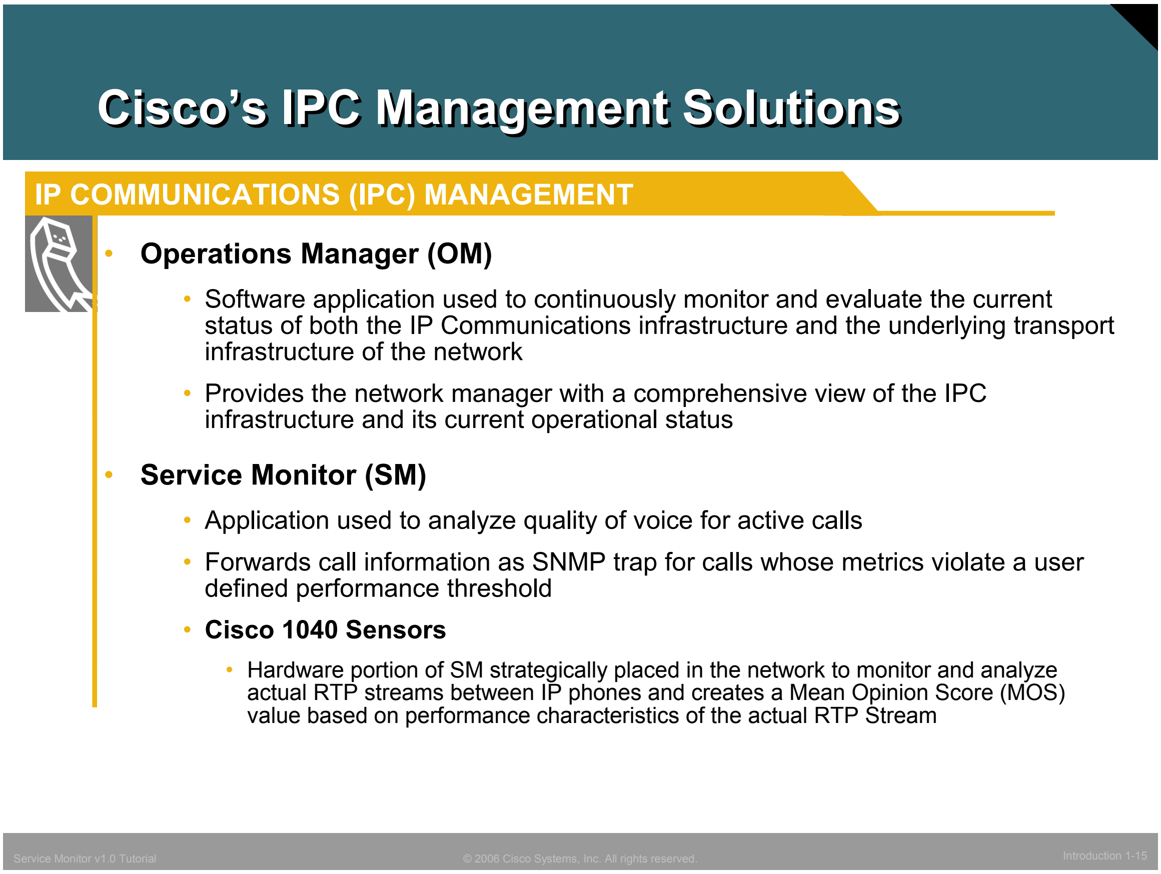
NetFlow

IEEE 802.3af PoE

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.



Cisco's IPC Management Solutions

IP COMMUNICATIONS (IPC) MANAGEMENT

- **Operations Manager (OM)**
  - Software application used to continuously monitor and evaluate the current status of both the IP Communications infrastructure and the underlying transport infrastructure of the network
  - Provides the network manager with a comprehensive view of the IPC infrastructure and its current operational status
- **Service Monitor (SM)**
  - Application used to analyze quality of voice for active calls
  - Forwards call information as SNMP trap for calls whose metrics violate a user defined performance threshold
  - **Cisco 1040 Sensors**
    - Hardware portion of SM strategically placed in the network to monitor and analyze actual RTP streams between IP phones and creates a Mean Opinion Score (MOS) value based on performance characteristics of the actual RTP Stream

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-15

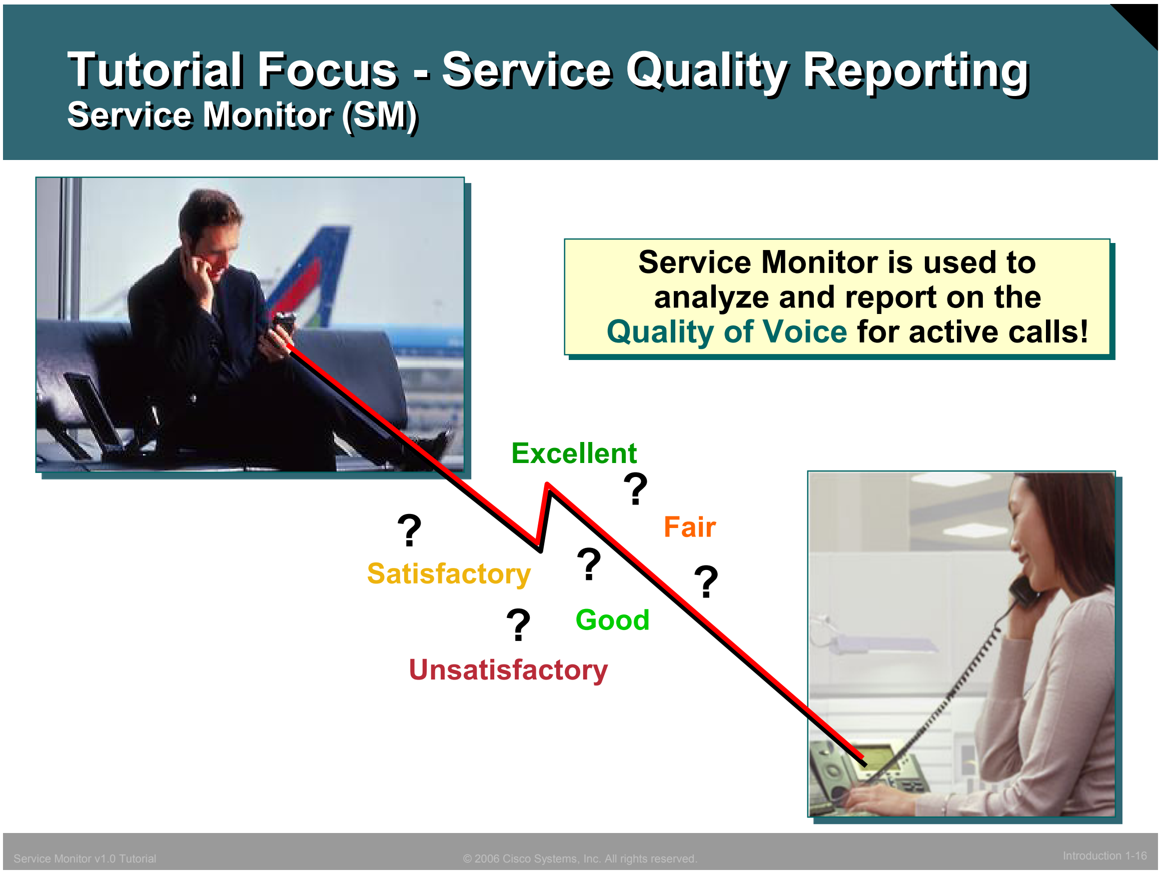
Cisco's IPC Management Solutions

CiscoWorks is a family of network management products that share a common user interface and underlying services. There are two components of the CiscoWorks IP Communications management solution that provide real-time management information and diagnostic tools to help ensure an efficient deployment and subscriber satisfaction: *Operations Manager* and *Security Monitor*.

Operations Manager provides a unified view of the entire IPC infrastructure and presents the current operational status of each element of the IPC network. Operations Manager also provides a rich set of diagnostic capabilities for faster trouble isolation and resolution.

Service Monitor evaluates and provides quality of voice metrics about active IP telephony calls in a monitored network. The Cisco 1040 sensors are a hardware appliance that performs the monitoring of the call streams and forwards Mean Opinion Score (MOS) values to the Service Monitor server. Service Monitor can then forward alerts for MOS values violating a user-defined threshold to Operations Manager or other enterprise network management systems.

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



Tutorial Focus - Service Quality Reporting

Service Monitor (SM)

Service Monitor is used to analyze and report on the Quality of Voice for active calls!

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Introduction 1-16

Service Monitor (SM)

This tutorial focuses on the Service Monitor application of the IPC 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.

Cisco Systems

Empowering the Internet Generation^{SM}

Thank You!

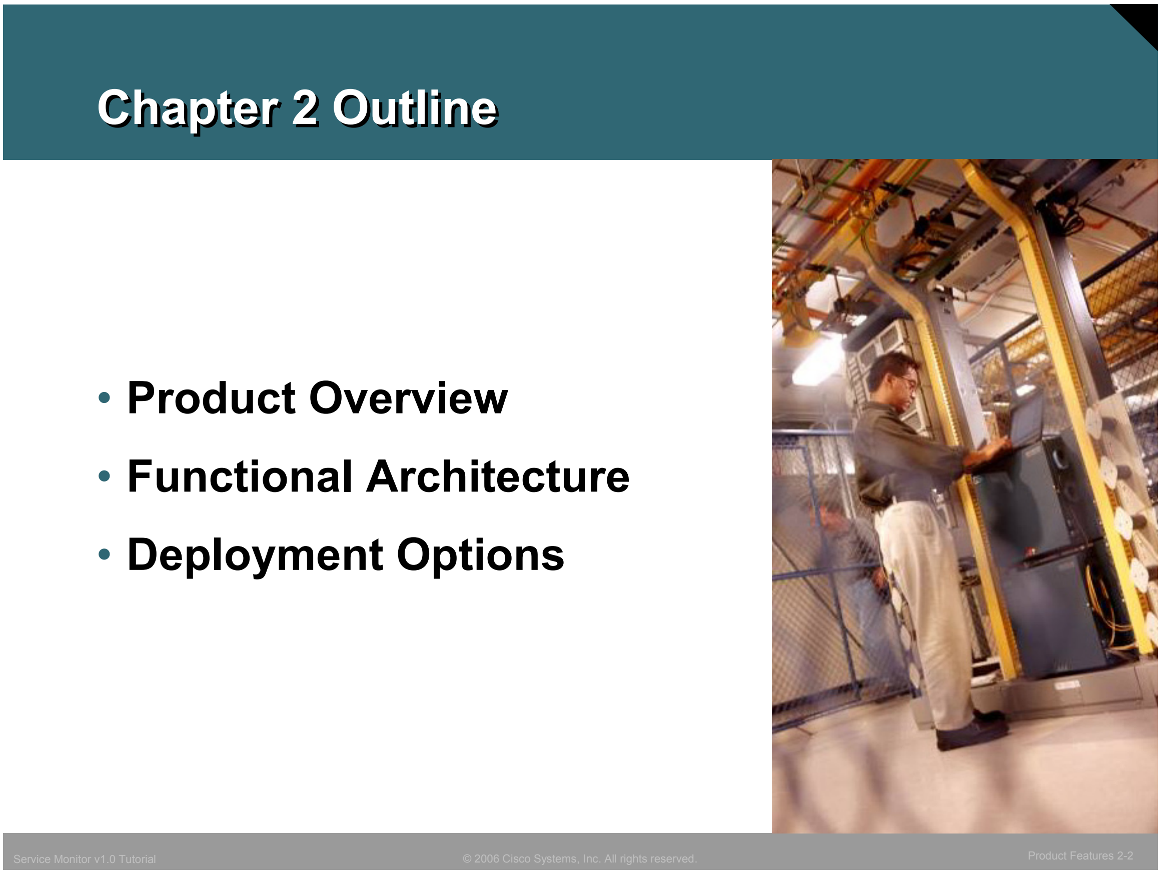
Continue on to Chapter 2 to discover the many features of Service Monitor.

<Intentionally Left Blank>

Service Monitor

Product Features

Chapter 2



Chapter 2 Outline

- Product Overview
- Functional Architecture
- Deployment Options

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-2

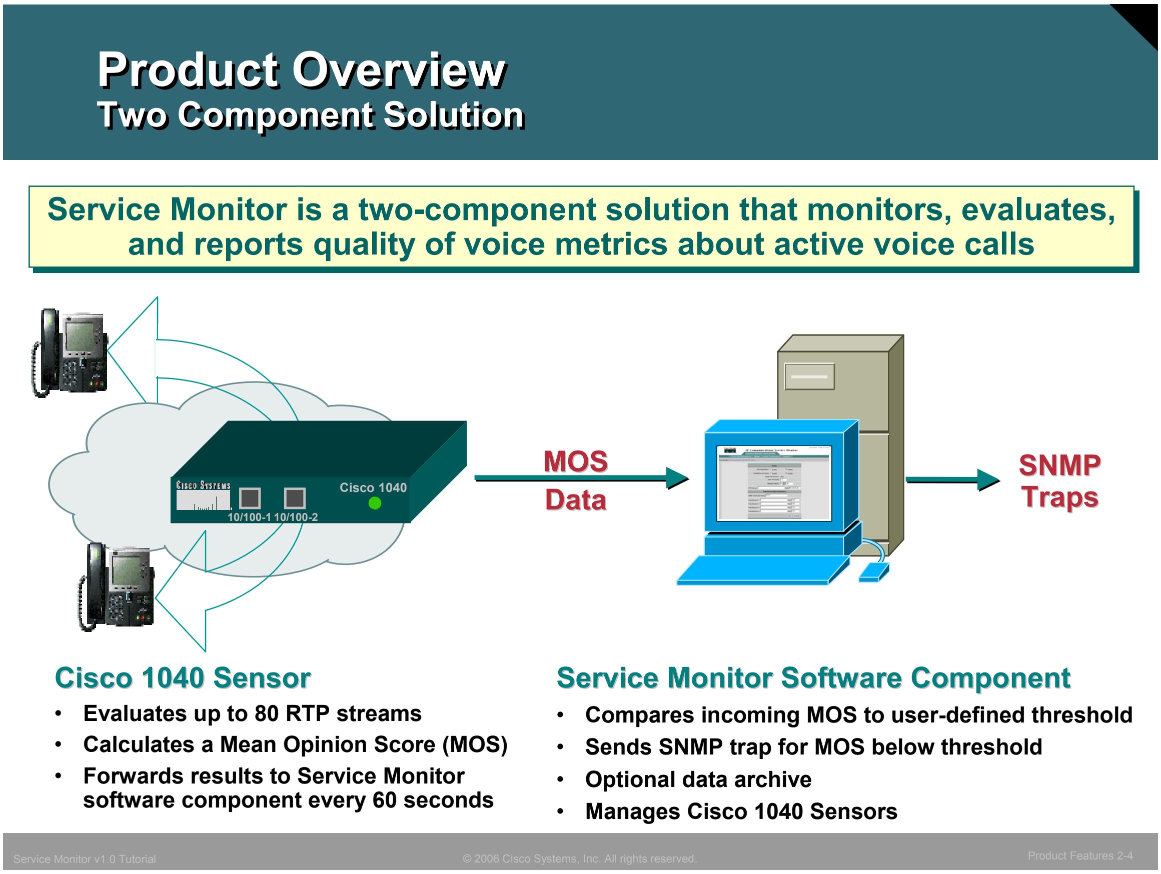
Chapter 2 Outline

Hopefully Chapter 1 has excited you to the benefits of monitoring the quality of voice for active calls using 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.

Service Monitor Product Overview

- Product Overview
- Functional Architecture
- Deployment Options



Product Overview
Two Component Solution

Service Monitor is a two-component solution that monitors, evaluates, and reports quality of voice metrics about active voice calls

Cisco 1040 Sensor

- Evaluates up to 80 RTP streams
- Calculates a Mean Opinion Score (MOS)
- Forwards results to Service Monitor software component every 60 seconds

Service Monitor Software Component

- Compares incoming MOS to user-defined threshold
- Sends SNMP trap for MOS below threshold
- Optional data archive
- Manages Cisco 1040 Sensors

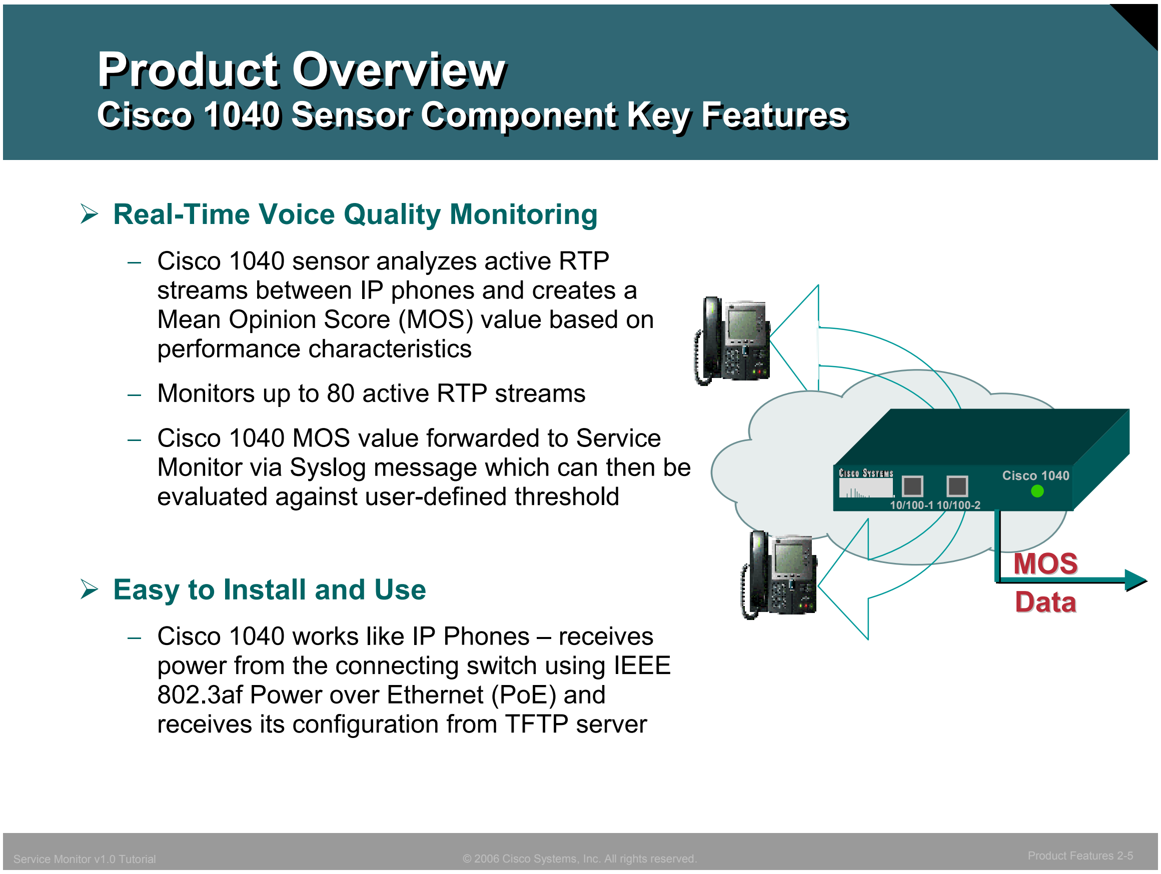
Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-4

Service Monitor Overview

Service Monitor is a two component solution for monitoring and evaluating the quality of voice for active IP telephony calls. It consists of both a hardware component – Cisco 1040 sensors, and a software component – simply referred to as Service Monitor. Let's take a high-level look at the functions of each of these components, while a more detailed look will be presented in the next section of this chapter.

Cisco 1040 Sensor – A hardware appliance or probe used to monitor quality of voice for up to 40 active IP telephony calls (80 RTP streams). 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.

Service Monitor Sever – 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 up to four trap recipients. Service Monitor can also optionally archive all incoming metrics, and is used to manage the Cisco 1040 Sensors.



Product Overview

Cisco 1040 Sensor Component Key Features

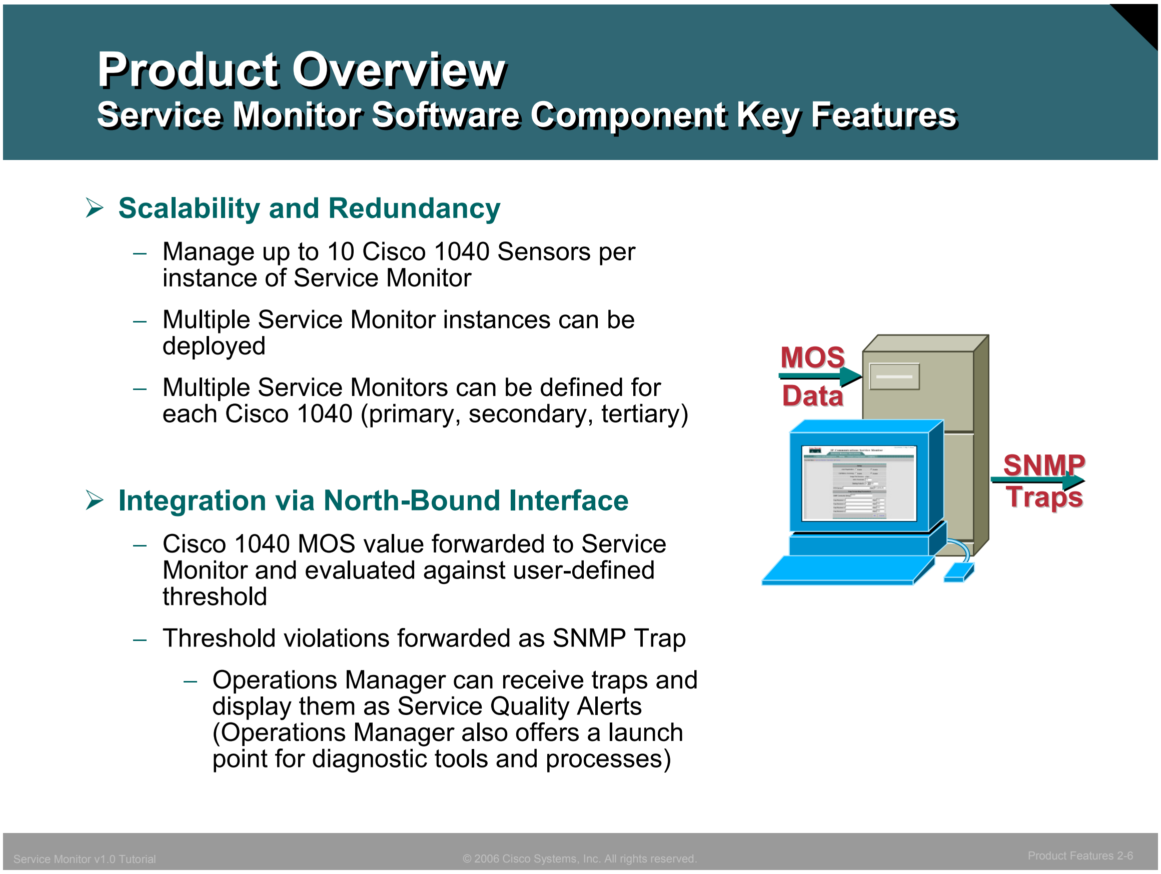
- **Real-Time Voice Quality Monitoring**
  - Cisco 1040 sensor analyzes active RTP streams between IP phones and creates a Mean Opinion Score (MOS) value based on performance characteristics
  - Monitors up to 80 active RTP streams
  - Cisco 1040 MOS value forwarded to Service Monitor via Syslog message which can then be evaluated against user-defined threshold
- **Easy to Install 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 Sensor Component Key Features

The Service Monitor 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 quality falls below a user-defined threshold.

The 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.



Product Overview
Service Monitor Software Component Key Features

- **Scalability and Redundancy**
  - Manage up to 10 Cisco 1040 Sensors per instance of Service Monitor
  - Multiple Service Monitor instances can be deployed
  - Multiple Service Monitors can be defined for each Cisco 1040 (primary, secondary, tertiary)
- **Integration via North-Bound Interface**
  - Cisco 1040 MOS value forwarded to Service Monitor and evaluated against user-defined threshold
  - Threshold violations forwarded as SNMP Trap
    - Operations Manager can receive traps and display them as Service Quality Alerts (Operations Manager also offers a launch point for diagnostic tools and processes)

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-6

Service Monitor Software Component Key Features

The second part of the active voice call monitoring solution is the Service Monitor software. Each instance of Service Monitor software installed is used to receive and evaluate the MOS call metrics for up to 10 Cisco 1040 sensors. There are no limits to the number of Service Monitor servers that can be deployed. For redundancy purposes, each Cisco 1040 can be configured with a primary, secondary, and tertiary 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.

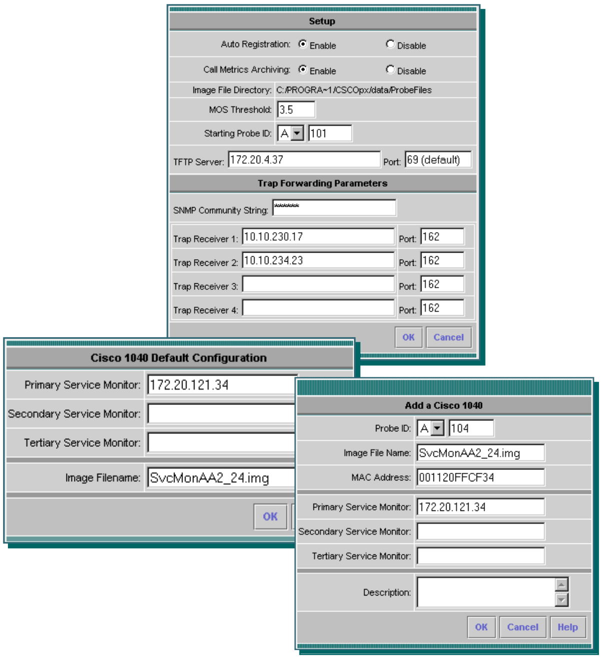
The MOS value sent by the Cisco 1040 sensor is evaluated by the Service Monitor server against a user-defined threshold. If a threshold violation is detected, Service Monitor sends the violation information as a SNMP trap to up to four recipients. One such recipient, Operations Manager (OM), displays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

Product Overview

Service Monitor Software Tasks

- **Server Setup**
  - 1040 Registration Type
  - Call Metrics Archiving
  - MOS Threshold Setting
  - Trap Forwarding
- **Cisco 1040 Configuration and Management**
  - Default or Individual
  - Set Image
  - Set Backup SM Servers

Usage details found in Chapter 3



Setup

Auto Registration: ● Enable ○ Disable
Call Metrics Archiving: ● Enable ○ Disable
Image File Directory: C:/PROGRA~1/CSCOpx/data/ProbeFiles
MOS Threshold: 3.5
Starting Probe ID: A 101
TFTP Server: 172.20.4.37 Port: 69 (default)

Trap Forwarding Parameters

SNMP Community String: ******
Trap Receiver 1: 10.10.230.17 Port: 162
Trap Receiver 2: 10.10.234.23 Port: 162
Trap Receiver 3: Port: 162
Trap Receiver 4: Port: 162

Cisco 1040 Default Configuration

Primary Service Monitor: 172.20.121.34
Secondary Service Monitor:
Tertiary Service Monitor:
Image Filename: SvcMonAA2_24.img

Add a Cisco 1040

Probe ID: A 104
Image File Name: SvcMonAA2_24.img
MAC Address: 001120FFCF34
Primary Service Monitor: 172.20.121.34
Secondary Service Monitor:
Tertiary Service Monitor:
Description:

Service Monitor Software Tasks

The Service Monitor software component only has a few tasks. The **Setup** tasks allows the network administrator 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 arching, set the MOS threshold, and configure the Trap receivers that MOS violations will be forwarded to.

The Service Monitor software component is also used to manage the Cisco 1040s. After selecting the type of registration, the network administrator will either define a default configuration to be used by all 1040s, or will create specific configurations for each individual Cisco 1040. Configurations include the image to use and the SM server to send MOS values to. The network manager can also configure a secondary and tertiary SM server in case the primary fails. The software can then be used to verify that the configured Cisco 1040s have registered with SM.

Usage of the Service Monitor software tasks discussed above are discussed in detail in Chapter 3. An additional Service Monitor software task that is used to set the troubleshooting logging level is discussed in Chapter 4.

Product Overview

Product Compatibility

Service Monitor supports Cisco IP Communications deployments consisting of:

- Cisco Call Manager
- Cisco Unity
- IP Contact Center
- Call Manager Express
- Cisco Unity Express
- Cisco Meeting Place
- Cisco Conference Connection
- Cisco Personal Assistant
- Cisco Emergency Responder
- Routers, Gateways, Switches, and IP Phones

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-8

Product Compatibility

Currently, Service Monitor’s monitoring capabilities are compatible with the following voice related products:

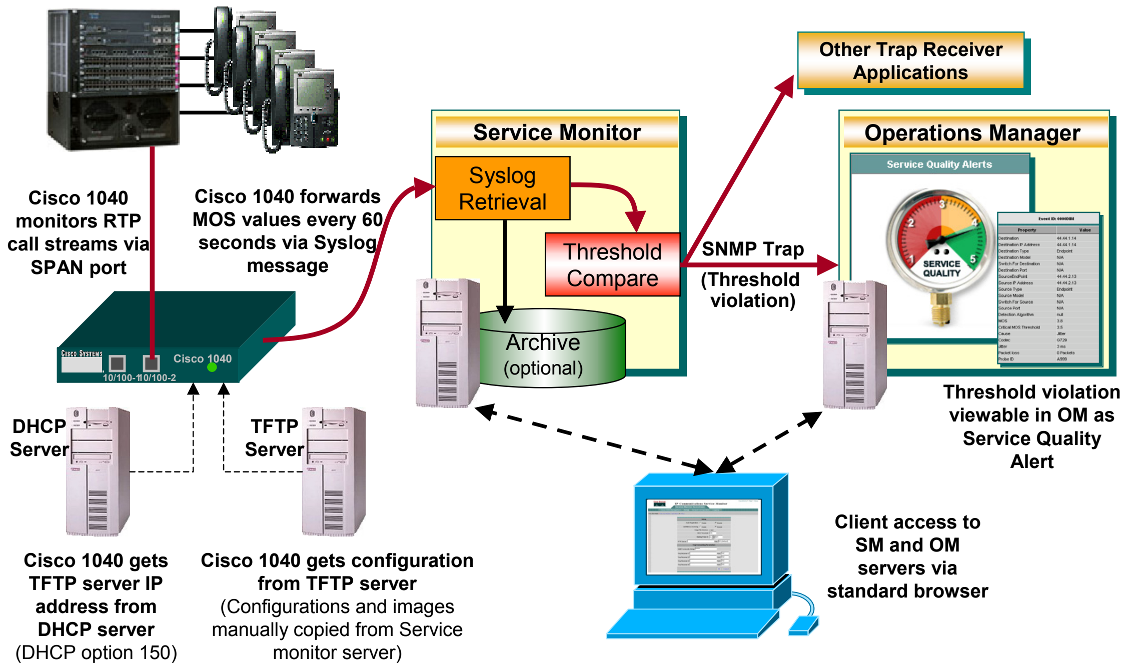
- Cisco Call Manager
- Cisco Unity
- IP Contact Center
- Call Manager Express
- Cisco Unity Express
- Cisco Meeting Place
- Cisco Conference Connection
- Cisco Personal Assistant
- Cisco Emergency Responder
- Routers, Gateways, Switches, and IP Phones

CISCO SYSTEMS

Service Monitor Functional Architecture

- Product Overview
- Functional Architecture
- Deployment Options

Service Monitor Functional Architecture



Other Trap Receiver Applications

Service Monitor

Syslog Retrieval

Threshold Compare

Archive (optional)

Operations Manager

Service Quality Alerts

SNMP Trap (Threshold violation)

Cisco 1040 monitors RTP call streams via SPAN port

Cisco 1040 forwards MOS values every 60 seconds via Syslog message

Threshold violation viewable in OM as Service Quality Alert

DHCP Server

TFTP Server

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

Cisco 1040 gets configuration from TFTP server (Configurations and images manually copied from Service monitor server)

Client access to SM and OM servers via standard browser

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-10

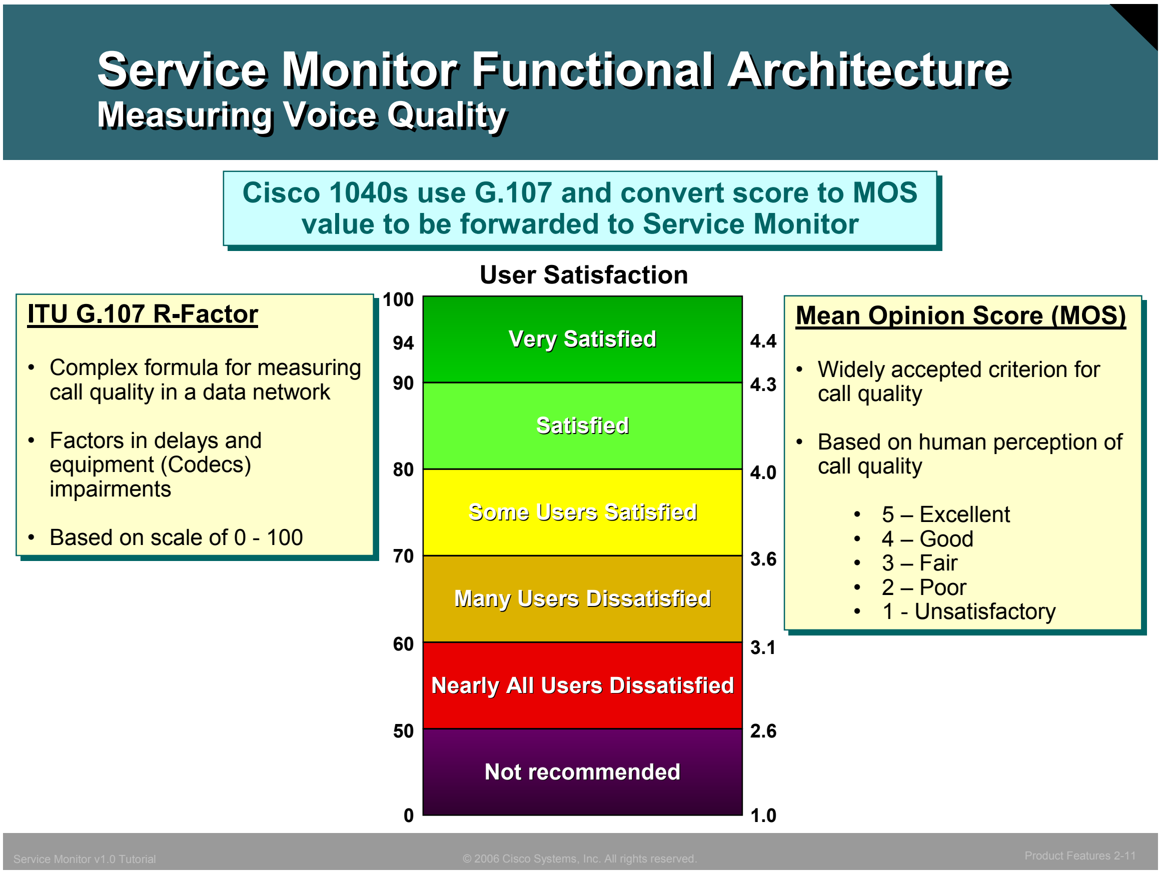
Service Monitor Functional Flow

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. The SM server retrieves the Syslog message 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

ITU G.107 R-Factor

- Complex formula for measuring call quality in a data network
- Factors in delays and equipment (Codecs) impairments
- Based on scale of 0 - 100

Mean Opinion Score (MOS)

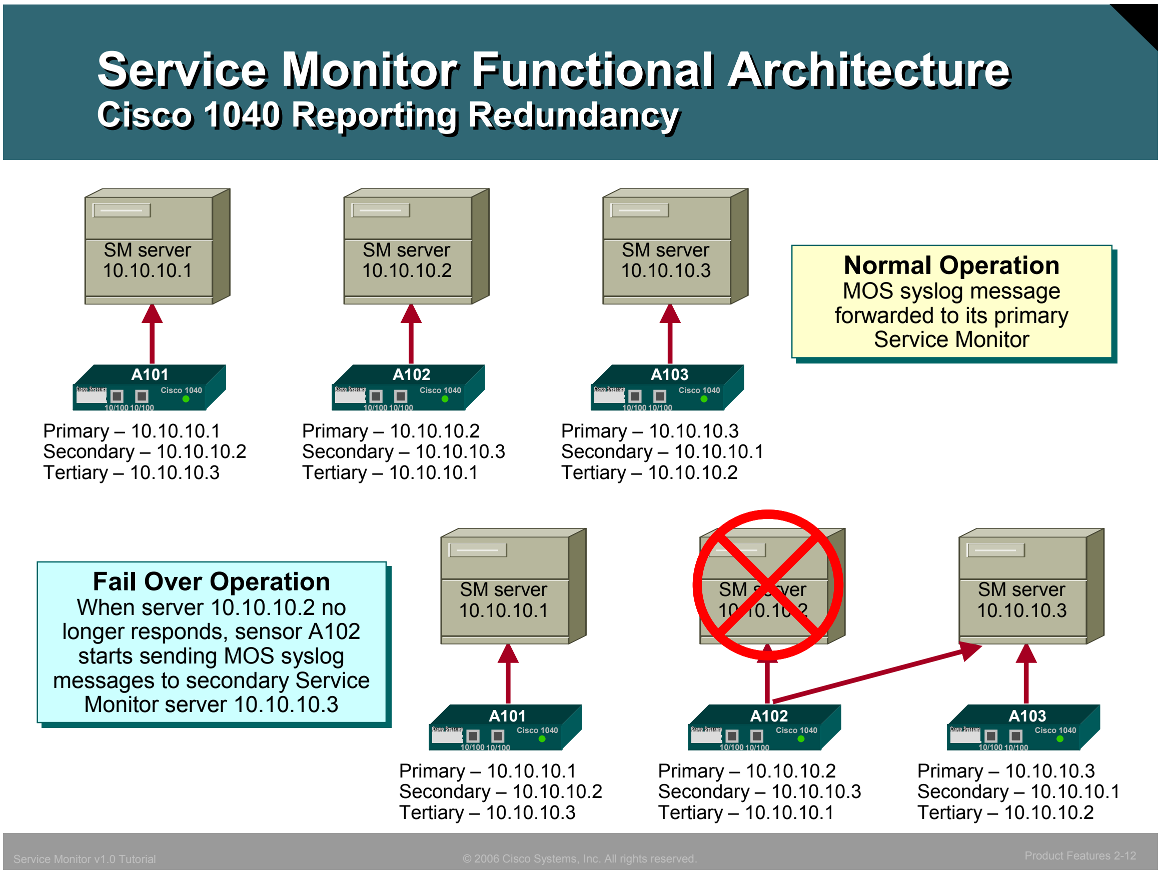
- Widely accepted criterion for call quality
- Based on human perception of call quality
  - 5 – Excellent
  - 4 – Good
  - 3 – Fair
  - 2 – Poor
  - 1 - Unsatisfactory

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-11

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.



Service Monitor Functional Architecture

Cisco 1040 Reporting Redundancy

A101: Primary – 10.10.10.1
Secondary – 10.10.10.2
Tertiary – 10.10.10.3

A102: Primary – 10.10.10.2
Secondary – 10.10.10.3
Tertiary – 10.10.10.1

A103: Primary – 10.10.10.3
Secondary – 10.10.10.1
Tertiary – 10.10.10.2

Normal Operation
MOS syslog message forwarded to its primary Service Monitor

Fail Over Operation
When server 10.10.10.2 no longer responds, sensor A102 starts sending MOS syslog messages to secondary Service Monitor server 10.10.10.3

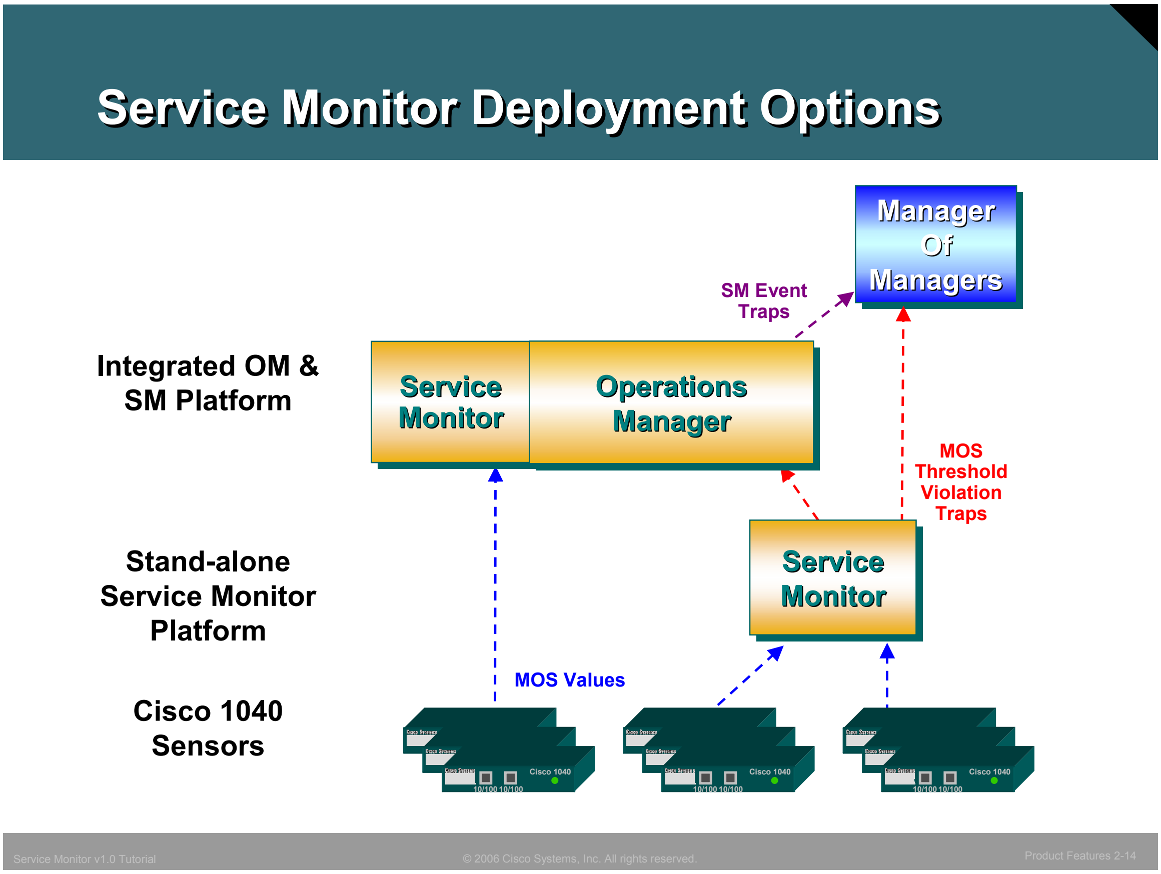
Cisco 1040 Reporting Redundancy

It was mentioned earlier that when creating configurations for a Cisco 1040 sensor, the administrator could add a secondary and tertiary SM server. What is the purpose of the secondary and tertiary servers?

Each sensor forwards call quality metrics to the SM server every 60 seconds. 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 SM server, it will then register with the secondary SM server (if configured in its configuration) and begin sending call quality metrics to it. This design ensures that no threshold violations are missed.

Service Monitor Deployment Options

- Product Overview
- Functional Architecture
- Deployment Options



Service Monitor Deployment Options

Manager Of Managers

SM Event Traps

Integrated OM & SM Platform

Service Monitor

Operations Manager

MOS Threshold Violation Traps

Stand-alone Service Monitor Platform

Service Monitor

MOS Values

Cisco 1040 Sensors

Service Monitor v1.0 Tutorial

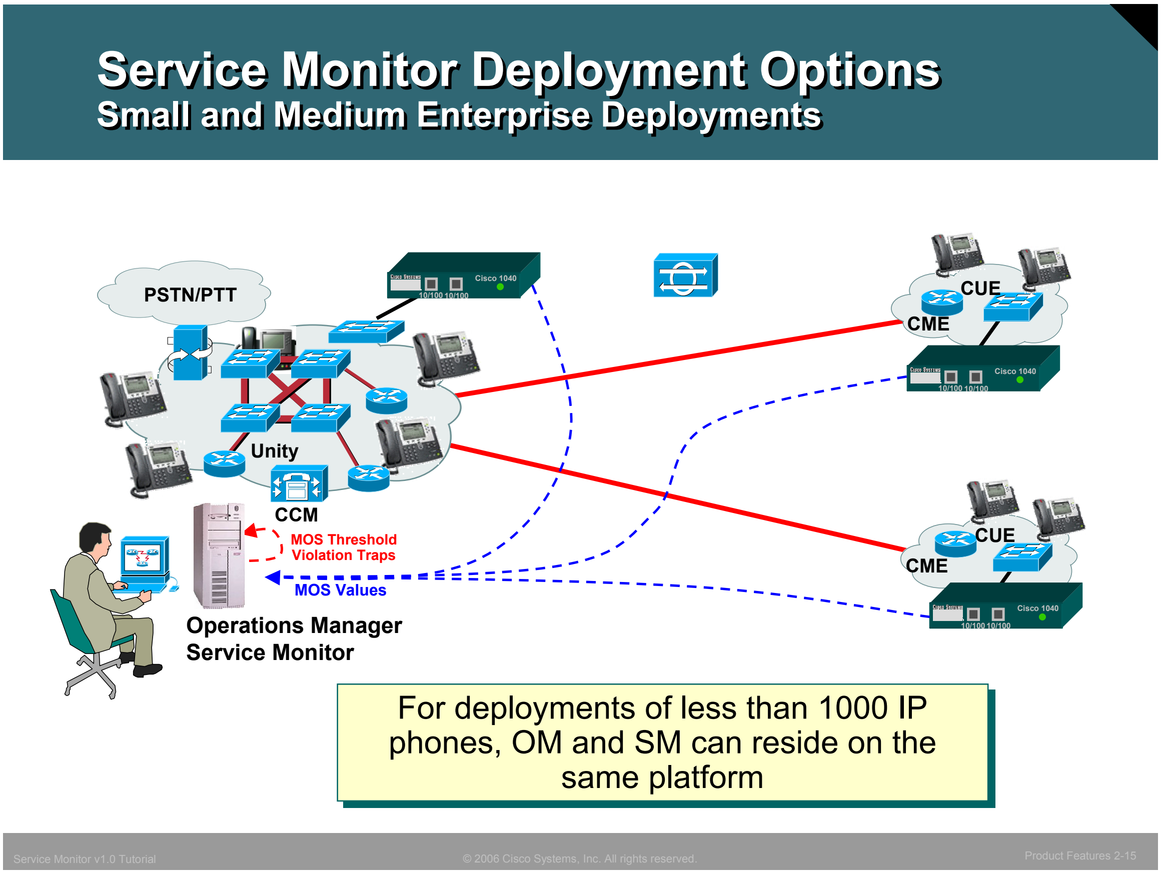
© 2006 Cisco Systems, Inc. All rights reserved.

Product Features 2-14

Service Monitor Deployment Options

One of the reason for limiting the number of 1040s reporting to an SM server is the I/O intensive nature of the application. With 10 Cisco 1040s reporting, an instance of SM could potentially receive up to 800 syslog messages a minute, archive them, evaluate them, and potentially generate and send up to four SNMP traps per syslog. This extreme case is simply used to demonstrate the need to possibly employ multiple instances of Service Monitor servers. Since, Service Monitor and Operations Manager are both CiscoWorks applications relying on the same underlying software (CiscoWorks Common Services), both Service Monitor and Operations Manager could potentially reside on the same server.

For large enterprises, it is not uncommon to have multiple instances of SM server all reporting to a single instance of OM. The next two slides look at small/medium and large enterprise deployments.



Service Monitor Deployment Options
Small and Medium Enterprise Deployments

Operations Manager
Service Monitor

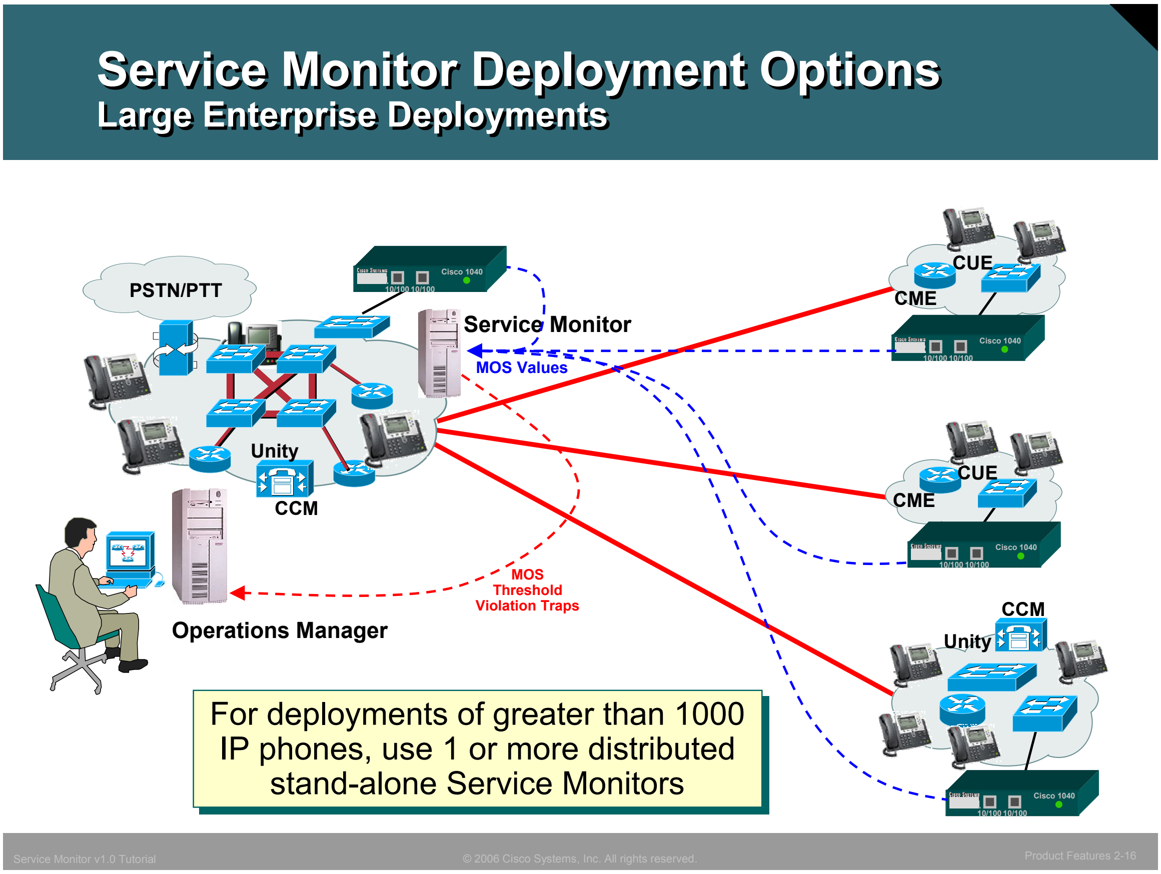
For deployments of less than 1000 IP phones, OM and SM can reside on the same platform

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-15

Small and Medium Enterprise Deployments

In small to medium enterprises (generally less than 1000 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

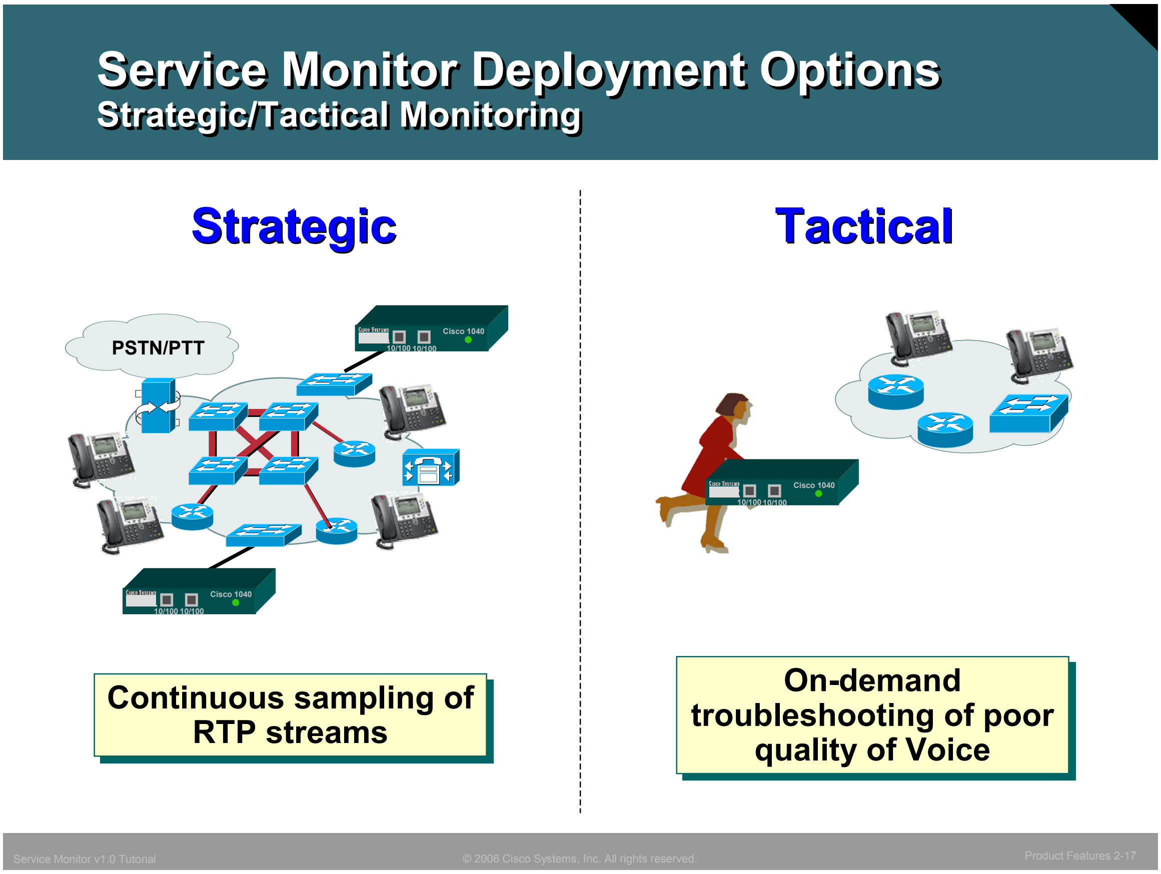
Large Enterprise Deployments

For deployments of greater than 1000 IP phones, use 1 or more distributed stand-alone Service Monitors

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-16

Large Enterprise Deployments

For larger enterprises (generally more than 1000 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 10 Cisco 1040s to provide a distributed, highly scalable, and redundant mechanism to analyze IP telephony voice quality.



Service Monitor Deployment Options
Strategic/Tactical Monitoring

Strategic

Continuous sampling of RTP streams

Tactical

On-demand troubleshooting of poor quality of Voice

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Product Features 2-17

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 – the continuous sampling of RTP streams. Sensors should be placed based upon 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, and can immediately 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 deployed. If the *Call Detail Records* (CDR) option is enabled in *Call Manager*, 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.

Cisco Systems®

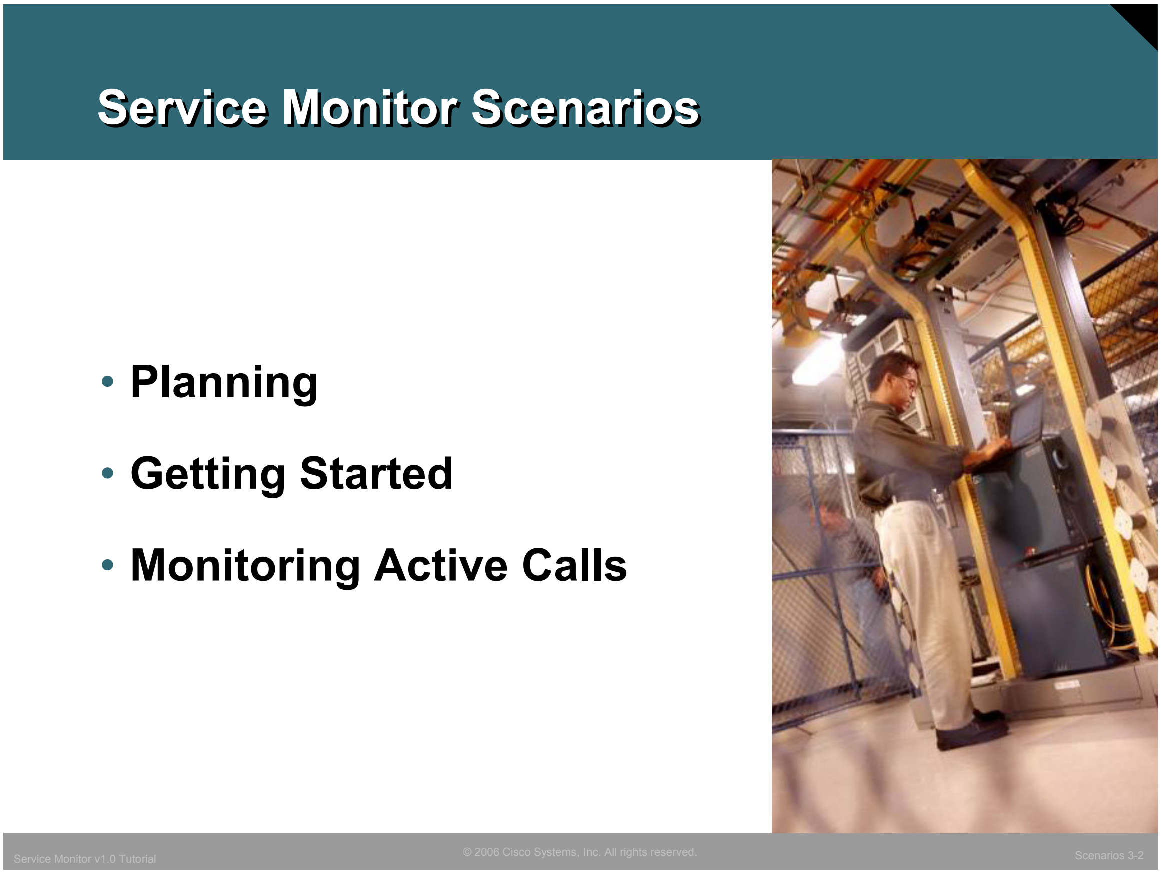
Empowering the
Internet Generation℠

Thank You!

Continue on to Chapter 3 to learn how to use Service Monitor through a series of scenarios.

Service Monitor Scenarios

Chapter 3



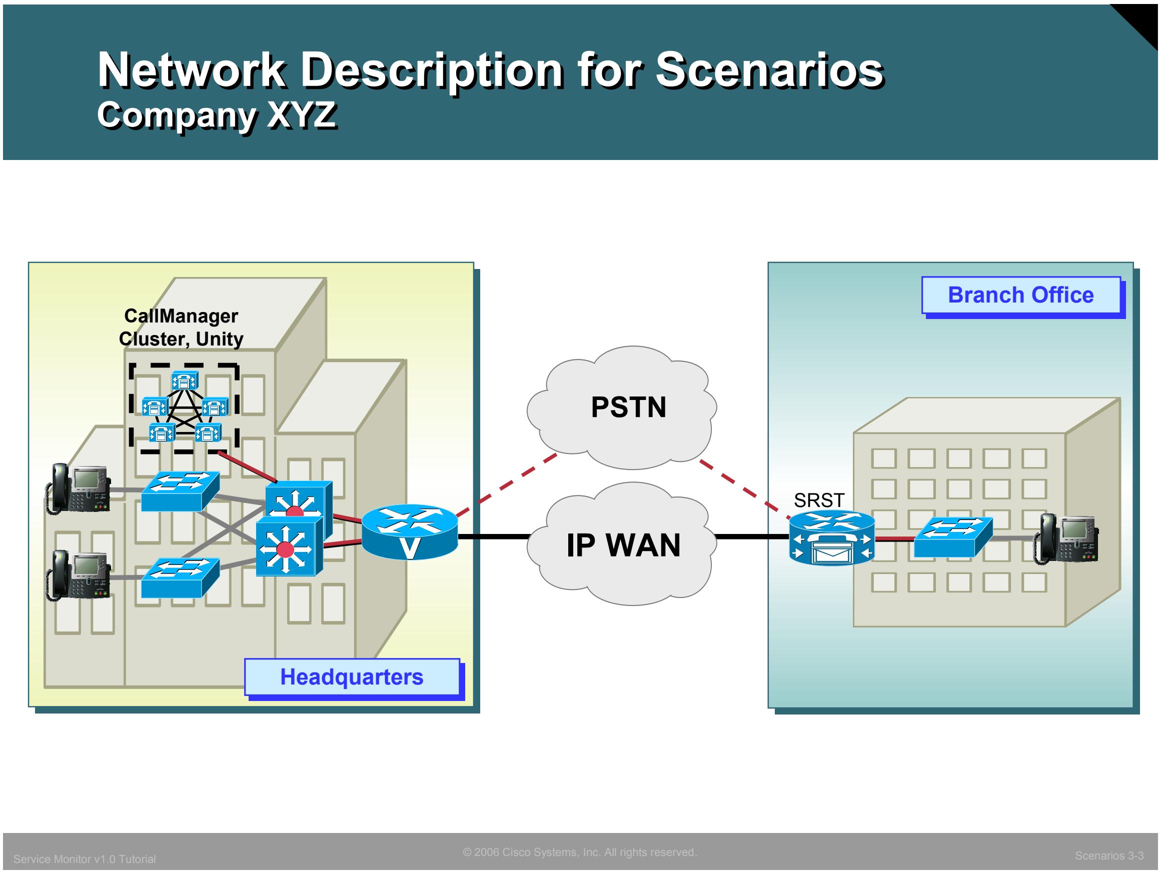
Service Monitor Scenarios

- Planning
- Getting Started
- Monitoring Active Calls

Service Monitor Scenarios

This chapter uses several scenarios to illustrate how to setup and use 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 and the Cisco 1040 Sensors, 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

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Scenarios 3-3

Network Description – Company XYZ

To help facility the reader's understanding of the setup and use of Service Monitor, the scenarios will follow the deployment of Service Monitor in a fictional 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.

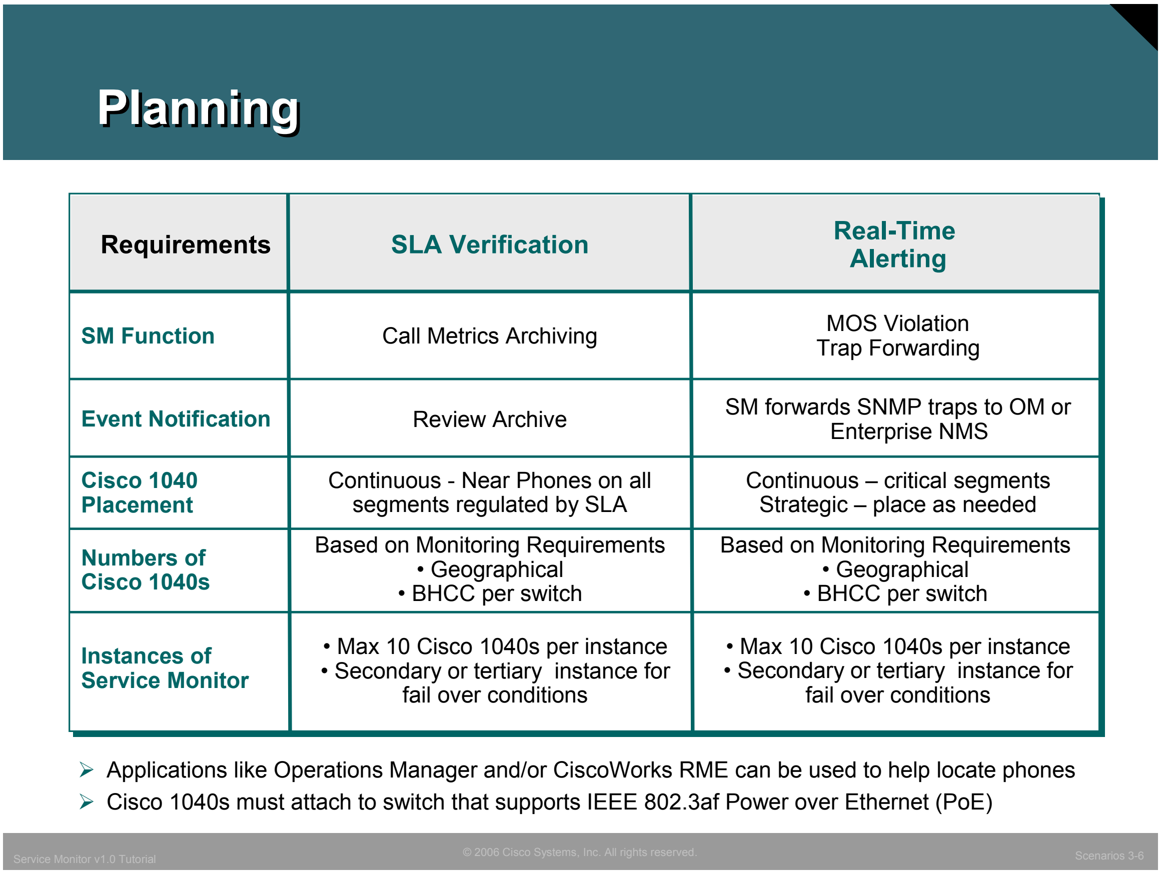
<Intentionally Left Blank>

Planning

Planning

Getting Started

Monitoring Active Calls



Planning

Requirements	SLA Verification	Real-Time Alerting
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)

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 Service Monitor.

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

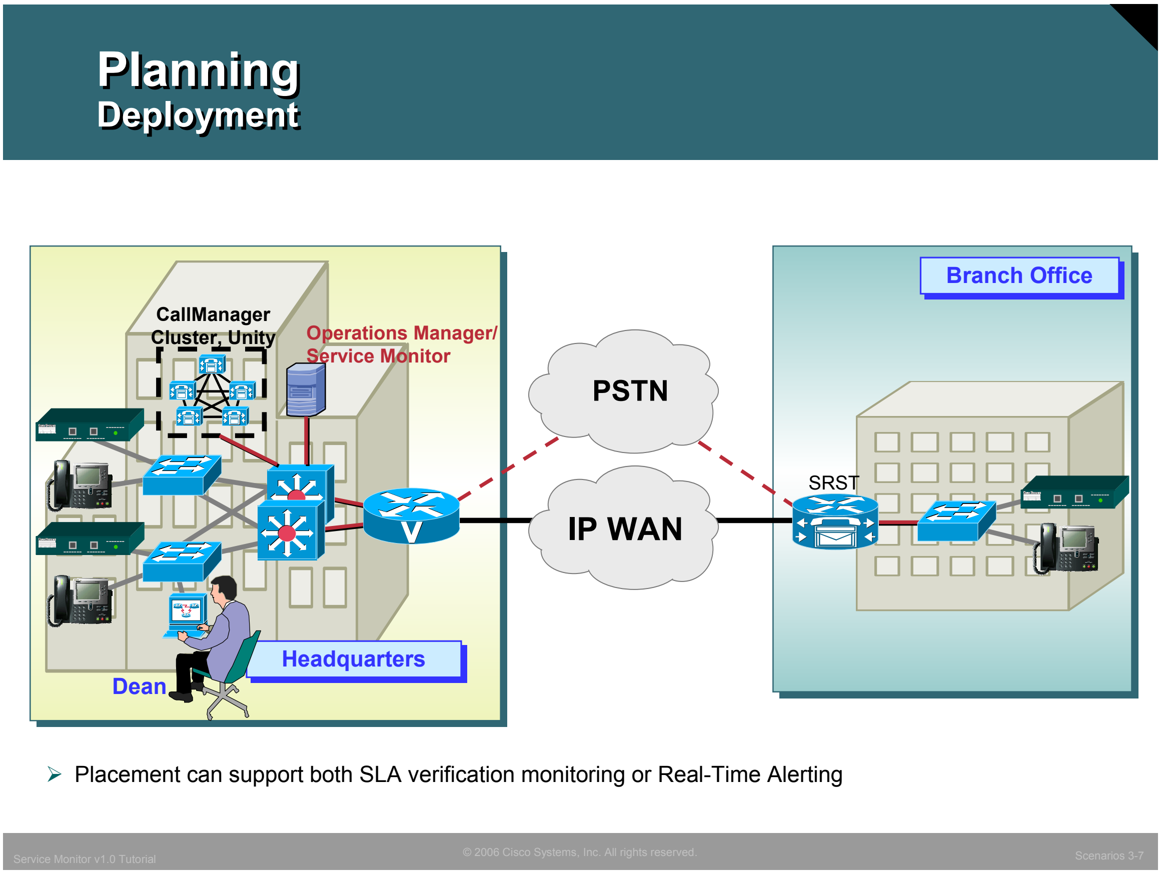
The requirements of Dean’s task have a direct correlation to the configuration of Service Monitor – Dean will need to both look for current voice concerns (MOS violation threshold) and make sure he archives the call metrics for every call to help him determine if the SLAs are being met. Since Dean wants 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 IPC 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 monitoring. It is for this issue that 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), and 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.

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.

Note(s):

- 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.



Planning
Deployment

- Placement can support both SLA verification monitoring or Real-Time Alerting

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Scenarios 3-7

Deployment

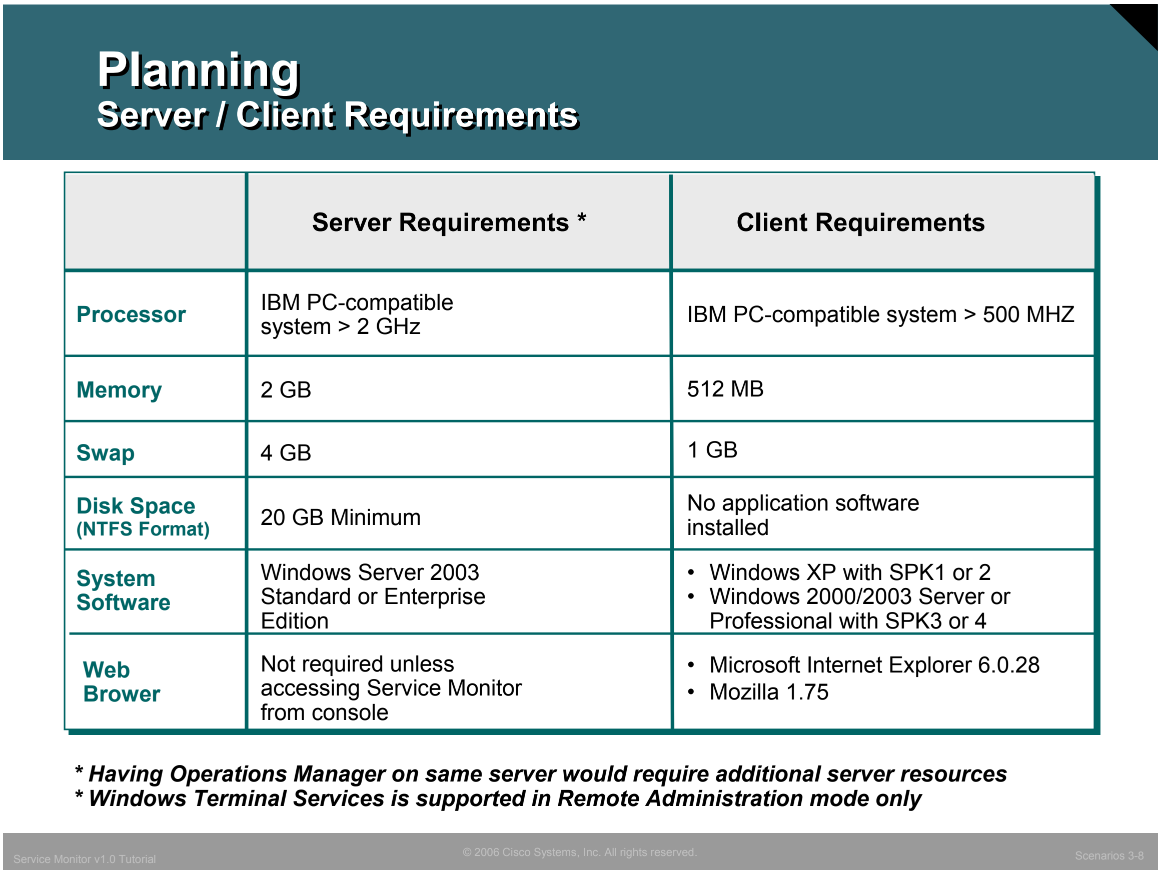
Currently, Company XYZ is a small firm and Dean will only need 3 Cisco 1040 sensors to give him complete coverage at the access layer. Two Cisco 1040 sensors will handle all the phones in the building at the corporate headquarters, and another Cisco 1040 sensor will be deployed to handle the phones at the remote branch facility. Since the current deployment is small (less than a 1000 phones), Dean will have the IPC applications, Operations Manager and Service Monitor, 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.

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).



Planning
Server / Client Requirements

	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***
**** Windows Terminal Services is supported in Remote Administration mode only***

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Scenarios 3-8

Server / Client Requirements

The chart above details the sizing requirements for a stand-alone Service Monitor server supporting up to 10 Cisco 1040 sensors. If Service Monitor is to reside on the same server as 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.

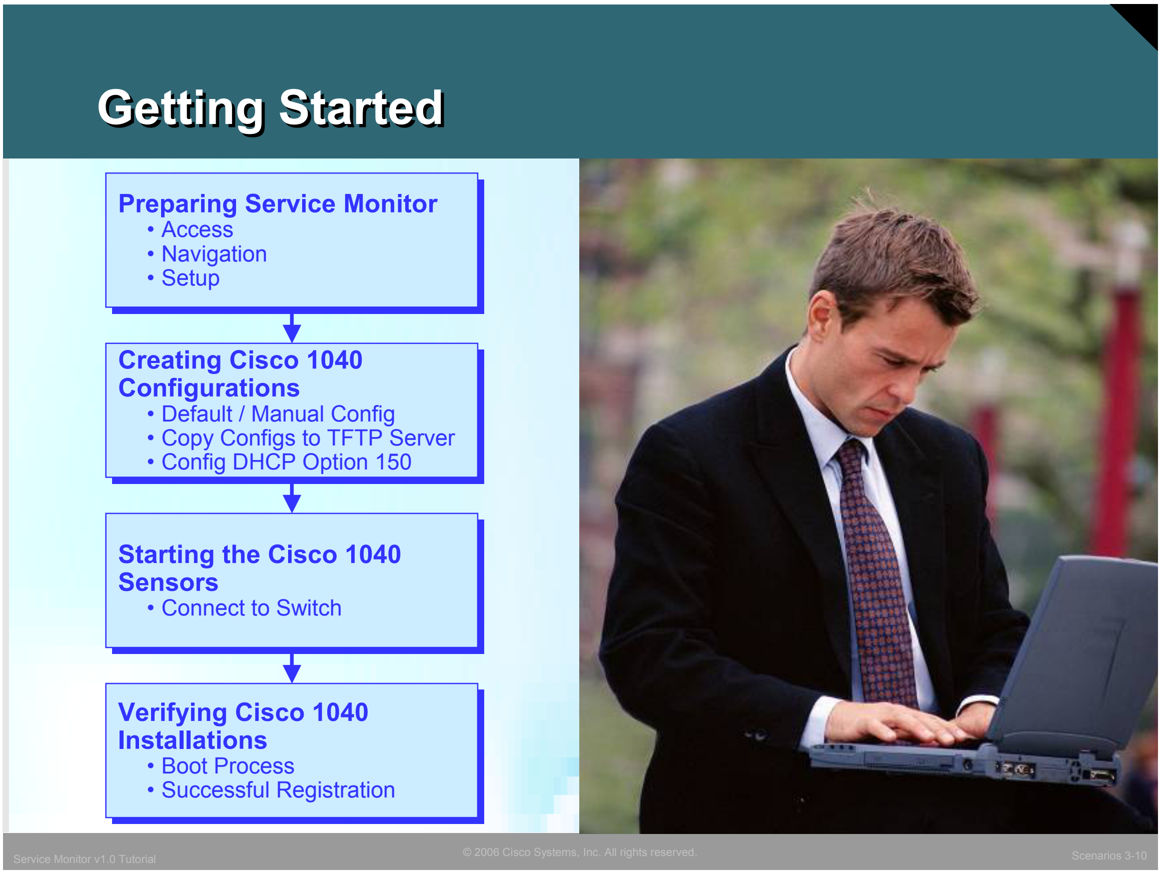
It is always a good idea to check the latest Release Notes for up-to-date information regarding system requirements.

Getting Started

Planning

Getting Started

Monitoring Active Calls



Getting Started

Preparing Service Monitor
- Access
- Navigation
- Setup

Creating Cisco 1040 Configurations
- Default / Manual Config
- Copy Configs to TFTP Server
- Config DHCP Option 150

Starting the Cisco 1040 Sensors
- Connect to Switch

Verifying Cisco 1040 Installations
- Boot Process
- Successful Registration

Getting Started

In this scenario, Getting Started, Dean is going to complete 4 main tasks:

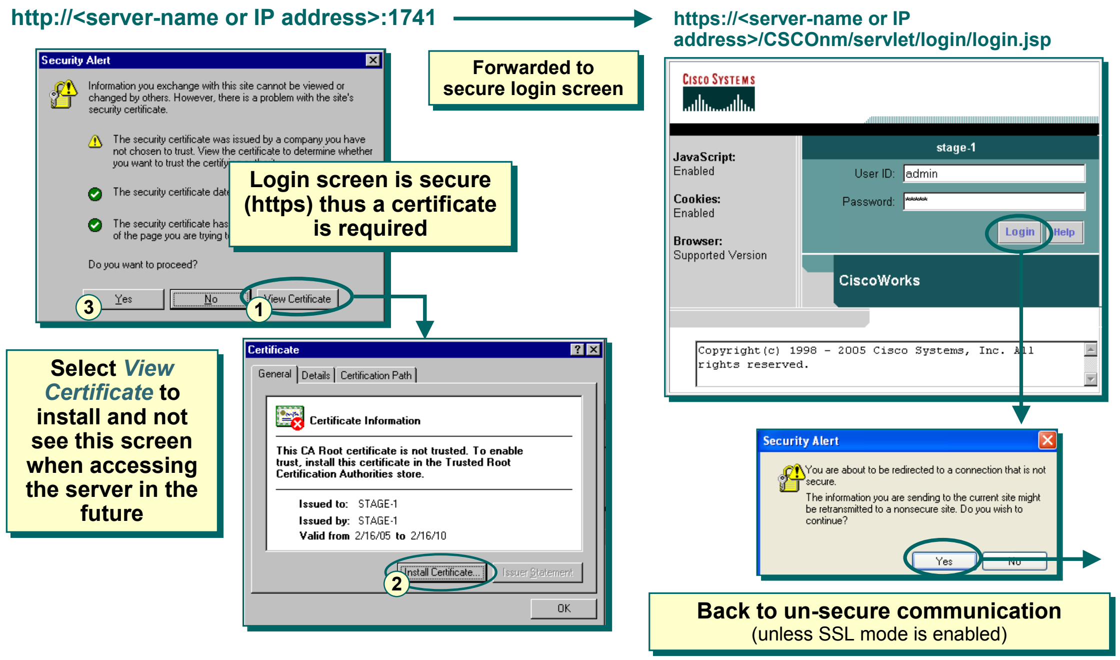
1. **Preparing Service Monitor** – For this task, Dean will access the Service Monitor application, log in, get comfortable in the navigation of menus and location of tasks, and complete the ***Setup*** task. (To understand SM security, including how to create local users, see Chapter 4, System Administration.)

2. **Creating Cisco 1040 Configurations** –Dean will create a default configuration to be used by the two Cisco 1040 sensors at the headquarters building, and create a specific configuration for the sensor at the branch office. Dean will also look at the configurations necessary for the DHCP server and the TFTP server.

3. **Starting the Cisco 1040 Sensors** –Dean will connect the sensors to the switch and watch the boot process to make sure everything is OK.

4. **Verifying Communications** – To ensure operational readiness, Dean will verify that the Cisco 1040 sensors have properly registered and are communicating with the Service Monitor server.

Getting Started
Accessing the Service Monitor Server



http://<server-name or IP address>:1741

https://<server-name or IP address>/CSCOnm/servlet/login/login.jsp

Forwarded to secure login screen

Login screen is secure (https) thus a certificate is required

Select *View Certificate* to install and not see this screen when accessing the server in the future

Back to un-secure communication (unless SSL mode is enabled)

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certify

The security certificate date

The security certificate has of the page you are trying t

Do you want to proceed?

3 Yes | No | 1 View Certificate

Certificate

General | Details | Certification Path

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: STAGE-1

Issued by: STAGE-1

Valid from 2/16/05 to 2/16/10

2 Install Certificate... | Issuer Statement

OK

Cisco Systems

JavaScript: Enabled

Cookies: Enabled

Browser: Supported Version

stage-1

User ID: admin

Password: *****

Login | Help

CiscoWorks

Copyright(c) 1998 - 2005 Cisco Systems, Inc. All rights reserved.

Security Alert

You are about to be redirected to a connection that is not secure.

The information you are sending to the current site might be retransmitted to a nonsecure site. Do you wish to continue?

Yes | No

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Scenarios 3-11

Access the Service Monitor Server

Accessing the Service Monitor server is easy, Dean simply enters the server's DNS name or IP address followed by the http port being used (port 1741 is used by default during installation) as a URL in a standard web browser (see Chapter 4 for complete client requirements):

http://<server-name or IP address>:1741

The login is done using a secure transaction (https). Prior to being redirected to a secure page displaying the login banner, a pop-up *Security Alert* is displayed informing Dean of a problem with the security certificate. To continue, Dean can select **Yes**, but the Security Alert will continue to be presented at each subsequent login. To stop this behavior, Dean installs the certificate by selecting **View Certificate**. The *Certificate* dialog is displayed and Dean selects **Install Certificate** and follows the instructions presented. When finished, Dean selects **OK** in the *Certificate* dialog, and then **Yes** on the Security Alert window.

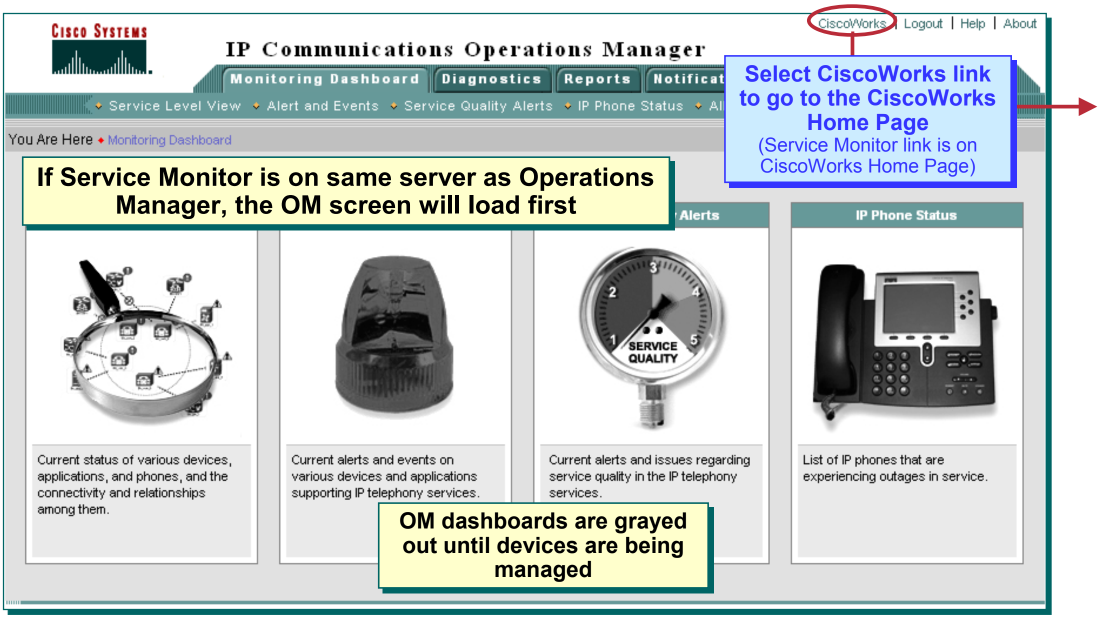
The Login banner will now be displayed on a secured page (https). Dean enters the Admin user account information and password (created during installation) and selects **Login**. An alert informing him that the page will be redirected from a secure page to an un-secure page (https -> http) is displayed for acknowledgement.

Note(s):

- For more information on creating users, see Chapter 4 of this tutorial for a quick overview, and refer to the CiscoWorks Common Services tutorial for complete details.

Getting Started

Navigation – Operations Manager (OM) Desktop



Current status of various devices, applications, and phones, and the connectivity and relationships among them.

Current alerts and events on various devices and applications supporting IP telephony services.

Current alerts and issues regarding service quality in the IP telephony services.

List of IP phones that are experiencing outages in service.

Select CiscoWorks link to go to the CiscoWorks Home Page
(Service Monitor link is on CiscoWorks Home Page)

If Service Monitor is on same server as Operations Manager, the OM screen will load first

OM dashboards are grayed out until devices are being managed

Navigation – Operations Manager Desktop

Since this instance of Service Monitor is co-resident with Operations Manager, after successful login authentication, the desktop for Operations Manager will be displayed. By default, the Monitoring Dashboard tab is selected. (If no devices exist in the Operations Manager inventory, all dashboards are grayed out.)

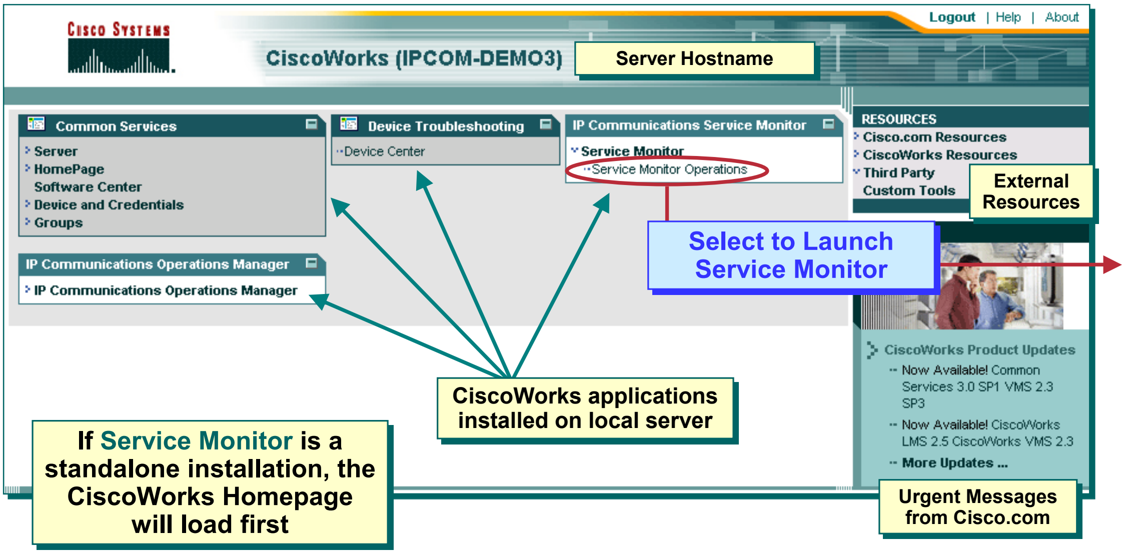
To actually get to the Service Monitor desktop, the next step is to launch the CiscoWorks homepage. Dean does this by selecting the **CiscoWorks** link in the upper right-hand corner of the screen.

Note(s):

- The ***Help*** link will open a new browser window and take to you an extensive on-line help system for the application. The ***About*** link will report on the running version of the application.

Getting Started

Navigation - CiscoWorks Homepage



Server Hostname

External Resources

Select to Launch Service Monitor

CiscoWorks applications installed on local server

If Service Monitor is a standalone installation, the CiscoWorks Homepage will load first

Urgent Messages from Cisco.com

Navigation - CiscoWorks Homepage

When launched from the Operations Manager desktop, the CiscoWorks homepage opens in a new window. For most CiscoWorks application, including a standalone instance of Service Monitor, this is the first page that loads. As illustrated above, the CiscoWorks homepage displays the different registered CiscoWorks applications, which are used as launch points to those applications' desktops. The right-hand side of the homepage displays some links to helpful external resources at Cisco.com, as well as, other user defined links to third party applications or tools. Important updates from Cisco can be found in the lower right-hand panel including information about new releases or service packs.

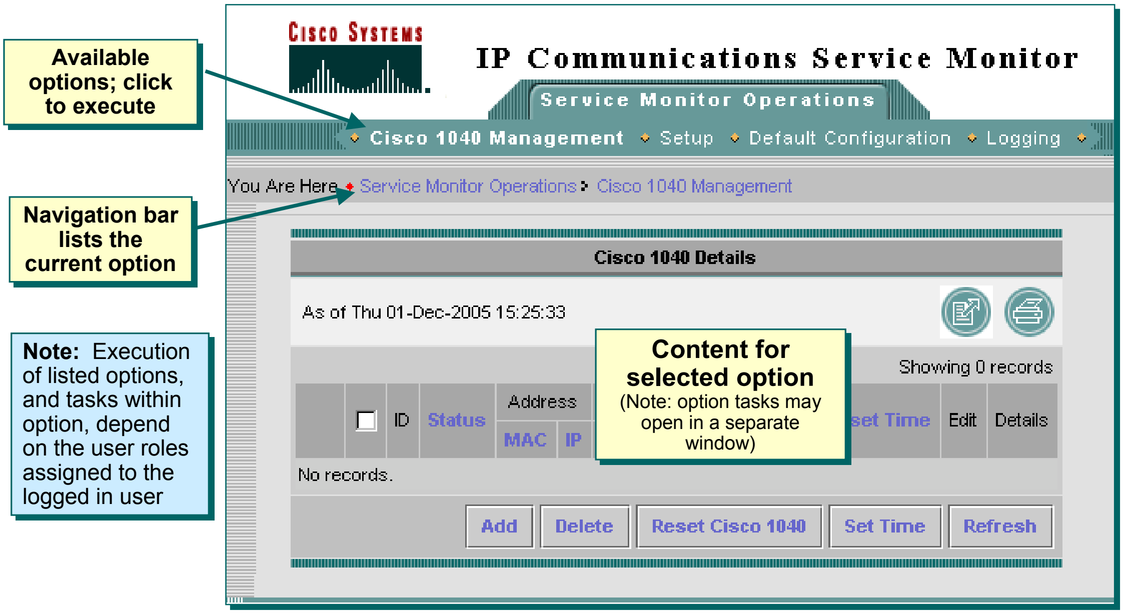
Tasks related to the operations and configuration of the CiscoWorks server (including the creation of users) are performed using the Common Services application. To launch Common Services, find the Common Services panel and click on the header to take you to the main window for Common Services, or select one of the Common Services tasks listed to go directly to that task.

Dean can now launch the Service Monitor desktop by either clicking the header in the **IP Communications Service Monitor** panel or expanding the Service Monitor entry and clicking the **Service Monitor Operations** task.

Note(s):

- For more information regarding the CiscoWorks homepage and tasks within the Common Service application, refer to the CiscoWorks Common Services tutorial.

Getting Started
Navigation - Desktop Layout



IP Communications Service Monitor

Cisco 1040 Management • Setup • Default Configuration • Logging

You Are Here • Service Monitor Operations > Cisco 1040 Management

Cisco 1040 Details

As of Thu 01-Dec-2005 15:25:33

Showing 0 records

	☐	ID	Status	Address		...	set Time	Edit	Details
				MAC	IP				

No records.

Available options; click to execute

Navigation bar lists the current option

Note: Execution of listed options, and tasks within option, depend on the user roles assigned to the logged in user

Content for selected option
(Note: option tasks may open in a separate window)

Navigation - Desktop Layout

The Service Monitor desktop is now displayed in a new window. Though there are only a few tasks within Service Monitor, it would still be beneficial to discuss the basic layout to assist in navigation.

All CiscoWorks applications employ the same user interfaces and layouts. The applications' desktops appear as a series of folders representing the major task categories (SM only has 1 folder). The contents of these folders are accessible by selecting the appropriate folder tab. The currently selected folder is identifiable by the different color of the tab and its text. Immediately under the tabs are the options associated with the selected folder. This bar is the same color as the selected tab helping to further identify which tab is selected. To select one of these options, simply click on it. The selected option will then be displayed in bold text (the selected option in the picture above is 'Cisco 1040 Management'). At this point, the selected option may have a dialog box associated with it, which will be displayed in the content area. The selected option may also have sub-tasks associated with it. These will be listed in a Table of Content (TOC) dialog on the left-hand side of the screen. Again, to select one of the sub tasks, simply click it and its text will now become bold to identify it as the selected task.

When the selected task has no further sub-tasks, a dialog box with further instructions or simply displaying the requested information will be shown in the content display area. To determine where the user currently is, the display line (appropriately titled "You Are Here") under the tab options indicates the path currently selected.

Note(s):

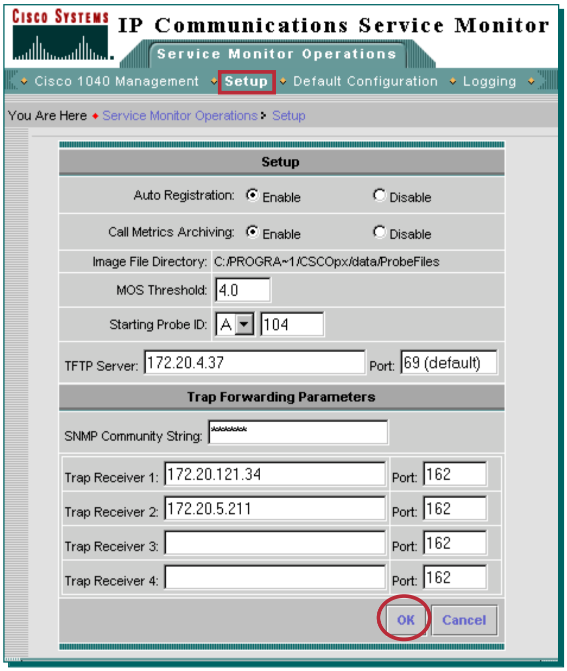
- Often times in this tutorial the entire desktop is not always shown. To facilitate the user in understanding what task is being displayed, the following notation is used to represent the options selected:

  application > folder tab > option > TOC sub-task

  For example to access the Local User Setup task, the user would go to the Common Services application, click the Server folder tab, then click the Security option, and finally the Local User Setup sub-task from the TOC. The tutorial will denote this selection as:

  Common Services > Server > Security > Local User Setup

Getting Started
Setup


Cisco Systems
IP Communications Service Monitor
Service Monitor Operations
Cisco 1040 Management
Setup
Default Configuration
Logging
You Are Here • Service Monitor Operations > Setup

Setup

Auto Registration: ● Enable ○ Disable

Call Metrics Archiving: ● Enable ○ Disable

Image File Directory: C:/PROGRA~1/CSCOpx/data/ProbeFiles

MOS Threshold: 4.0

Starting Probe ID: A 104

TFTP Server: 172.20.4.37 Port: 69 (default)

Trap Forwarding Parameters

SNMP Community String: ******

Trap Receiver 1: 172.20.121.34 Port: 162

Trap Receiver 2: 172.20.5.211 Port: 162

Trap Receiver 3: Port: 162

Trap Receiver 4: Port: 162

OK Cancel

Auto-Registration
Enable - 1040s will automatically register with the SM defined in default config file
Disable - 1040 only registers with an SM server if a specific config file is available

Call Metrics Archiving
After analysis, Service Monitor saves data from 1040s to disk files, if option is enabled

MOS Threshold
If received MOS value, sent by Cisco 1040 sensor, is below this defined value, a SNMP trap is generated

Starting Probe ID
SM assigns this value to the first Cisco 1040 to register; then increments for every sensor thereafter

TFTP Server
IP address of a TFTP server where the Cisco 1040s will retrieve their configurations

Trap Receiver
Enter up to 4 IP addresses of servers to receive threshold violation traps (i.e. OM) when they occur

Setup

Dean is now ready to configure Service Monitor to get the application ready for his environment and monitoring needs. These are the steps Dean performs in the Setup task.

1. From the Service Monitor desktop, Dean starts by selecting the **Setup** tab.
2. The *Setup* dialog is displayed in the Content area of the screen. Dean sets the following:

   Auto Registration – ***Enabled***, a Cisco 1040 sensor joining the network will automatically register with a Service Monitor using information provided in the default configuration file. (If Dean set this option to ***Disabled***, a Cisco 1040 sensor joining the network, will only register with a Service Monitor if a configuration file specifically for that Cisco 1040 has been created.)

   Call Metrics Archiving –**Enabled**, all metrics received from the 1040s will be archived to a flat file on a daily basis. Dean needs to enable this to meet the SLA verification requirement.

   MOS Threshold – User-defined threshold used to analyze received MOS values against. The SLA agreement with the VoIP provider says all calls will receive a MOS score of better than 4.0, hence Dean sets the threshold to 4.0 to be informed of any non conforming calls.

   Starting Probe ID – Since Auto Registration is enabled, SM will assigns this ID to the first Cisco 1040 using the Default configuration to register with it. This ID will increment for each subsequent Cisco 1040 to register. If Auto Registration is Disabled or a specific 1040 configuration exists, the probe ID is configured in the manual configuration for the sensor.

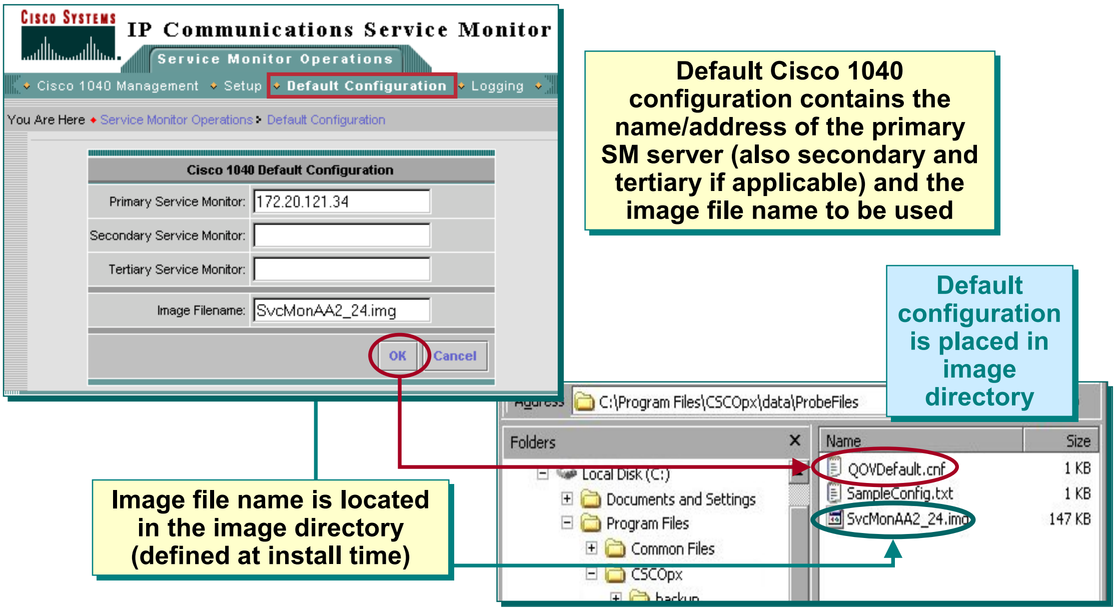
   TFTP Server and Port – Dean sets this field to the IP address of the TFTP Server.

   SNMP Community String – SNMP community string for the trap receivers. Default is public.

   Trap Receivers – IP Address or DNS name for up to 4 trap receivers. These are the servers that SM will send SNMP traps to if a threshold is violated. Dean sets one entry to the IP address of the Operations Manager server and the other to an enterprise network management system (NMS) that they are evaluating. By default, most NMS use UDP port 162 for receiving SNMP traps. This port can not be shared by other local applications.
3. Dean selects **OK** to have the Setup configuration take effect.

Getting Started

Creating the Cisco 1040 Default Configuration



Cisco Systems
IP Communications Service Monitor
Service Monitor Operations
Cisco 1040 Management
Setup
Default Configuration
Logging
You Are Here ♦ Service Monitor Operations ▸ Default Configuration

Cisco 1040 Default Configuration

Primary Service Monitor: 172.20.121.34

Secondary Service Monitor:

Tertiary Service Monitor:

Image Filename: SvcMonAA2_24.img

Default Cisco 1040 configuration contains the name/address of the primary SM server (also secondary and tertiary if applicable) and the image file name to be used

Default configuration is placed in image directory

Image file name is located in the image directory (defined at install time)

Creating the Default Cisco 1040 Configuration

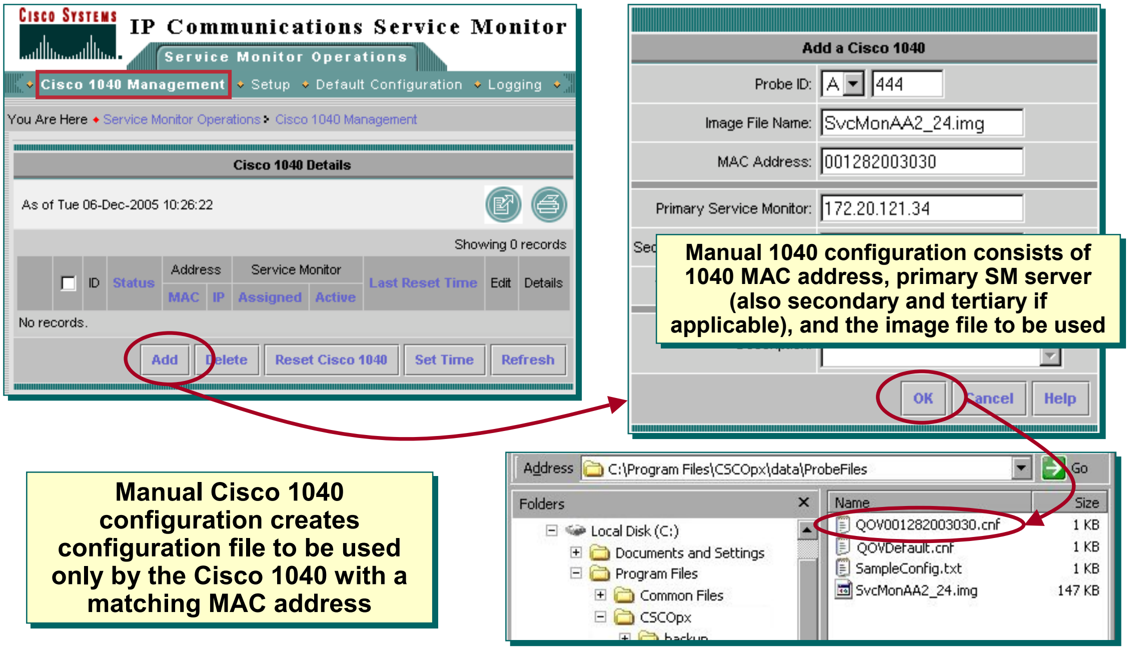
The next step is for Dean to create the configurations for the Cisco 1040 sensors. Dean decides to have the two Cisco 1040s in the headquarters building use the default configuration. This is possible since ***Auto Registration*** was enabled during the **Setup** task.

1. Dean selects the **Default Configuration** task from the list of four options under the **Service Monitor Operations** tab.
2. The Cisco 1040 Default Configuration dialog is displayed. The configuration couldn't be simpler – Dean simply enters the IP address of the Service Monitor server and the name of the 1040 binary image. (The image is located in the directory listed by the Setup task and set during installation). Optionally, if so deployed, a secondary and tertiary SM server can be added to the default configuration for fail over operations.
3. When the **OK** button is clicked, Service Monitor generates the default configuration and places it in the directory selected during installation (listed by the Setup task). The file has the format of QOVDefault.cnf.

.

Getting Started

Creating the Cisco 1040 Manual Configuration



IP Communications Service Monitor

You Are Here • Service Monitor Operations > Cisco 1040 Management

Cisco 1040 Details

As of Tue 06-Dec-2005 10:26:22

Showing 0 records

	ID	Status	Address MAC	 IP	Service Monitor Assigned	 Active	Last Reset Time	Edit	Details

No records.

Add a Cisco 1040

Probe ID: A 444

Image File Name: SvcMonAA2_24.img

MAC Address: 001282003030

Primary Service Monitor: 172.20.121.34

Manual 1040 configuration consists of 1040 MAC address, primary SM server (also secondary and tertiary if applicable), and the image file to be used

Address C:\Program Files\CSCOpx\data\ProbeFiles

Name	Size
QOV001282003030.cnf	1 KB
QOVDefault.cnf	1 KB
SampleConfig.txt	1 KB
SvcMonAA2_24.img	147 KB

Manual Cisco 1040 configuration creates configuration file to be used only by the Cisco 1040 with a matching MAC address

Creating Manual or Specific Cisco 1040 Configurations

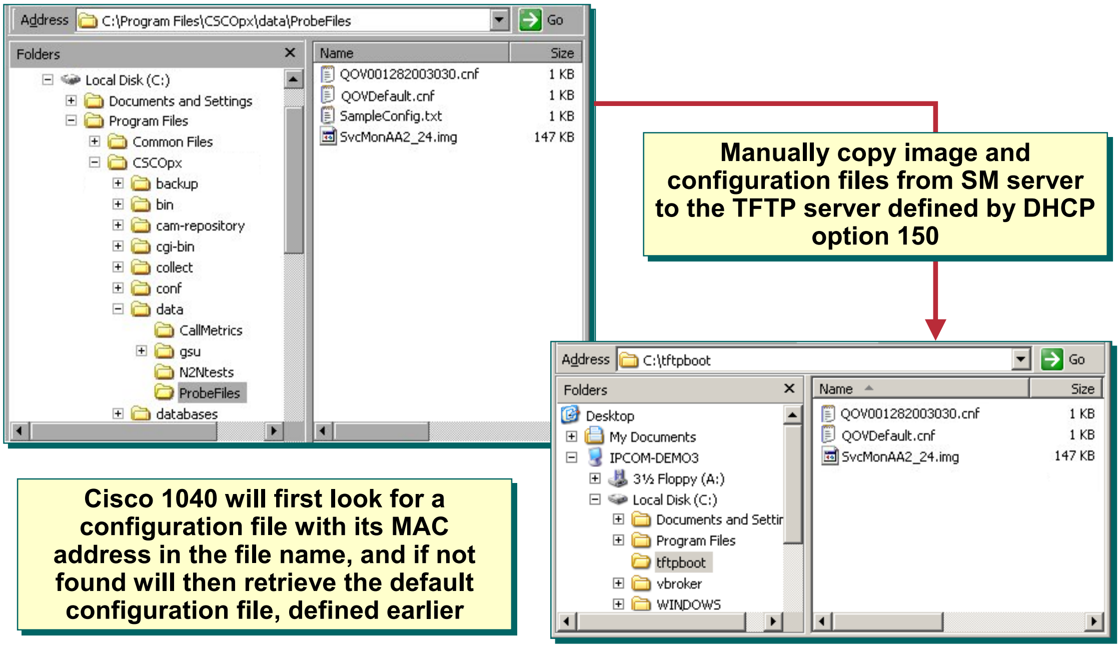
Dean wants to create a specific configuration for the Cisco 1040 because long term plans has the branch office getting its own management server. So to minimize the reconfiguration necessary when that day comes, Dean chooses to create a specific configuration for this sensor by performing these steps:

1. Dean selects the **Cisco 1040 Management** task.
2. The *Cisco 1040 Details* dialog is displayed showing a list of any previously defined or registered Cisco 1040s. Dean selects ***Add*** to create an individual configuration for the branch office 1040.
3. The *Add a Cisco 1040* dialog is displayed. Like before, Dean enters both the IP address of the Service Monitor server and the name 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 him. Also, Dean selects the Probe ID for the sensor. If so deployed, a secondary and tertiary SM server can also be added.
4. When the **OK** button is clicked, Service Monitor generates the specific configuration and places it in the directory defined during installation (listed by the Setup task). The file has the format of QOV<*1040_mac_address*>.cnf.

Note(s):

- In the future, when a new primary Service Monitor is brought on line for the branch office, Dean will need to edit this configuration to change the IP address of the primary server. The file will then need to be copied to the TFTP server, and the sensor must then be reset (using the **Reset Cisco 1040** button in the *Cisco 1040 Details* dialog) in order to begin using the new configuration.

Getting Started
Copy Files to TFTP Server



Address C:\Program Files\CSCOpx\data\ProbeFiles

Name	Size
QOV001282003030.cnf	1 KB
QOVDefault.cnf	1 KB
SampleConfig.txt	1 KB
SvcMonAA2_24.img	147 KB

Manually copy image and configuration files from SM server to the TFTP server defined by DHCP option 150

Address C:\tftpboot

Name	Size
QOV001282003030.cnf	1 KB
QOVDefault.cnf	1 KB
SvcMonAA2_24.img	147 KB

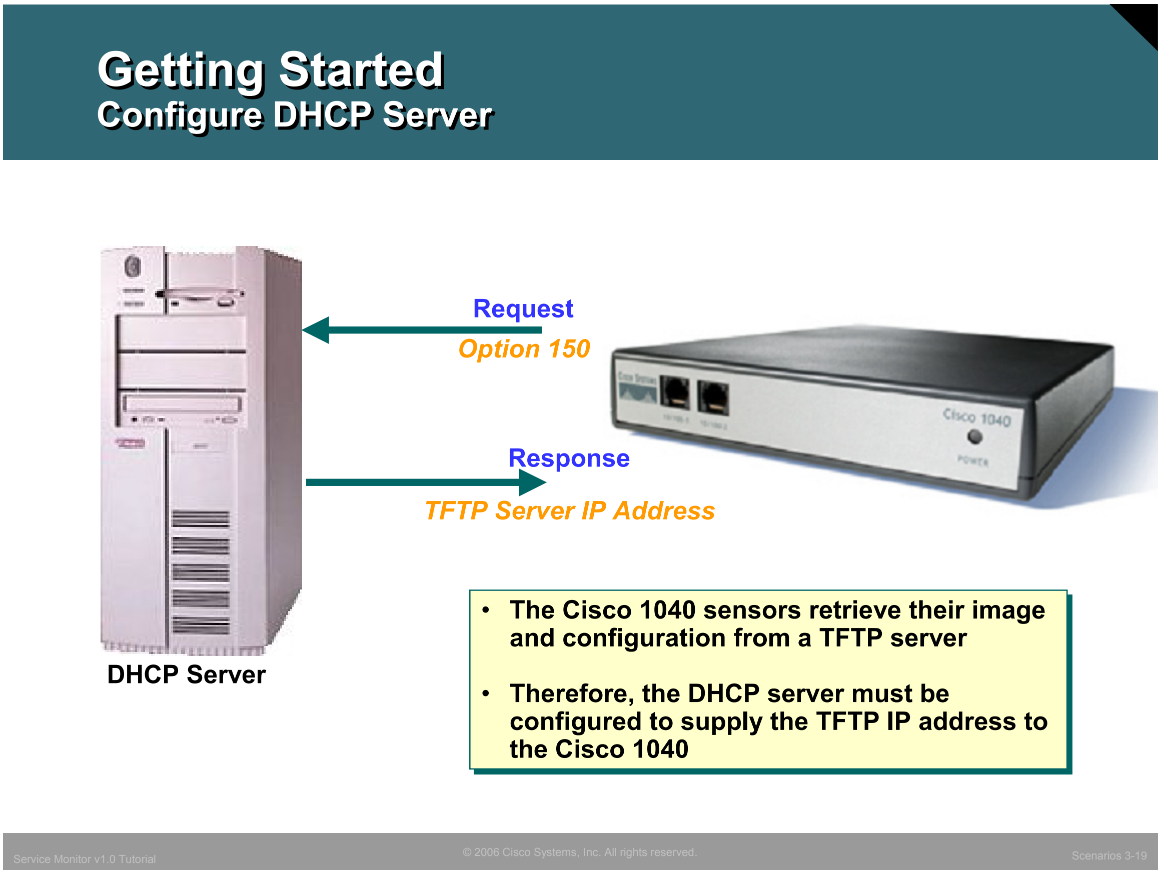
Cisco 1040 will first look for a configuration file with its MAC address in the file name, and if not found will then retrieve the default configuration file, defined earlier

Copy Files 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 Dean must copy all 1040 configuration and image files from the SM server to the TFTP server prior to bringing any 1040 on-line. The 1040s will always first attempt to pull a specific configuration from the TFTP server and if none exists, will then attempt to pull the the default configuration.

Note(s):

- This is a manual process, no Service Monitor task exists to perform this operation. Therefore, Dean must have access to the server's console to perform this step.



Getting Started

Configure DHCP Server

Request

Option 150

Response

TFTP Server IP Address

DHCP Server

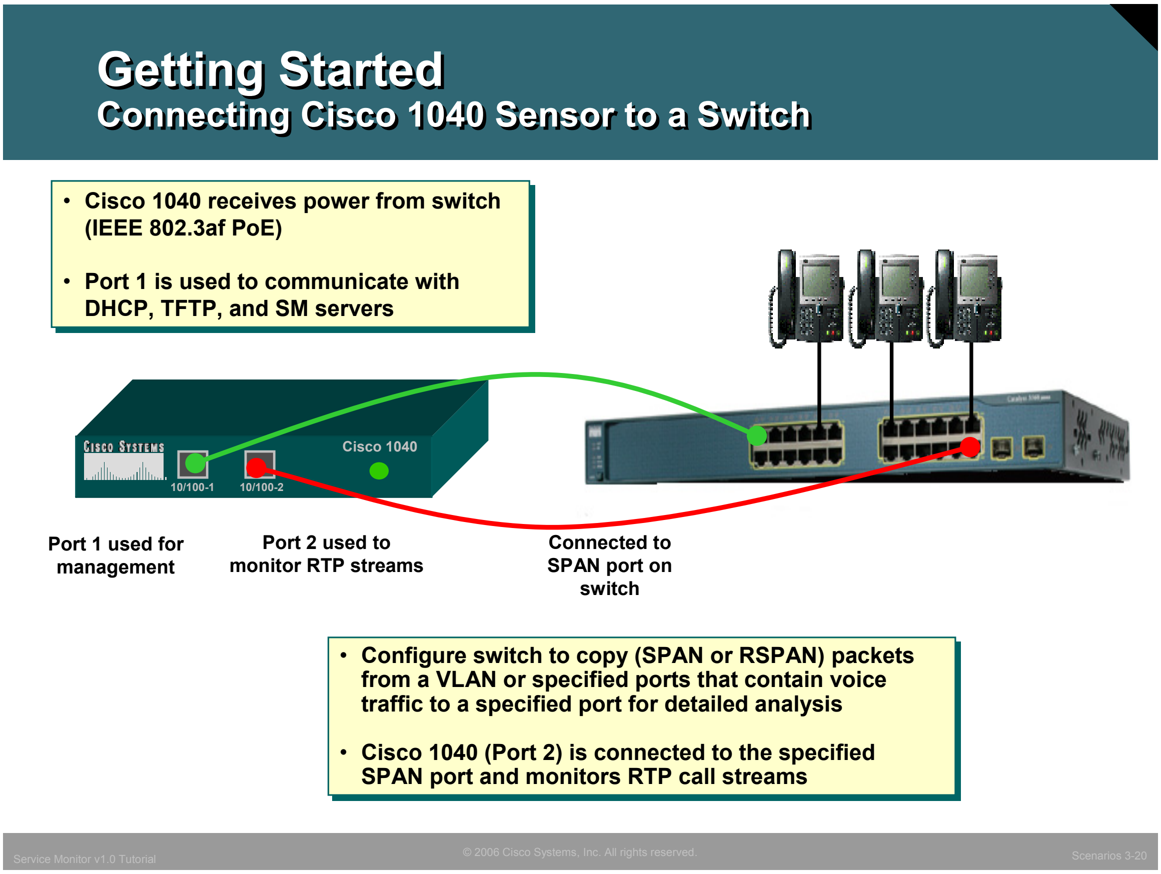
- **The Cisco 1040 sensors retrieve their image and configuration from a TFTP server**
- **Therefore, the DHCP server must be configured to supply the TFTP IP address to the Cisco 1040**

Service Monitor v1.0 Tutorial

Scenarios 3-19

Configure DHCP Server

As just discussed, the Cisco 1040s will pull their image and configuration files from the TFTP server, but how do they know which TFTP server to go to? 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. The DHCP server must be configured to respond to this request with the IP address of the TFTP server where the sensor files resides.



Getting Started

Connecting Cisco 1040 Sensor to a Switch

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

Port 1 used for management

Port 2 used to monitor RTP streams

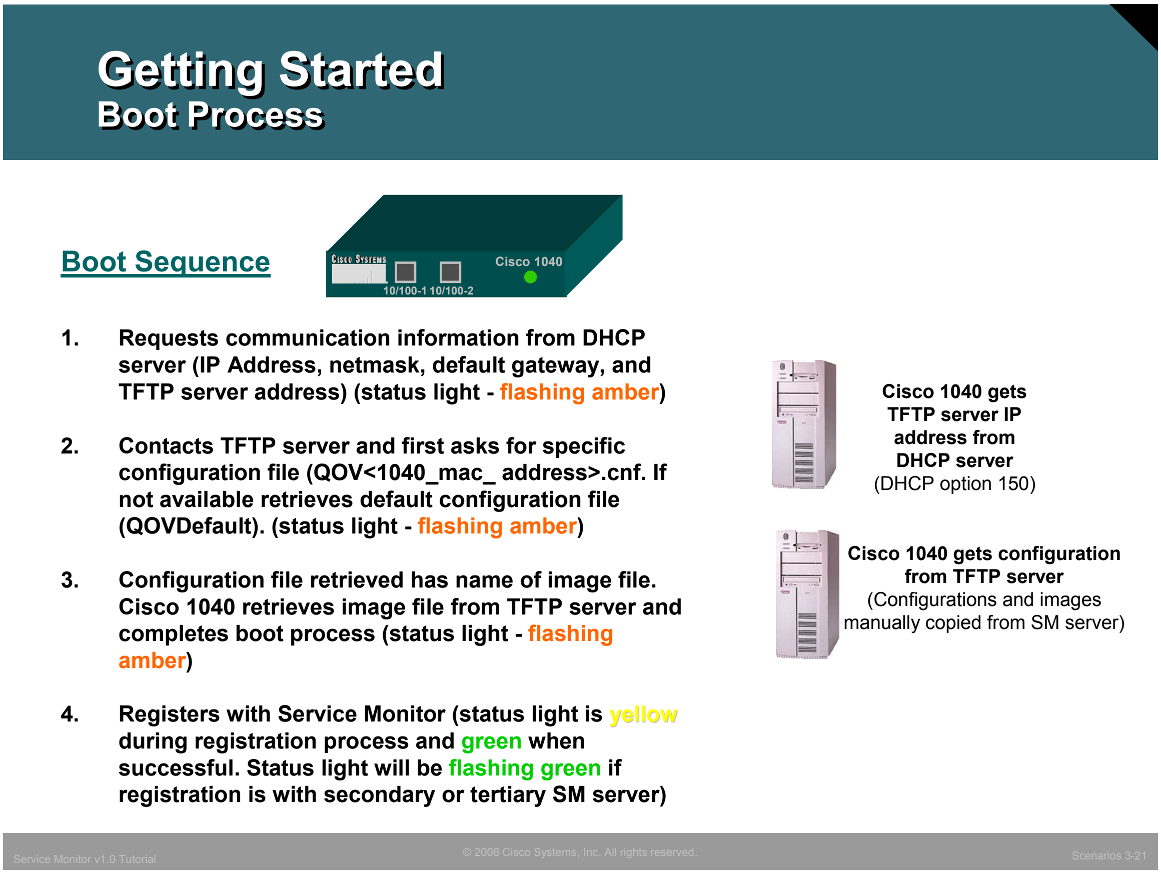
Connected to SPAN port on switch

- 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

Connecting Cisco 1040 to a Switch

Dean has waited until now to actually install the Cisco 1040 sensors because as soon as they are connected to a switch supporting IEEE 802.3af PoE, they power up and begin their boot cycle which includes retrieving its image and configuration files from the TFTP server.

Each Cisco 1040 has two Ethernet 10/100 ports. 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. The second port is used for monitoring call streams. Typically it is connected to a SPAN port on a switch.



Cisco Systems
Cisco 1040
10/100-1 10/100-2

Getting Started

Boot Process

Boot Sequence

1. **Requests communication information from DHCP server (IP Address, netmask, default gateway, and TFTP server address) (status light - flashing amber)**

2. **Contacts 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 amber)**

3. **Configuration file retrieved has name of image file. Cisco 1040 retrieves image file from TFTP server and completes boot process (status light - flashing amber)**

4. **Registers with Service Monitor (status light is yellow during registration process and green when successful. Status light will be flashing green if registration is with secondary or tertiary SM server)**

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

Cisco 1040 gets configuration from TFTP server
(Configurations and images manually copied from SM server)

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Scenarios 3-21

Cisco 1040 Boot Process

Once Dean connects Port 1 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.

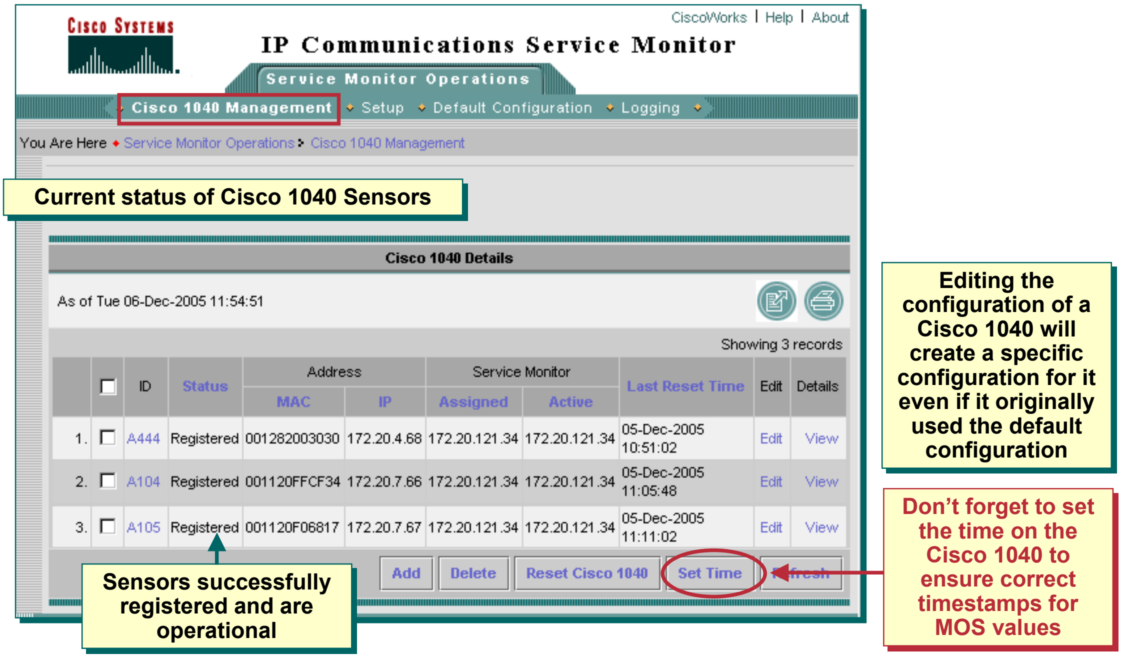
Once the configuration file is retrieved, the Cisco 1040 looks in the configuration file to get the name of the image it is to use, and then pulls it from the TFTP server. Once received, the Cisco 1040 loads the image.

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, and then tertiary if configured; 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 or tertiary server.

Getting Started
Cisco 1040 Registration with Service Monitor


Cisco Systems
CiscoWorks | Help | About
IP Communications Service Monitor
Service Monitor Operations
Cisco 1040 Management ◆ Setup ◆ Default Configuration ◆ Logging ◆
You Are Here ◆ Service Monitor Operations ▸ Cisco 1040 Management
Add
Delete
Reset Cisco 1040
Set Time
Refresh

Cisco 1040 Details

As of Tue 06-Dec-2005 11:54:51

Showing 3 records

	☐	ID	Status	Address		Service Monitor		Last Reset Time	Edit	Details
				MAC	IP	Assigned	Active			
1.	☐	A444	Registered	001282003030	172.20.4.68	172.20.121.34	172.20.121.34	05-Dec-2005 10:51:02	Edit	View
2.	☐	A104	Registered	001120FFCF34	172.20.7.66	172.20.121.34	172.20.121.34	05-Dec-2005 11:05:48	Edit	View
3.	☐	A105	Registered	001120F06817	172.20.7.67	172.20.121.34	172.20.121.34	05-Dec-2005 11:11:02	Edit	View

Current status of Cisco 1040 Sensors

Sensors successfully registered and are operational

Editing the configuration of a Cisco 1040 will create a specific configuration for it even if it originally used the default configuration

Don't forget to set the time on the Cisco 1040 to ensure correct timestamps for MOS values

Cisco 1040 Registration with Service Monitor

The sensors are now ready to begin monitoring active calls for quality of voice; however, Dean still needs to configure the SPAN port on the switch before the Cisco 1040 will actually see traffic to analyze. Before doing that, Dean wants to check with the SM server to make sure the Cisco 1040s registered correctly and set the time on them to ensure consistent time-stamping for the reported MOS values.

Dean uses the **Cisco 1040 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 SM was either the secondary or tertiary server for a Cisco 1040) or *Unregistered* if the Cisco 1040 was no longer communicating with this SM (perhaps if failed over to a secondary or tertiary server).

To set the current time on a sensor, Dean selects all the listed sensors by checking the box to the left of the ID column header and then clicks the **Set Time** button. The *Confirm* dialog is displayed and Dean clicks **Yes**. The Cisco 1040 Management dialog can also be used to edit/ view configurations and reset or delete a 1040.

Viewing the Configuration File

If Dean wishes to view the configuration file actually being used on the Cisco 1040 (as opposed to the one configured using SM), he could browse to the Cisco 1040 using the following steps:

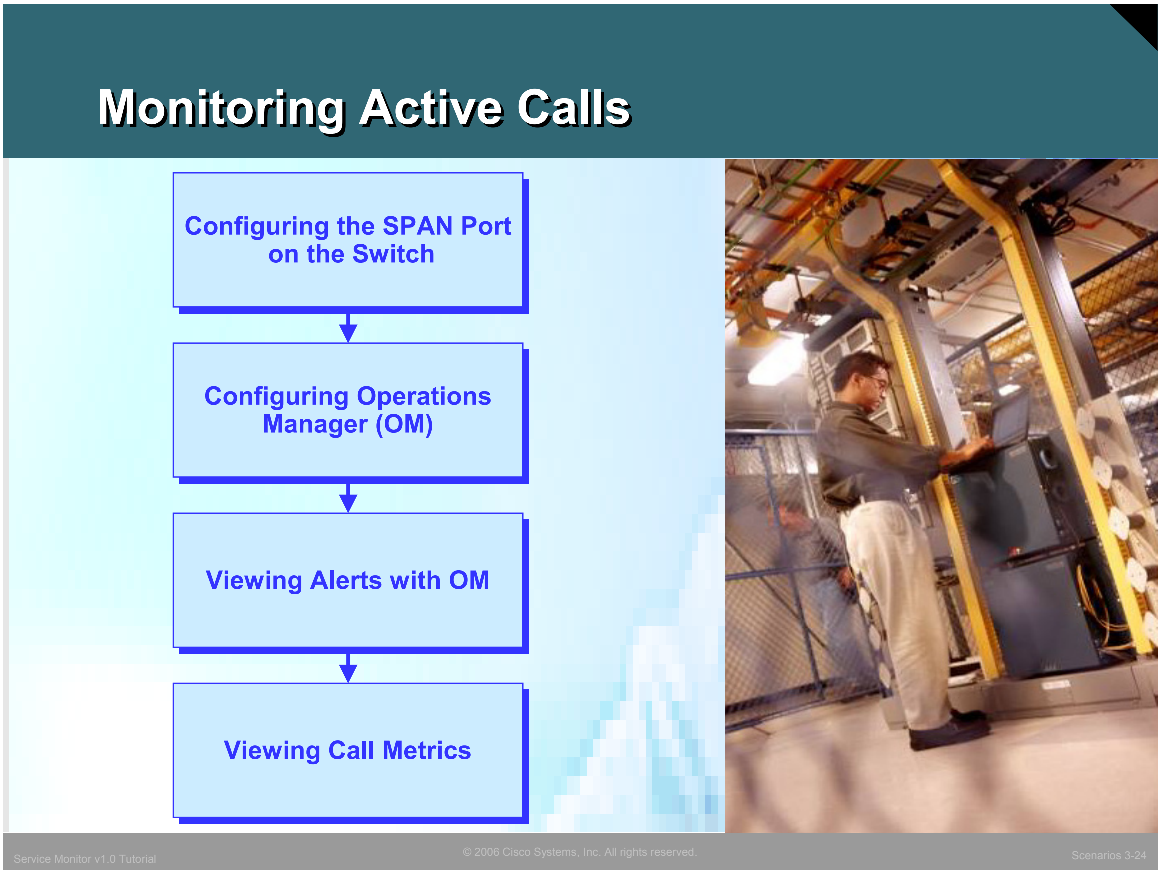
1. From a browser, enter **http://<*Cisco 1040 IP address or DNS name*>/Communication**
2. The *Communication Log File* window displays the following information from the configuration file retrieved from the the TFTP server for this Cisco 1040:
   - **Receiver**—IP address or DNS name of each Service Monitor—primary, secondary, and tertiary—defined in the configuration file, separated by semicolons.
   - **ID**—ID of the Cisco 1040 that uses this configuration file.
   - **Image**—Name of the binary image file that the Cisco 1040 should download from the TFTP server.
   - **Last Updated**—The last time that this configuration file was updated on the Service Monitor system.

Monitoring Active Calls

Planning

Getting Started

Monitoring Active Calls



Monitoring Active Calls

Configuring the SPAN Port on the Switch

Configuring Operations Manager (OM)

Viewing Alerts with OM

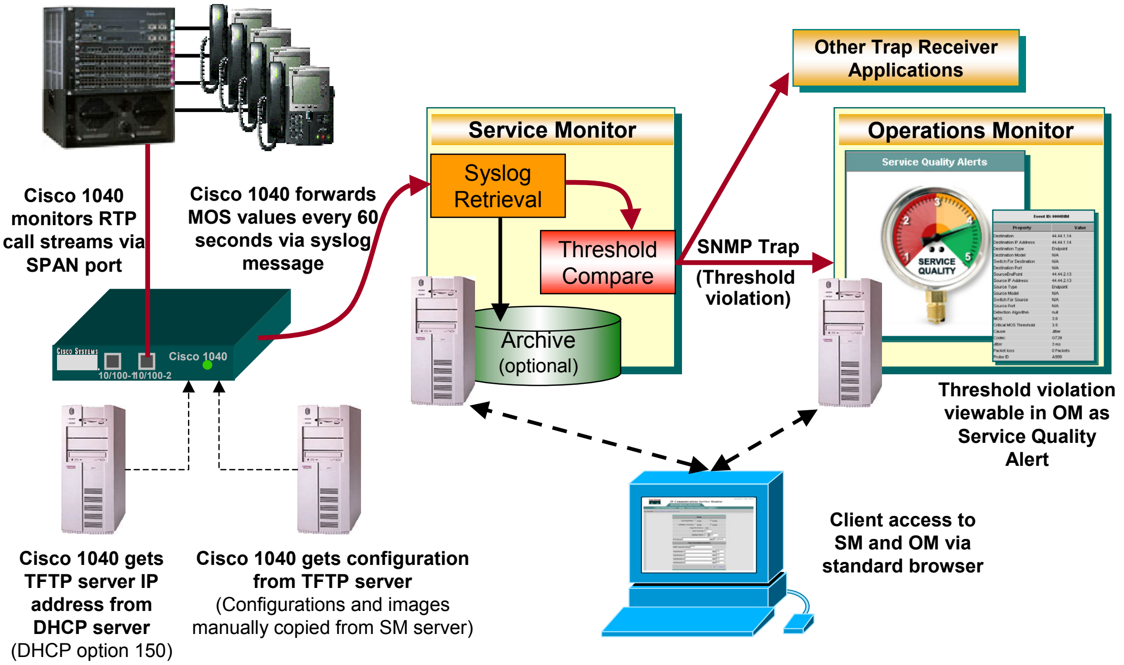
Viewing Call Metrics

Monitoring Active Calls

Dean is now ready to monitor active call streams using the deployed sensors. Dean has just a few more configuration steps, before seeing the results. Dean's remaining tasks include:

1. **Configuring SPAN on the Switch** – Though the Cisco 1040 is configured and ready to analyze voice streams, Dean needs to first send data to the port connected to the Cisco 1040 so that the Cisco 1040 has traffic to analyze.
2. **Configuring Operations Manager** – Dean previously configured Service Monitor to forward MOS violation traps to Operations Manager using the **Setup** task. He must now configure Operations Manager to accept the SNMP traps, and determine what severity level to display them with.
3. **Viewing Alerts** – Now all configurations are complete, and Dean can use the Operations Manager Service Quality Alerts Dashboard to view any MOS violation alerts.
4. **Viewing Call Metrics** – Dean decided to archive all reported MOS values forwarded by the Cisco 1040 to Service Monitor to help him evaluate conformance to SLAs. Dean takes a look at the Call Metrics Archive.

Monitoring Active Calls
Architecture Review



Cisco 1040 monitors RTP call streams via SPAN port

Cisco 1040 forwards MOS values every 60 seconds via syslog message

Service Monitor

Syslog Retrieval

Threshold Compare

Archive (optional)

SNMP Trap (Threshold violation)

Other Trap Receiver Applications

Operations Monitor

Threshold violation viewable in OM as Service Quality Alert

Client access to SM and OM via standard browser

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

Cisco 1040 gets configuration from TFTP server (Configurations and images manually copied from SM server)

Architecture Review

Before taking a look at the final configuration steps and actual results, let's review the Service Monitor architecture to complete the picture.

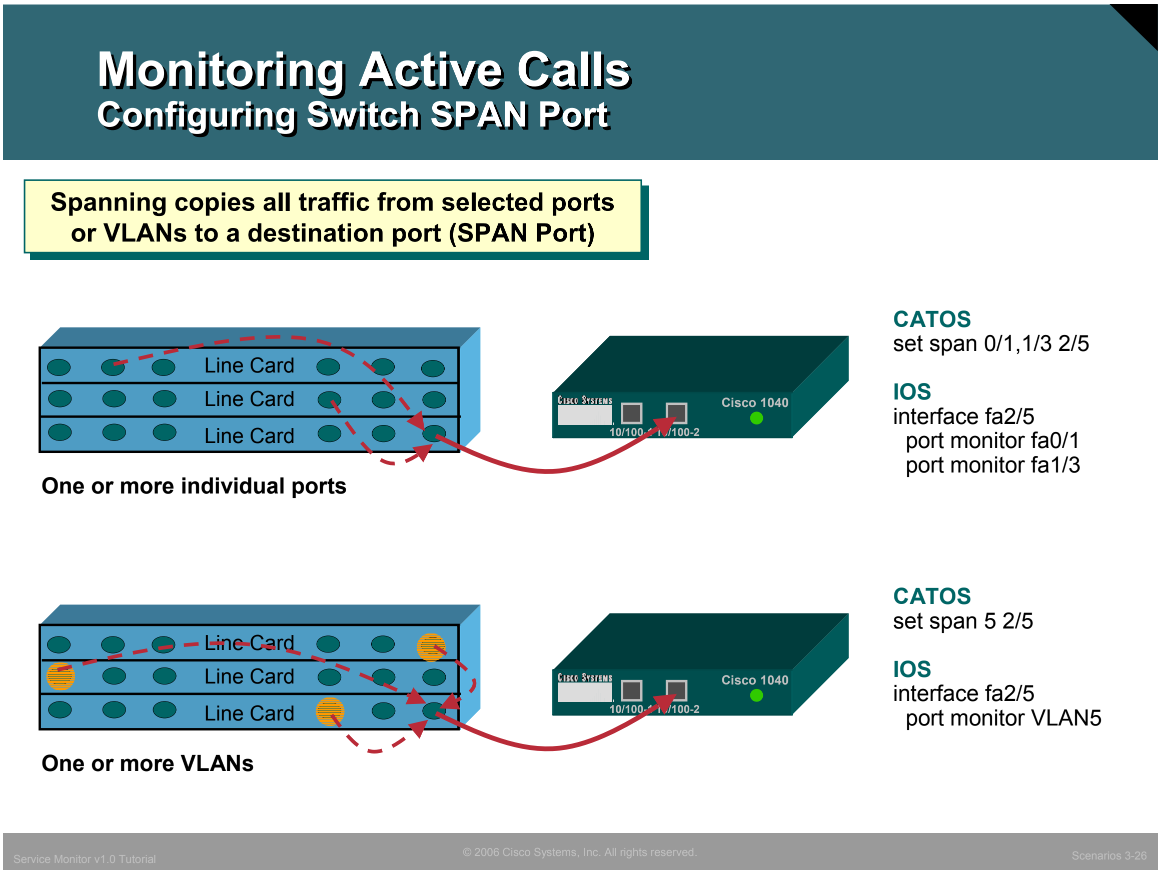
The figure above provides details about the Service monitor architecture and how all the pieces work together. One of the functions of the SM server is to manage the Cisco 1040 sensors. This entails creating the configurations for the sensors which informs the sensor where to forward the quality of voice 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. Port 1 to receive its configuration and report the call metrics to the SM server; and Port 2 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 the SPAN port. The sensor also receives its power from the switch port, using IEEE 802.3af PoE.

The sensors monitor each call stream for 60 seconds and then forwards the metrics to Service Monitor in the form of a Syslog message. The SM server retrieves the Syslog message and compares the MOS metric against a user-defined 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.

Note(s):

- The Cisco 1040 and SM server use keep-alive messages to ensure constant communication. If the Cisco 1040s no longer receive keep-alive messages, it will attempt to register with a backup SM server if so configured. If SM stops receiving keep-alive messages from a Cisco 1040 that is registered to it, SM generates a *Cisco 1040 Unreachable* SNMP trap, and sends this trap to the configured trap recipients. If OM is configured to receive traps from SM, then the *Cisco 1040 Unreachable* trap is displayed on the **Alerts and Events Monitoring** dashboard under the unidentified trap device type.



Monitoring Active Calls
Configuring Switch SPAN Port

Spanning copies all traffic from selected ports or VLANs to a destination port (SPAN Port)

One or more individual ports

CATOS

```
set span 0/1,1/3 2/5
```

IOS

```
interface fa2/5
  port monitor fa0/1
  port monitor fa1/3
```

One or more VLANs

CATOS

```
set span 5 2/5
```

IOS

```
interface fa2/5
  port monitor VLAN5
```

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Scenarios 3-26

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 data to the SPAN port connected to the Cisco 1040. SPAN allows the administrator to forward one or more ports or VLANs to the SPAN port and can even specify the direction (Rx/Tx/Both).

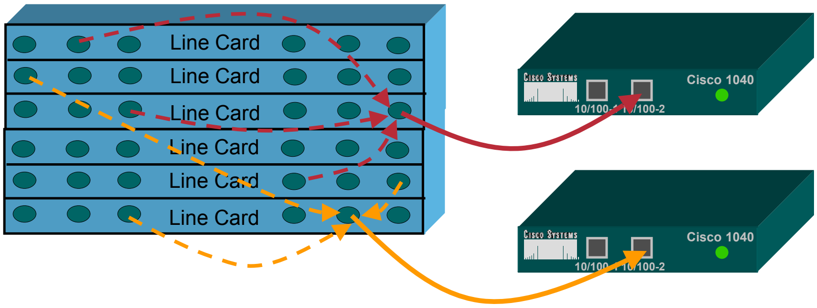
Dean and his fellow engineers configured all their voice traffic to use VLAN 5. Therefore, Dean needs to simply SPAN VLAN 5 to the SPAN port to have the Cisco 1040 begin monitoring and analyzing voice streams.

Note(s):

- One 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. Refer to Chapter 5 for a link to more deployment options found in the Service Monitor Deployment Guide.
- SPAN command syntax varies depending on the device type and OS in use. For details about the SPAN command see the appropriate documentation for your device and OS.

Monitoring Active Calls

Alternative Configurations



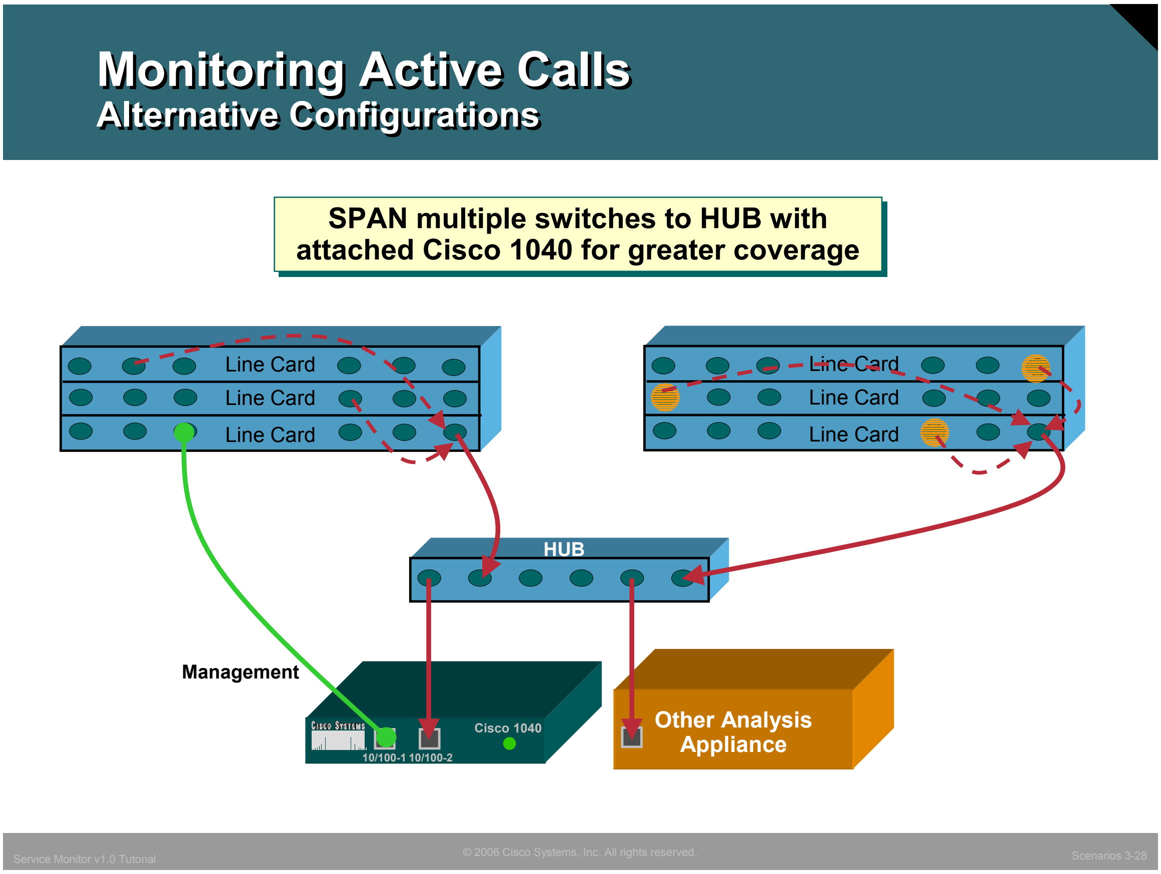
For large switches, with a BHCC exceeding the capacity of one Cisco 1040, use multiple SPAN ports and Cisco 1040s

Alternative Configuration

If his environment required it, Dean has many other options for deploying Cisco 1040s. In the case of large switches with many phones, and a Busy Hour Call Completions (BHCC) exceeding the capability of a single Cisco 1040 (80 active RTP streams per minute), Dean could configure the switch with more than one SPAN port and attach a Cisco 1040 to each.

Note(s);

- 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.



Monitoring Active Calls
Alternative Configurations

SPAN multiple switches to HUB with attached Cisco 1040 for greater coverage

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. Scenarios 3-28

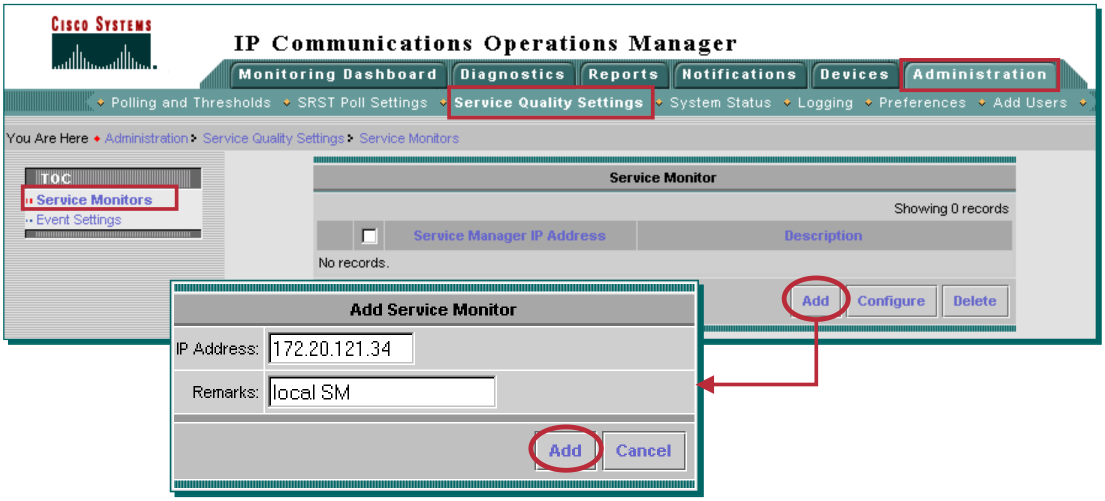
Alternative Configuration

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 the 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.

Monitoring Active Calls

Service Monitor Registration with Operations Manager

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



Service Monitor

Showing 0 records

☐	Service Manager IP Address	Description

No records.

Add Service Monitor

IP Address: 172.20.121.34

Remarks: local SM

Registering Service Monitor with Operations Manager

Dean earlier used the **Setup** task of Service Monitor to forward any MOS Violations as SNMP traps to Operations Manager. Dean must now configure Operations Manager to accept traps from Service Monitor using the following steps:

1. From the Operations Manager’s desktop, Dean selects the **Administration** folder (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, Dean selects the **Service Monitors** task.
4. The *Service Monitor* dialog is displayed listing any currently configured Service Monitor servers. Dean clicks 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.

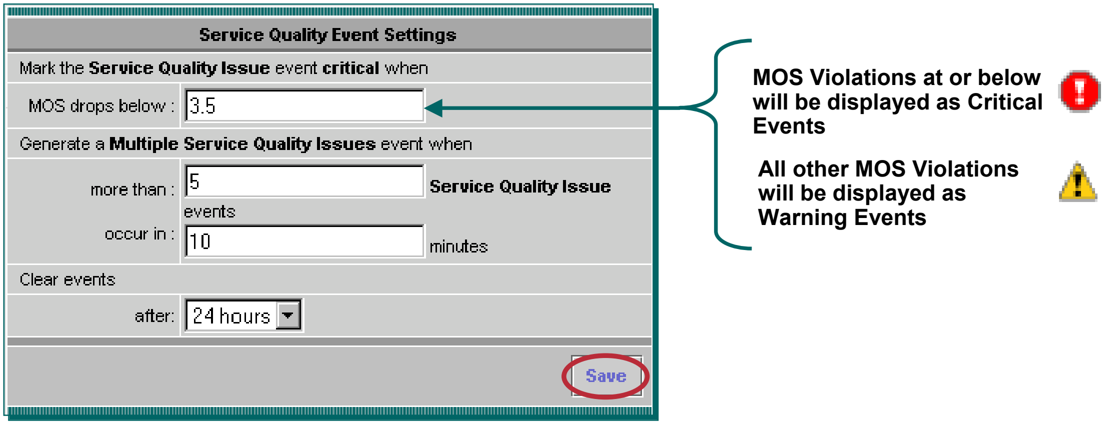
Tip(s):

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

Monitoring Active Calls
Operations Manager Event Settings

Of the MOS Violations received by Operations Manager, set which ones will be marked critical, all others will be set to warning

Operations Manager > Administration > Service Quality Settings > Event Settings



Service Quality Event Settings

Mark the **Service Quality Issue** event **critical** when

MOS drops below : 3.5

Generate a **Multiple Service Quality Issues** event when

more than : 5 **Service Quality Issue** events

occur in : 10 minutes

Clear events

after: 24 hours

MOS Violations at or below will be displayed as Critical Events ❗

All other MOS Violations will be displayed as Warning Events ⚠

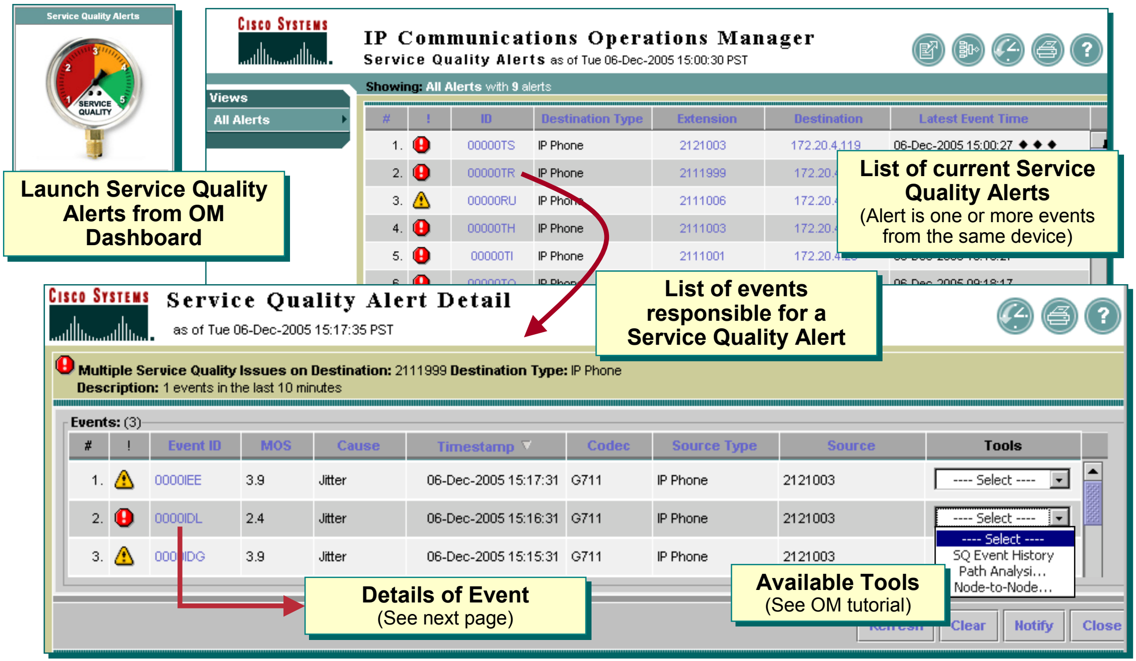
Operations Manager Event Settings

Dean has one final configuration to make before looking at the results. Dean can configure Operations Manager to display different MOS values with different levels of severity. Earlier, Dean configured Service Monitor to send a MOS violation trap for any MOS value of 4.0 or lower. Dean has decided that he wants Operations Manager to display any MOS value of 3.5 or lower as a *Critical* alert and any alert between 3.6 and 4.0 to be marked as a *Warning*. To achieve this, Dean uses the **Event Settings** task located in the Service Quality Settings.

1. From the Operations Manager's desktop, Dean selects 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. Dean sets the *MOS drops below* field to 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. Dean leaves these setting at the default value.
3. Click **Save** to have these parameters take effect.

Service Monitor is now fully configured and operational. Dean is now ready to look at the results.

Monitoring Active Calls
Viewing Alerts – OM Service Quality Alerts Dashboard



Cisco Systems

IP Communications Operations Manager
Service Quality Alerts as of Tue 06-Dec-2005 15:00:30 PST

Showing: All Alerts with **9** alerts

#	!	ID	Destination Type	Extension	Destination	Latest Event Time
1.	❗	00000TS	IP Phone	2121003	172.20.4.119	06-Dec-2005 15:00:27 ◆ ◆ ◆
2.	❗	00000TR	IP Phone	2111999	172.20.4	
3.	⚠	00000RU	IP Phone	2111006	172.20.4	
4.	❗	00000TH	IP Phone	2111003	172.20.4	
5.	❗	00000TI	IP Phone	2111001	172.20.4	
6.	❗	00000TO	IP Phone			06-Dec-2005 09:18:17

List of current Service Quality Alerts
(Alert is one or more events from the same device)
List of events responsible for a Service Quality Alert

Cisco Systems

Service Quality Alert Detail
as of Tue 06-Dec-2005 15:17:35 PST

❗ **Multiple Service Quality Issues on Destination:** 2111999 **Destination Type:** IP Phone
Description: 1 events in the last 10 minutes

Events: (3)

#	!	Event ID	MOS	Cause	Timestamp ▽	Codec	Source Type	Source	Tools
1.	⚠	0000IEE	3.9	Jitter	06-Dec-2005 15:17:31	G711	IP Phone	2121003	---- Select ----
2.	❗	0000IDL	2.4	Jitter	06-Dec-2005 15:16:31	G711	IP Phone	2121003	---- Select ----
3.	⚠	0000IDG	3.9	Jitter	06-Dec-2005 15:15:31	G711	IP Phone	2121003	

Viewing Alerts on the OM Service Quality Alerts Dashboard

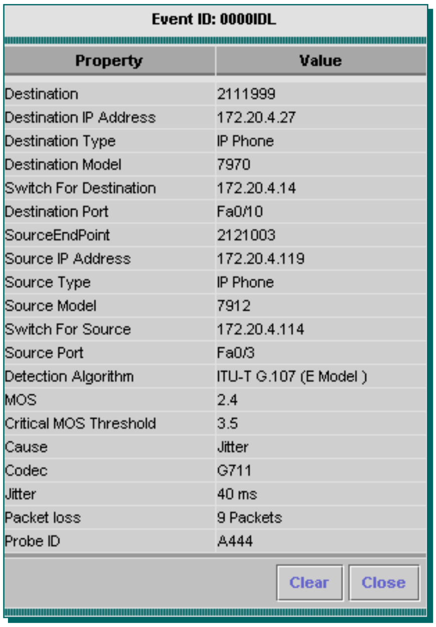
The Cisco 1040s are busy analyzing each RTP data stream and sending MOS values via Syslog messages to Service Monitor every 60 seconds. SM analyzes the incoming MOS values against the user-defined threshold and forwards any violations to Operations Manager (as configured in the SM **Setup** task).

Therefore, to view any MOS violation, Dean must use Operations Manger and follow these steps:

1. From the Operations Manager’s desktop, Dean selects the **Monitoring Dashboard** folder.
2. The content area of the OM desktop displays four icons for four different types of dashboards. Dean 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), Dean clicks 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. Dean now sees more information including the MOS value and primary cause for that MOS value. Dean also has the option to launch several Operations Manager’s tools to help in troubleshooting efforts. (For more information about the tools and their use, see the Operations Manager’s tutorial.) Dean can also quickly see the MOS values below 3.5 because they are displayed as critical events as defined in the *Event Settings* task.
5. Dean can now click on an individual Event ID to see its details (next page).

Monitoring Active Calls

Viewing Alerts – Service Quality Event Details



Event ID: 0000IDL

Property	Value
Destination	2111999
Destination IP Address	172.20.4.27
Destination Type	IP Phone
Destination Model	7970
Switch For Destination	172.20.4.14
Destination Port	Fa0/10
SourceEndPoint	2121003
Source IP Address	172.20.4.119
Source Type	IP Phone
Source Model	7912
Switch For Source	172.20.4.114
Source Port	Fa0/3
Detection Algorithm	ITU-T G.107 (E Model)
MOS	2.4
Critical MOS Threshold	3.5
Cause	Jitter
Codec	G711
Jitter	40 ms
Packet loss	9 Packets
Probe ID	A444

Service Quality Event Details

- **Call information**
  - **Devices**
  - **Phone Numbers**
  - **Ports**
  - **addresses**
- **MOS Values**
  - **Reported**
  - **Threshold**
- **Main Cause for low MOS**
  - **Can be either *Latency* or *Jitter***
- **Codec used**
- **Actual Jitter and Delay for the reported 60 second period**
- **Probe ID of the reporting Cisco 1040**

Viewing Alerts – Event Details

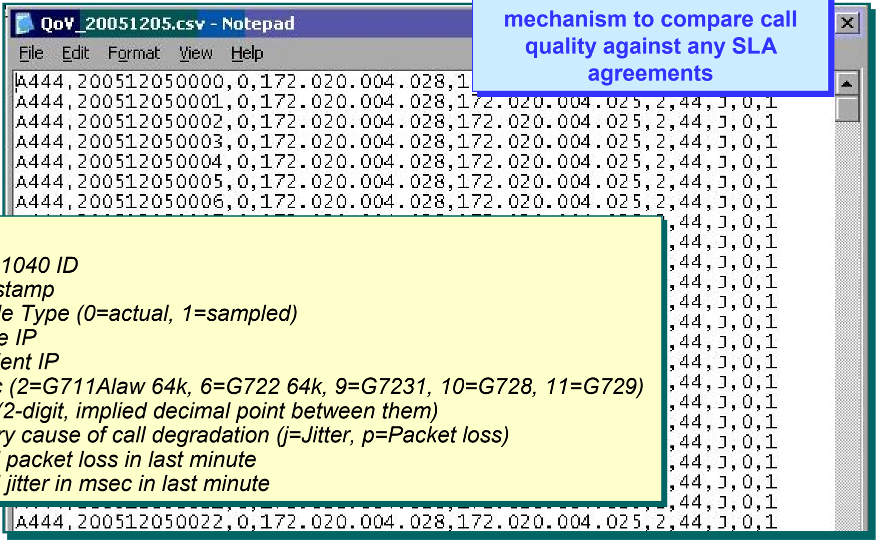
The *Event Details* will open in a new window. The *Event Details* includes information about the endpoints (phone numbers, IP address, switch and port connectivity), as well as information about the nature of the violation (reported MOS, user-defined MOS threshold, primary cause for low MOS, Codec used for call, actual jitter and packet loss values for the 60 seconds this violation represents).

For this particular violation, the reported MOS was 2.4 which is lower than the Service Monitor's user-defined threshold of 4.0, and the primary cause of the low MOS was jitter which was reported at 40 msec for the 60 second reporting period.

Monitoring Active Calls

Viewing Call Metrics Archived

- Archiving feature enabled in Setup task
- Metrics archived to directory specified during install
- New file for each day – *QoV_YYYYMMDD.csv*



```
A444,200512050000,0,172.020.004.028,1
A444,200512050001,0,172.020.004.028,172.020.004.025,2,44,J,0,1
A444,200512050002,0,172.020.004.028,172.020.004.025,2,44,J,0,1
A444,200512050003,0,172.020.004.028,172.020.004.025,2,44,J,0,1
A444,200512050004,0,172.020.004.028,172.020.004.025,2,44,J,0,1
A444,200512050005,0,172.020.004.028,172.020.004.025,2,44,J,0,1
A444,200512050006,0,172.020.004.028,172.020.004.025,2,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
,44,J,0,1
A444,200512050022,0,172.020.004.028,172.020.004.025,2,44,J,0,1
```

Archive can be used as a mechanism to compare call quality against any SLA agreements

Fields:

- *Cisco 1040 ID*
- *Time stamp*
- *Sample Type (0=actual, 1=sampled)*
- *Source IP*
- *Recipient IP*
- *Codec (2=G711Alaw 64k, 6=G722 64k, 9=G7231, 10=G728, 11=G729)*
- *MOS (2-digit, implied decimal point between them)*
- *Primary cause of call degradation (j=Jitter, p=Packet loss)*
- *Actual packet loss in last minute*
- *Actual jitter in msec in last minute*

Viewing Call Metrics Archived

During the Service Monitor **Setup** task, Dean enabled ***Call Metrics Archiving*** so that all incoming call metrics from the Cisco 1040 sensors will be archived to a flat file. Dean will then analyze this file using a custom spreadsheet application that he'll create to help verify conformance to the SLA.

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 are not sent to any recipient and are not viewable via the Service Monitor GUI, but 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.

Our peeking over Dean's shoulder is now complete. We have seen Dean setup and configure Service Monitor and view the reported results. Chapter 4 will now present some additional system administration features and tasks.

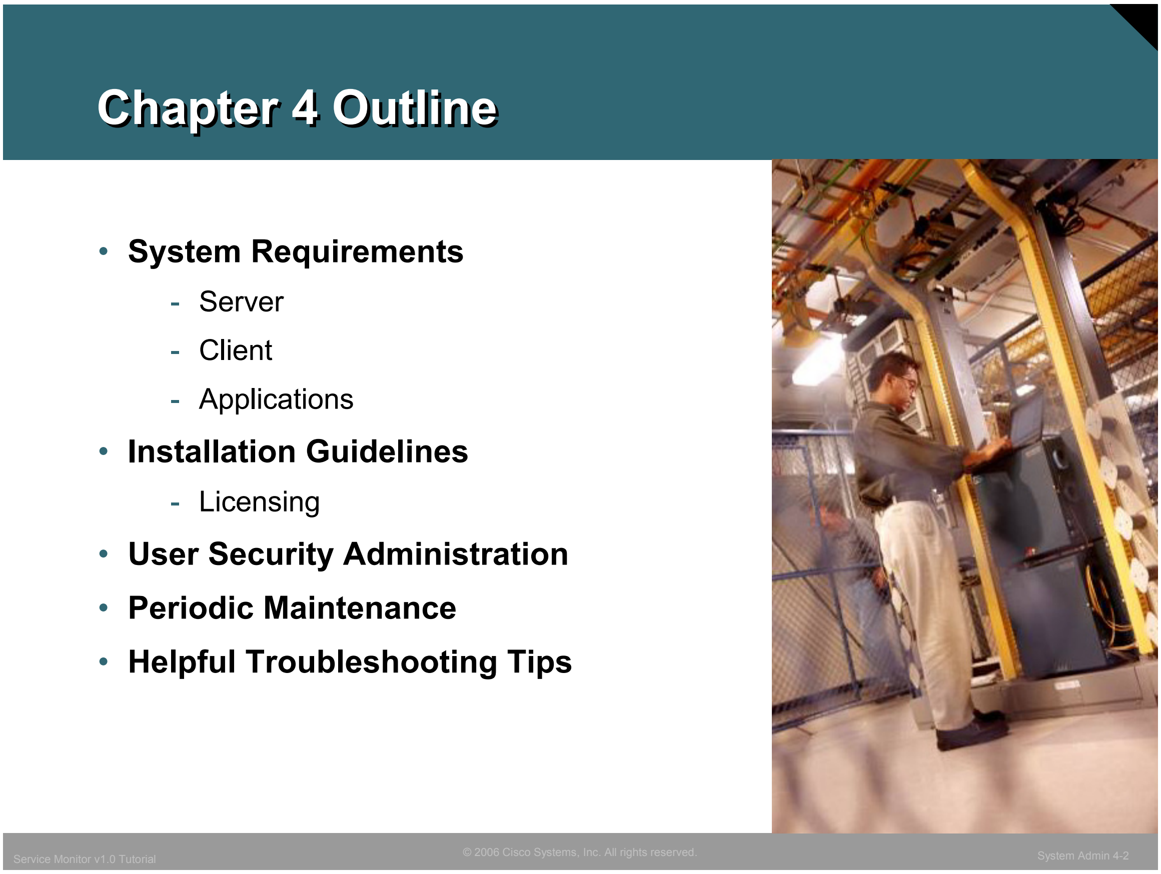
Thank You!

Continue on to Chapter 4 to learn about some additional system administration tasks not yet discussed.

Cisco Systems

Service Monitor System Administration

Chapter 4



Chapter 4 Outline

- **System Requirements**
  - Server
  - Client
  - Applications
- **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 the client used to access the server. Following the platform requirements are sections that briefly cover some installation guidelines, basic system administration tasks, periodic maintenance, and some helpful troubleshooting tips.

For detailed installation steps, also refer to the *IP Communications Service Monitor Install and Upgrade Guide v1.0*. A link to this document can be found in Chapter 5 of this tutorial.

System Requirements

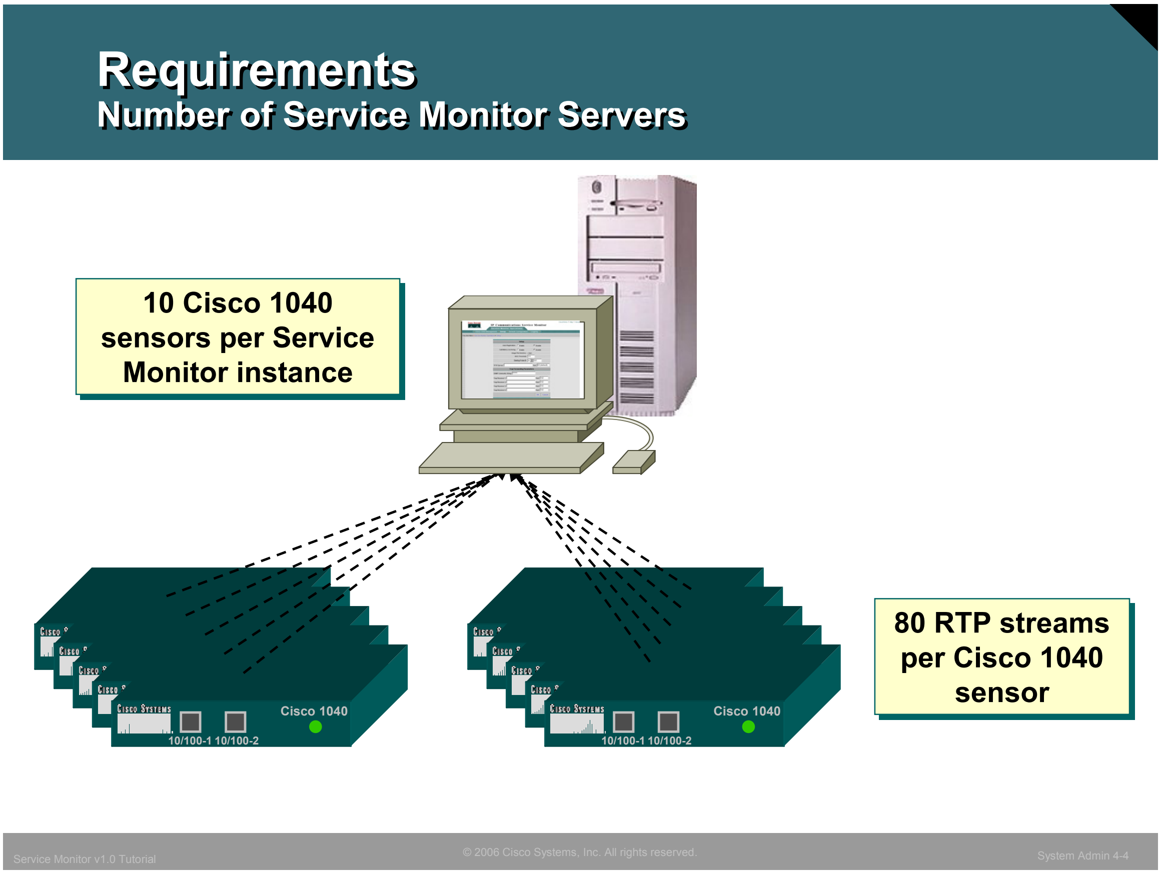
System Requirements

Installation Guidelines

User Security Administration

Periodic Maintenance

Helpful Troubleshooting Tips



Requirements
Number of Service Monitor Servers

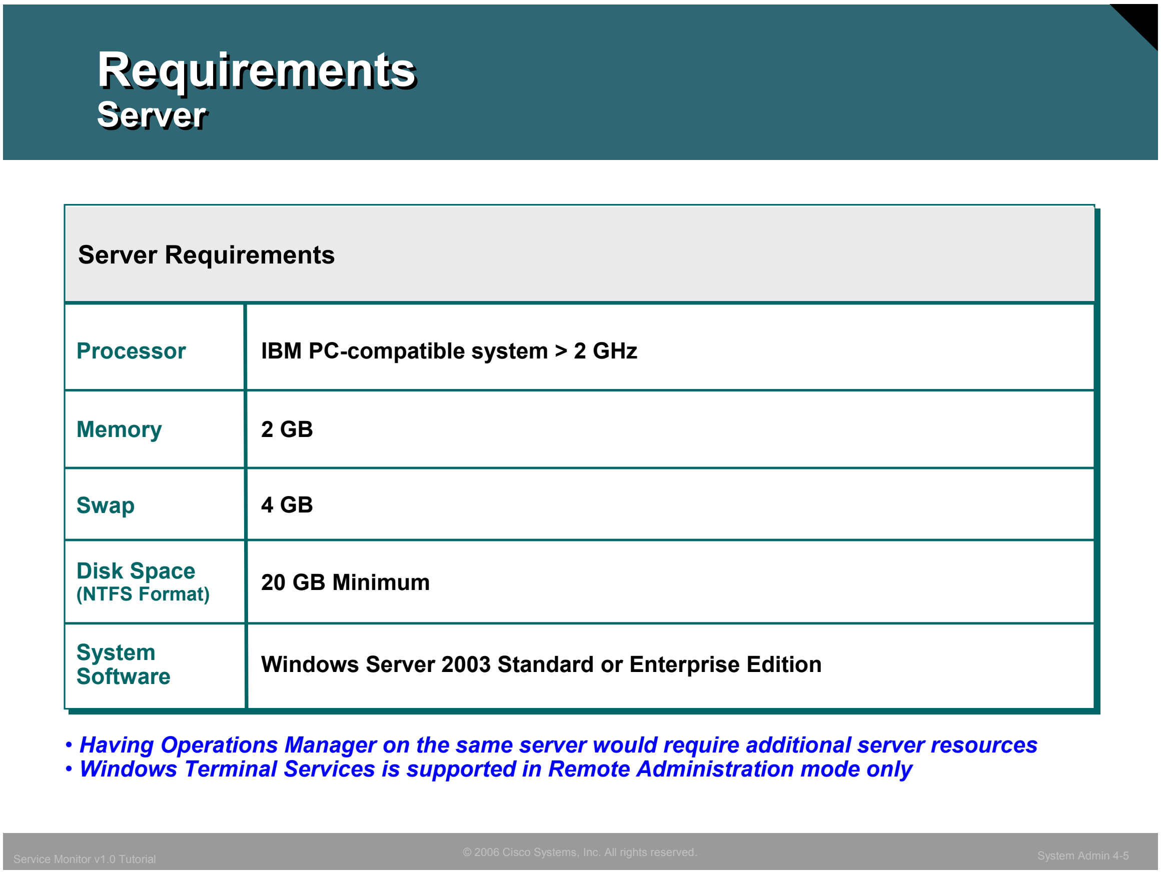
10 Cisco 1040 sensors per Service Monitor instance

80 RTP streams per Cisco 1040 sensor

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-4

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
Server

Server Requirements	
Processor	IBM PC-compatible system > 2 GHz
Memory	2 GB
Swap	4 GB
Disk Space (NTFS Format)	20 GB Minimum
System Software	Windows Server 2003 Standard or Enterprise Edition

- *Having Operations Manager on the same server would require additional server resources*
- *Windows Terminal Services is supported in Remote Administration mode only*

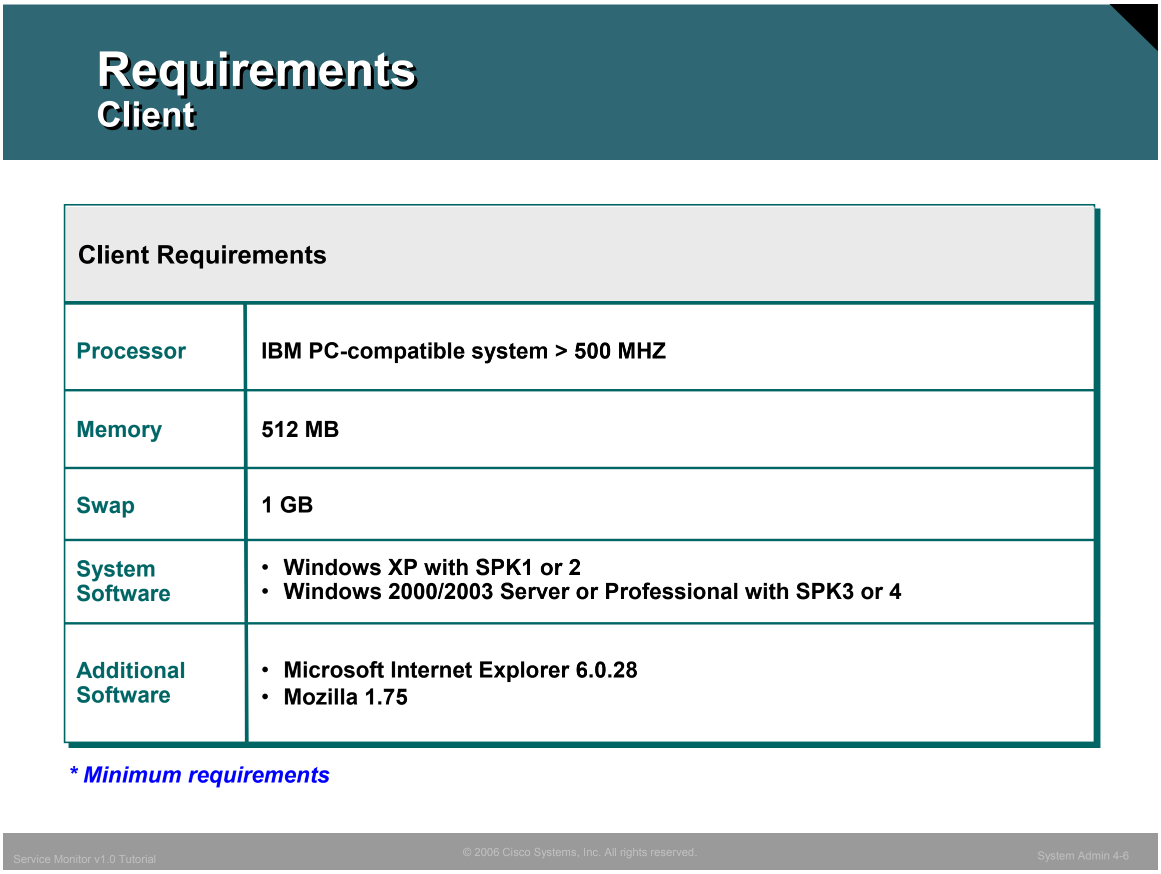
Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-5

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	
Processor	IBM PC-compatible system > 500 MHZ
Memory	512 MB
Swap	1 GB
System Software	• Windows XP with SPK1 or 2 • Windows 2000/2003 Server or Professional with SPK3 or 4
Additional Software	• Microsoft Internet Explorer 6.0.28 • Mozilla 1.75

**** Minimum requirements***

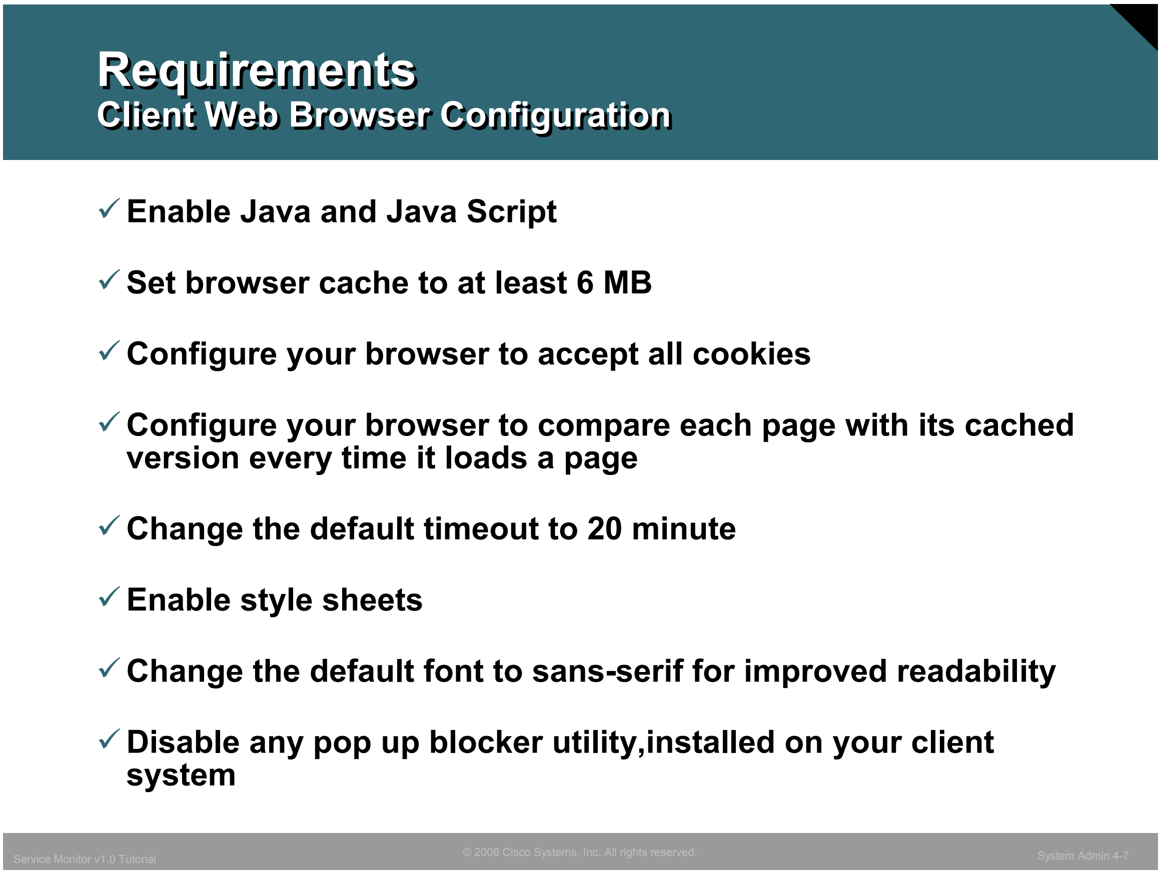
Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-6

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

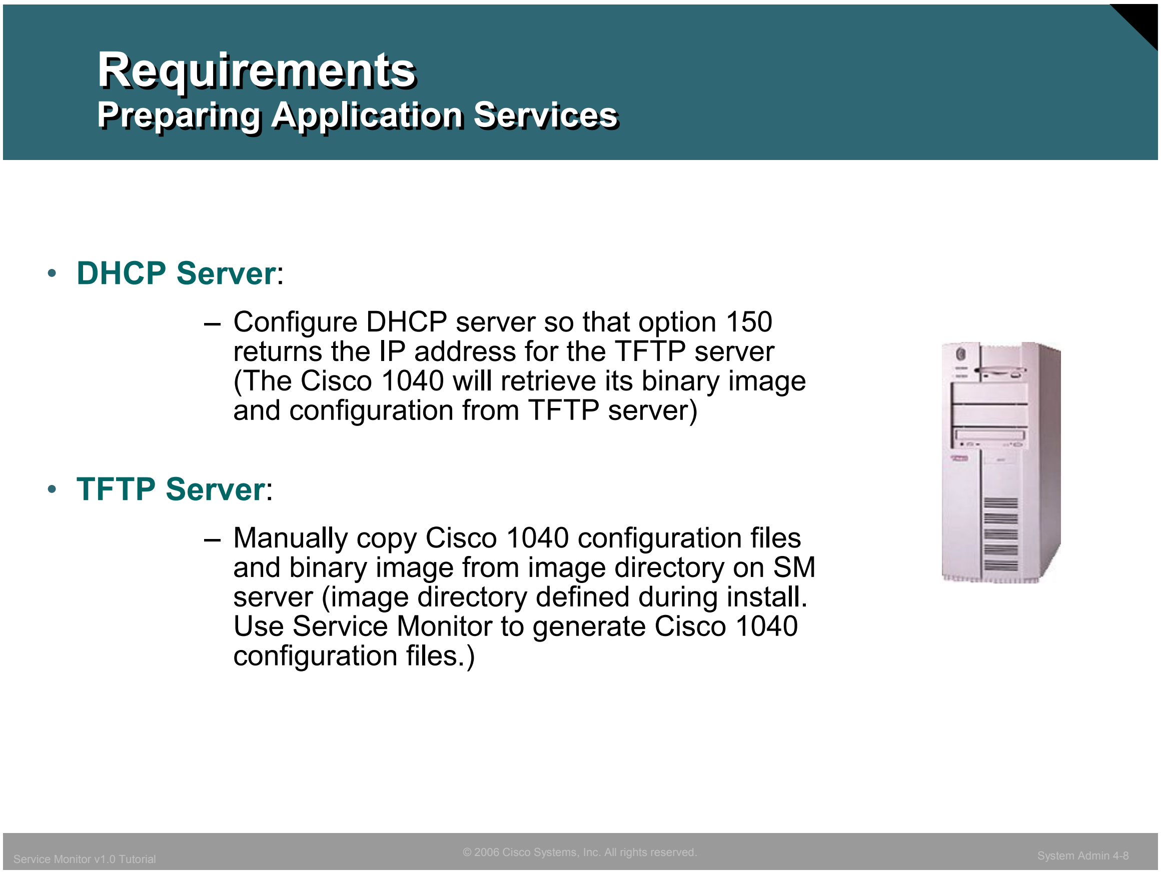
- ✓ Enable Java and Java Script
- ✓ Set browser cache to at least 6 MB
- ✓ Configure your browser to accept all cookies
- ✓ Configure your browser to compare each page with its cached version every time it loads a page
- ✓ Change the default timeout to 20 minute
- ✓ Enable style sheets
- ✓ Change the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

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-7

Web Browser Configuration

For best results, the client browser should be configured as displayed above. Customers often complain that they click a task and nothing happens. This is because many CiscoWorks applications use pop-ups. Therefore, ensure that pop-ups are allowed for the CiscoWorks server. 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.)

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 configuration files and binary image from image directory on SM server (image directory defined during install. Use Service Monitor to generate Cisco 1040 configuration files.)

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-8

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

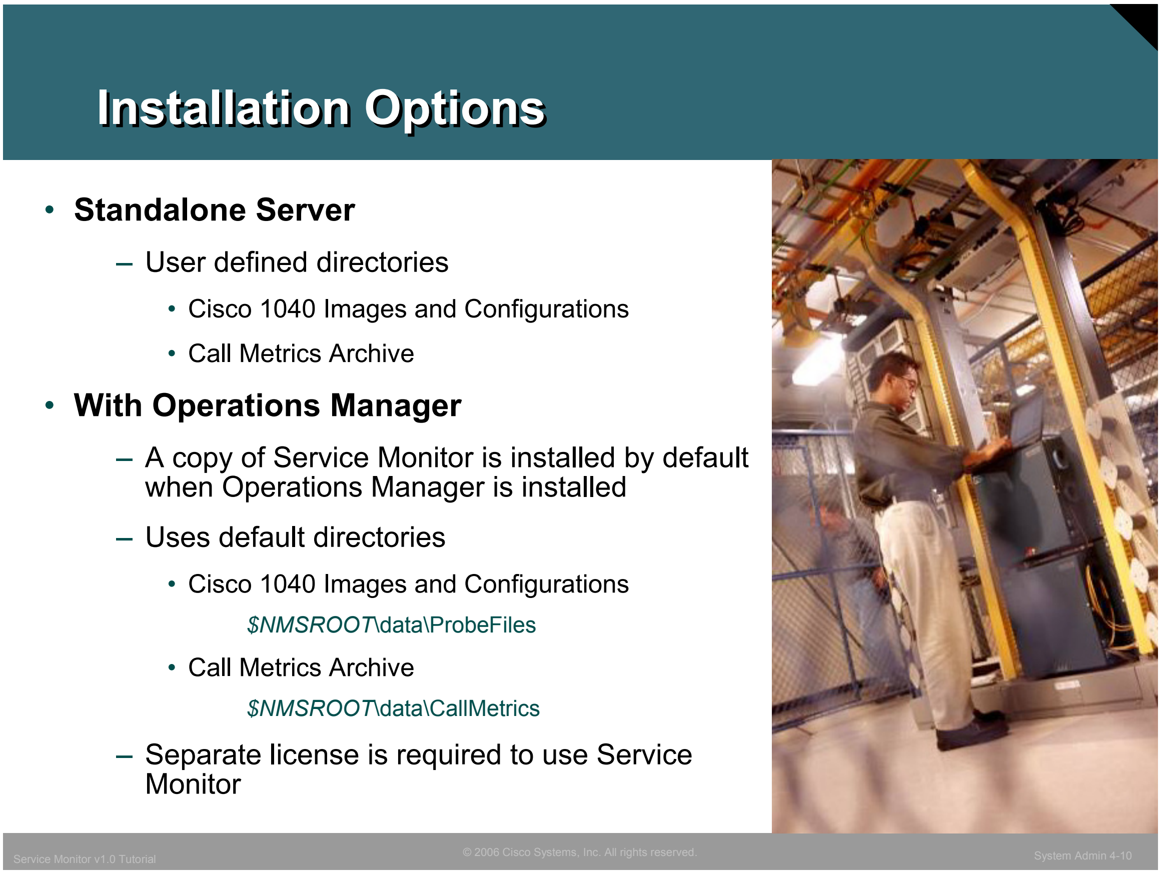
System Requirements

Installation Guidelines

User Security Administration

Periodic Maintenance

Helpful Troubleshooting Tips



Installation 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

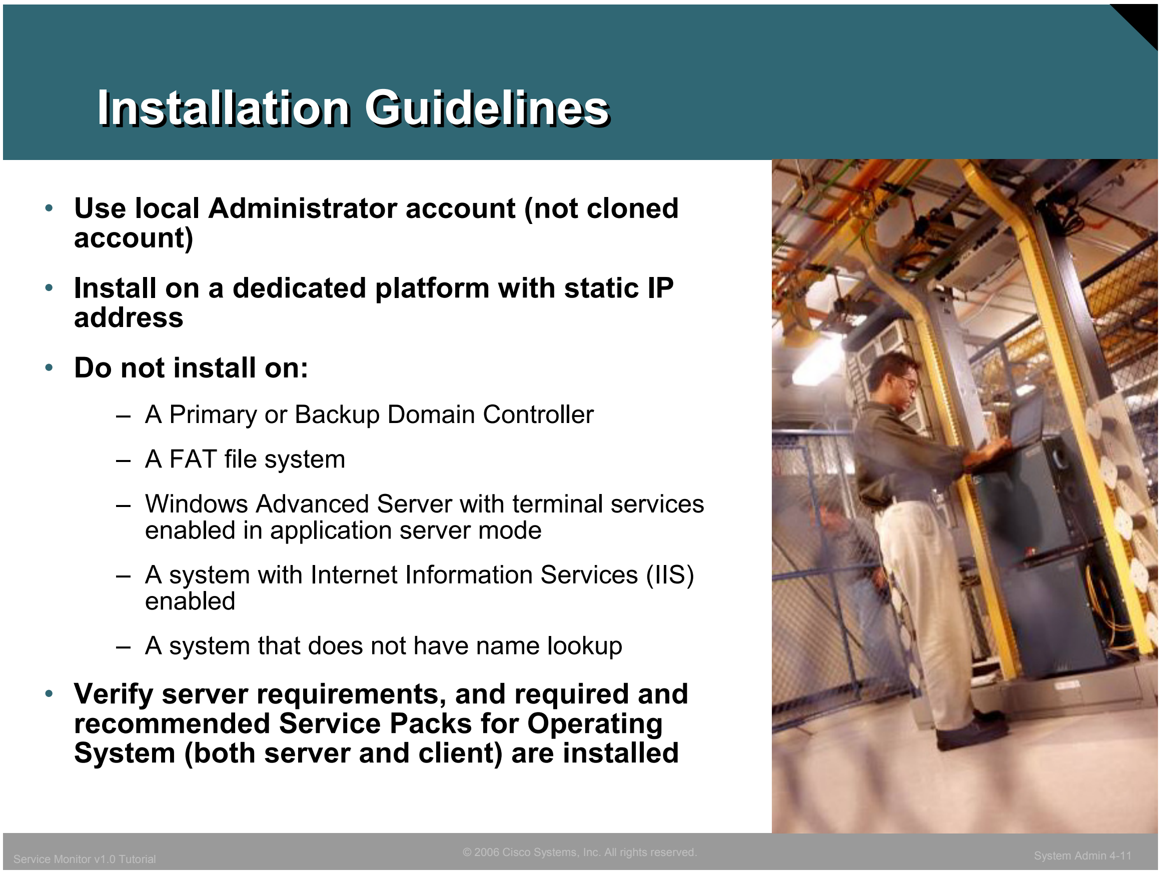
Installation Options

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
  - Windows 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 for Operating System (both server and client) are installed**

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.

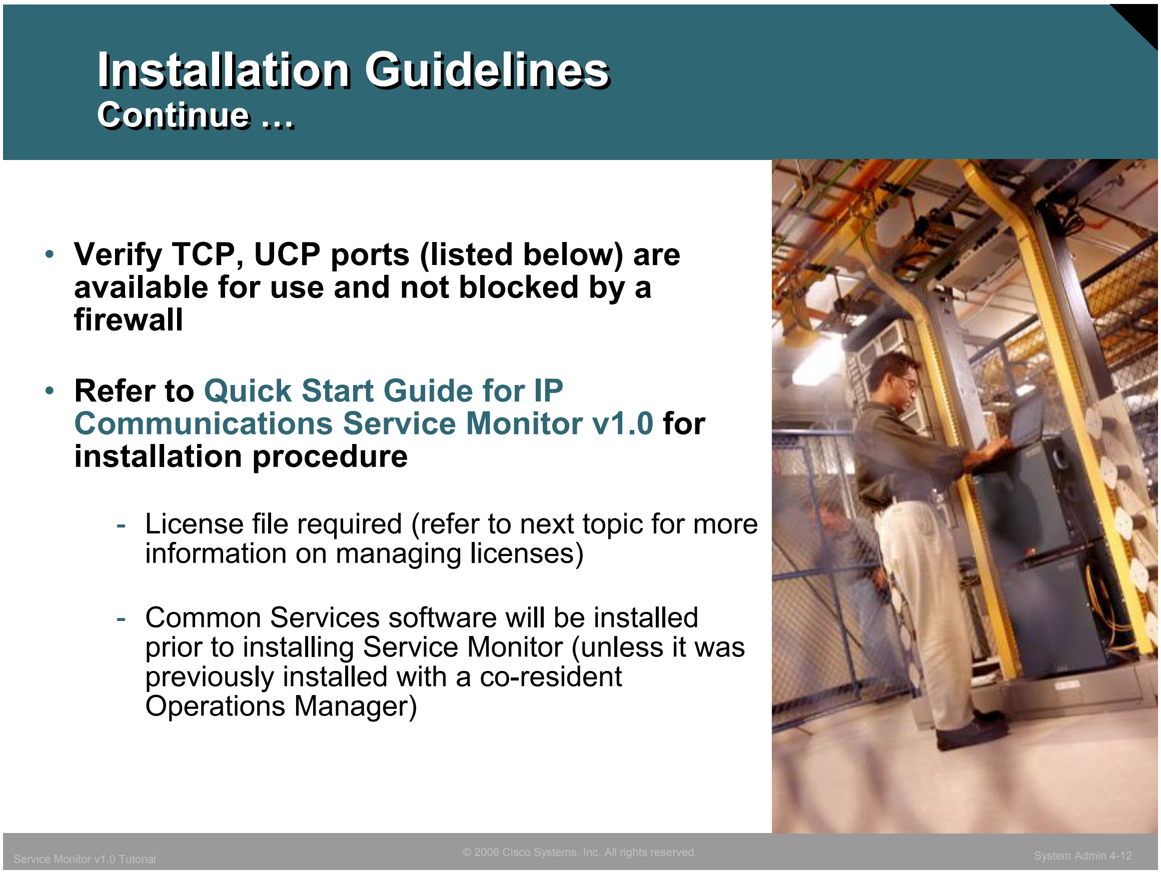
If required server patches are missing, the install script prompts whether to continue installation or not. Note that there are required and recommended service packs or patches for clients as well as the server. Remember that client patches are not necessary if the system is used only as a server.

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 v1.0 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)

Service Monitor v1.0 Tutorial

© 2006 Cisco Systems, Inc. All rights reserved.

System Admin 4-12

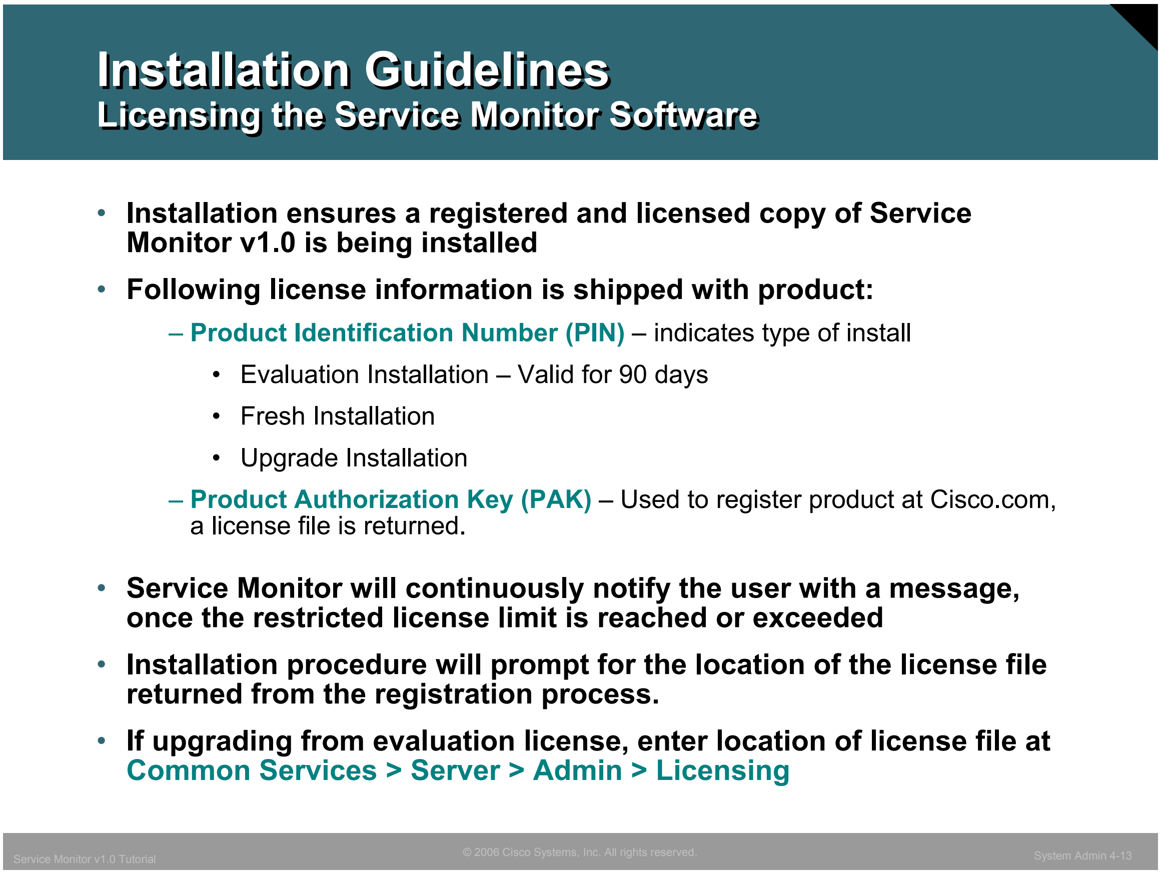
Installation Guidelines

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 v1.0 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**

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-13

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

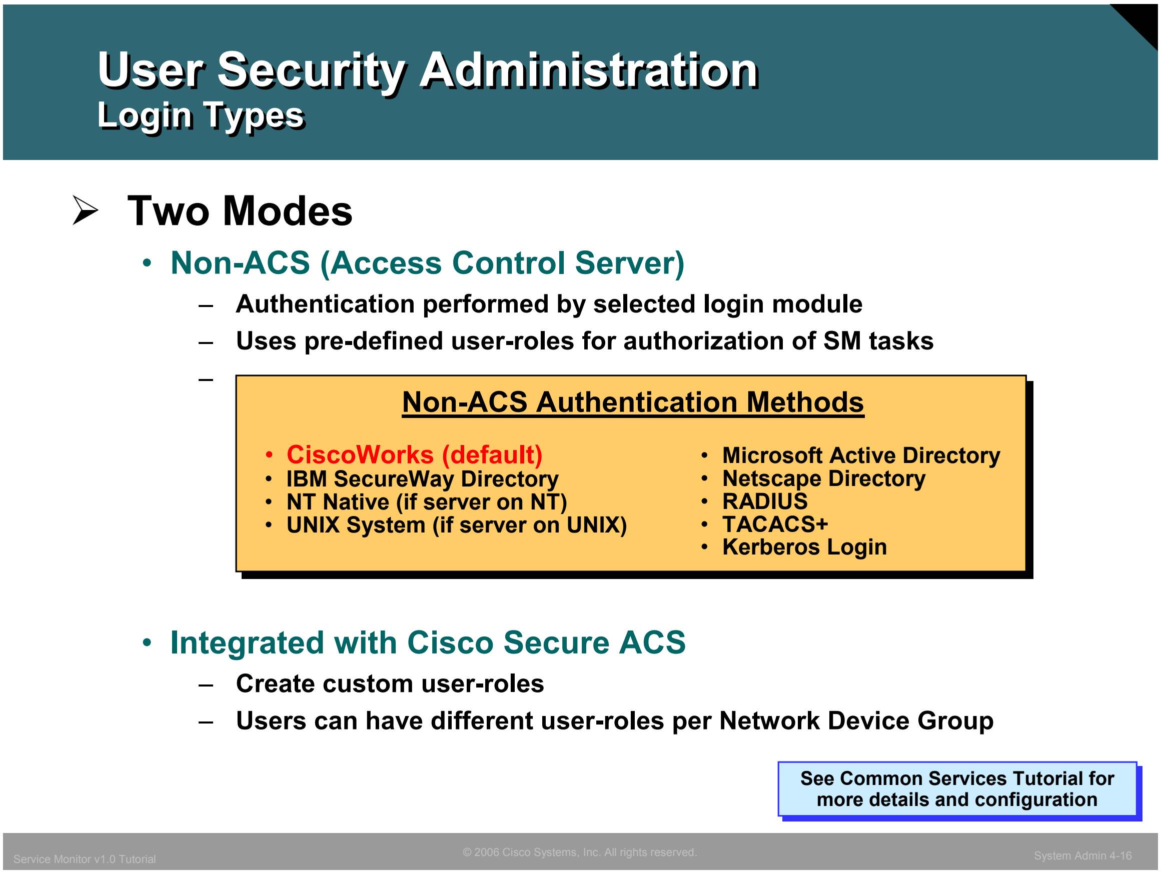
System Requirements

Installation Guidelines

User Security Administration

Periodic Maintenance

Helpful Troubleshooting Tips



User Security Administration
Login Types

- **Two Modes**
  - Non-ACS (Access Control Server)
    - Authentication performed by selected login module
    - Uses pre-defined user-roles for authorization of SM tasks
    - **Non-ACS Authentication Methods**
      - CiscoWorks (default)
      - IBM SecureWay Directory
      - NT Native (if server on NT)
      - UNIX System (if server on UNIX)
      - Microsoft Active Directory
      - Netscape Directory
      - RADIUS
      - TACACS+
      - Kerberos Login
  - Integrated with Cisco Secure ACS
    - Create custom user-roles
    - Users can have different user-roles per Network Device Group

See Common Services Tutorial for more details and configuration

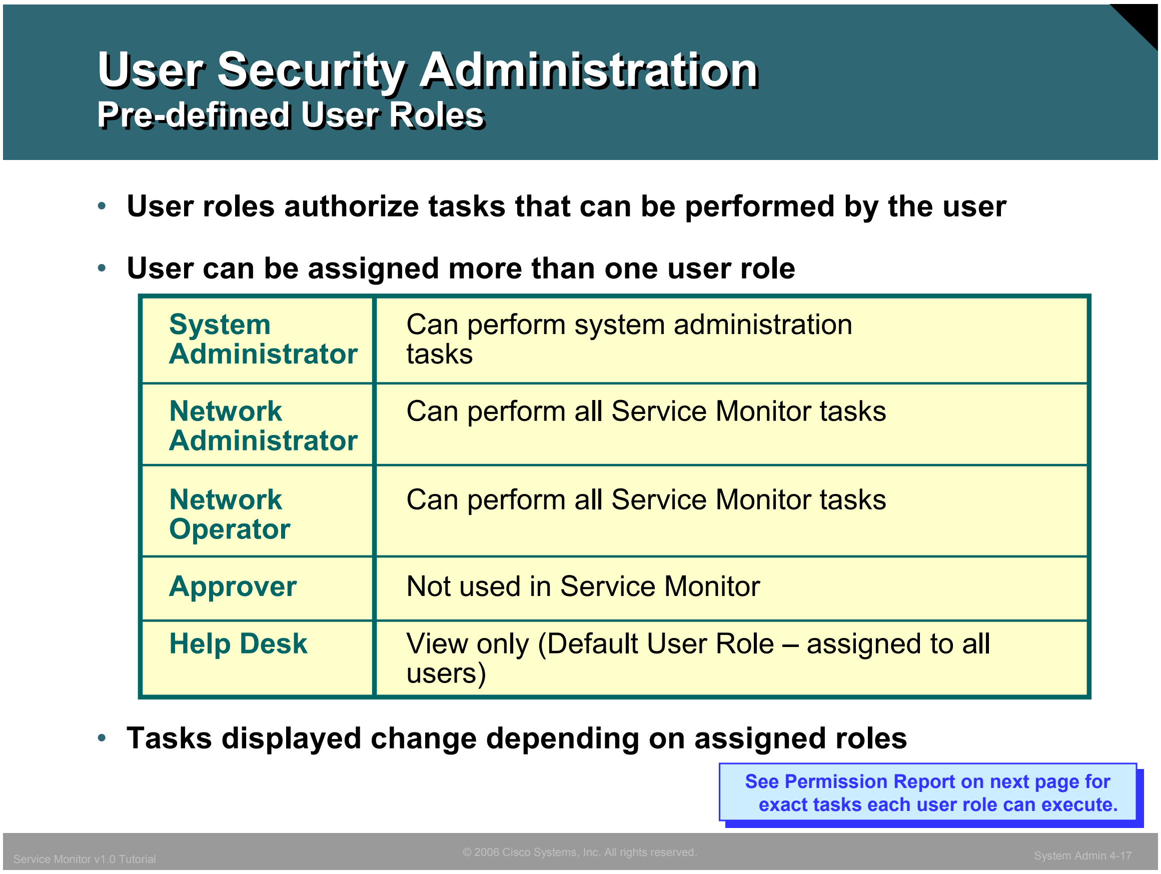
Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-16

Login Types

All CiscoWorks applications, including Service Monitor, rely on the services provided by Common Services. One of these services is security. Common Services supports two methods for Authentication (login) and Authorization (task execution) services: Non-ACS and ACS (Cisco Secure Access Control Server).

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 configure to use 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 execution 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 CiscoWorks 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 in the next topic) and every application and task on the CiscoWorks server.



User Security Administration
Pre-defined User Roles

- User roles authorize tasks that can be performed by the user
- User can be assigned more than one user role

System Administrator	Can perform 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 (Default User Role – assigned to all users)

- Tasks displayed change depending on assigned roles

See Permission Report on next page for exact tasks each user role can execute.

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-17

Pre-defined User Roles

CiscoWorks applications contain 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 good practice 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 general public information. To allow for proper access to all types of users, CiscoWorks employs the concept of User Roles (also known as user privileges or permissions). Use of the various functions or tasks within all CiscoWorks applications is based upon the “roles” assigned to user accounts. In fact, if a task can not be executed by a user role assigned to the logged in user, then that task will not even be displayed in the navigation tree of the application.

CiscoWorks uses five standard User Roles to define allowable task execution. The five user roles and their basic access ability are:

System Administrator – Can perform 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

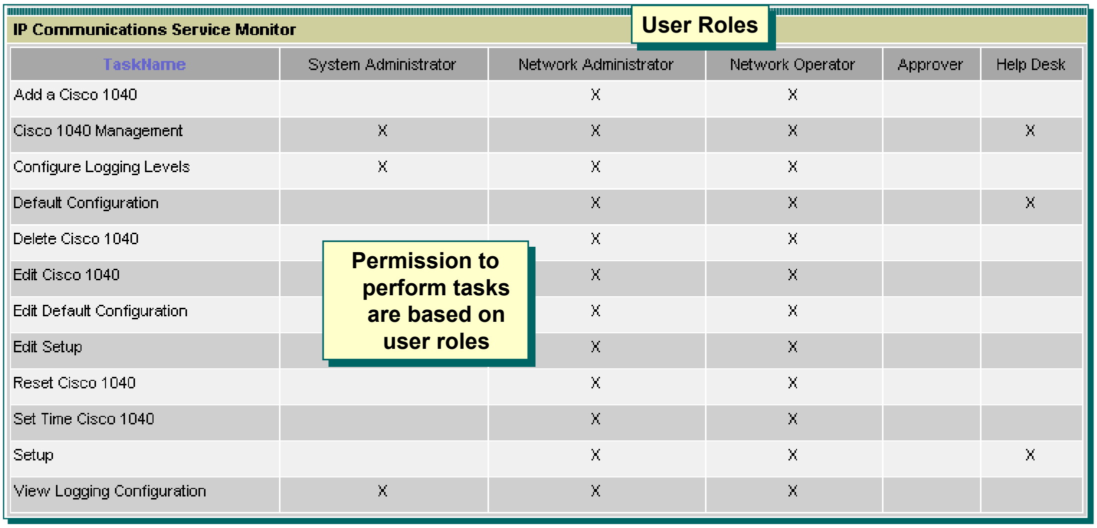
In Non-ACS mode (local CiscoWorks authorization), users can be assigned more than one user role, and all are assigned the basic user role – Help Desk. The task allowed per user role are static and cannot be modified. See next page for user roles assigned to Service Monitor tasks.

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

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

User Security Administration
Service Monitor Permissions

Common Services > Server > Reports > Permission Report



IP Communications Service Monitor

TaskName	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Add a Cisco 1040		X	X		
Cisco 1040 Management	X	X	X		X
Configure Logging Levels	X	X	X		
Default Configuration		X	X		X
Delete Cisco 1040		X	X		
Edit Cisco 1040		X	X		
Edit Default Configuration		X	X		
Edit Setup		X	X		
Reset Cisco 1040		X	X		
Set Time Cisco 1040		X	X		
Setup		X	X		X
View Logging Configuration	X	X	X		

User Roles

Permission to perform tasks are based on user roles

Permission Report lists all tasks for all CiscoWorks applications installed on server

Service Monitor Permissions

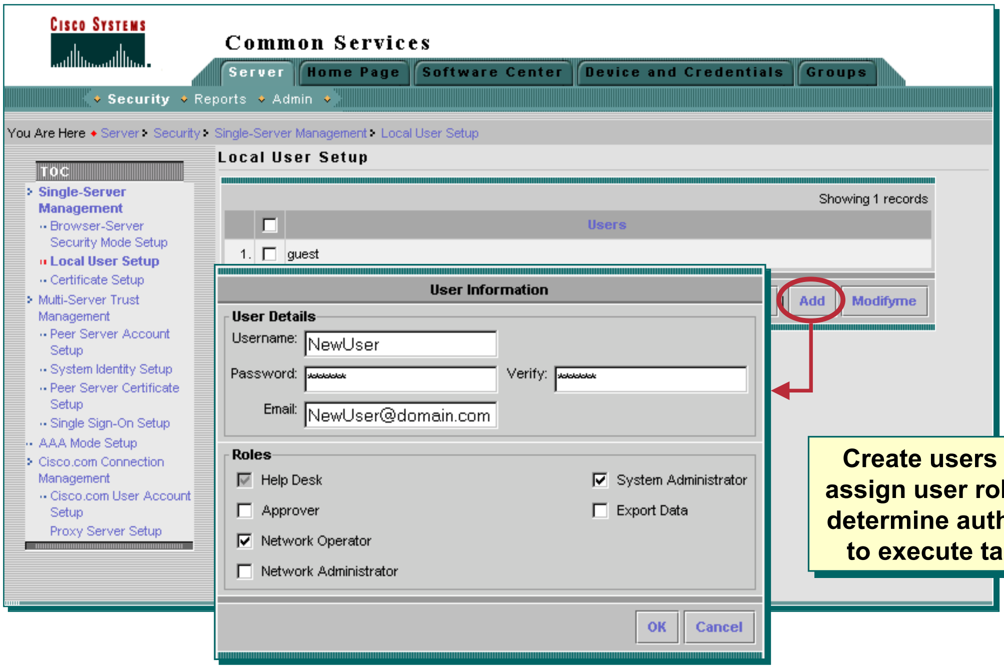
In the Non-ACS mode, the tasks that are executable by a user role are static and cannot be changed. Common Services includes a report that displays every task for every CiscoWorks application on the local server and which user roles have permission to execute it.

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. The Permission Report includes all installed CiscoWorks applications.

User Security Administration

Creating Users (Local Authentication)



Local User Setup

Showing 1 records

	□	Users
1.	□	guest

User Information

User Details

Username: NewUser

Password: ****** Verify: ******

Email: NewUser@domain.com

Roles

☑ Help Desk ☑ System Administrator

□ Approver □ Export Data

☑ Network Operator

□ Network Administrator

Create users and assign user roles to determine authority to execute tasks

Creating Users (Local Authentication)

Common Services allows users with the System Administration user role to create local 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 CiscoWorks informs 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 profile by selecting **ModifyMe** instead of Add. Only the password and e-mail address can be modified by a user without the System Administrator user role.

<Intentionally Blank>

Periodic Maintenance

System Requirements

Installation Guidelines

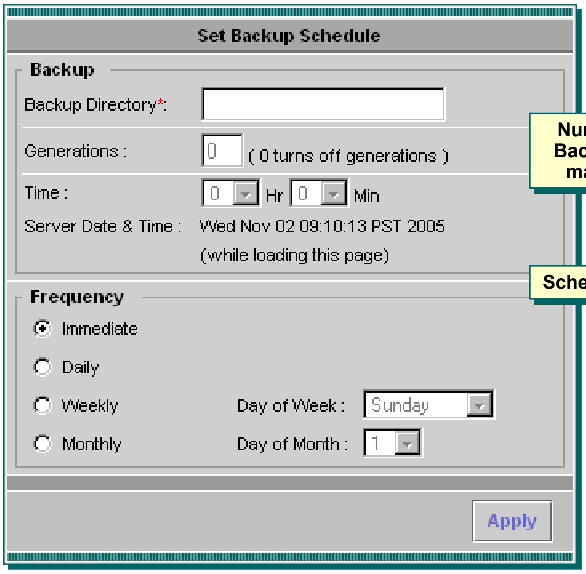
User Security Administration

Periodic Maintenance

Helpful Troubleshooting Tips

Periodic Maintenance
Database Management

Common Services > Server > Admin > Backup



Set Backup Schedule

Backup

Backup Directory*:

Generations : 0 (0 turns off generations)

Time : 0 Hr 0 Min

Server Date & Time : Wed Nov 02 09:10:13 PST 2005 (while loading this page)

Frequency

● Immediate

○ Daily

○ Weekly — Day of Week : Sunday

○ Monthly — Day of Month : 1

Apply

Number of Backups to maintain

Schedule Job

- **Backup the application databases 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 backed up periodically. 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:

Go to ***Common Services > Server > Admin > Backup***. The Set Backup Schedule dialog box appears.

1. 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.
2. Enter the number of backup Generations to be stored in the backup directory
3. Enter the Time for the backup to occur. Use a 24-hour format.
4. 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.
5. Periodically, examine the log file at the following location to verify backup status:

   NMSROOT/log/dbbackup.log

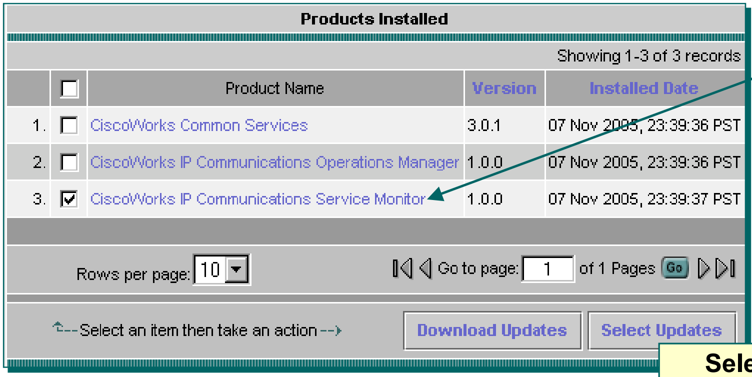
Note(s):

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

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

Periodic Maintenance
Service Monitor Server Software Updates

Common Services > Software Center > Software Update



Products Installed

Showing 1-3 of 3 records

	☐	Product Name	Version	Installed Date
1.	☐	CiscoWorks Common Services	3.0.1	07 Nov 2005, 23:39:36 PST
2.	☐	CiscoWorks IP Communications Operations Manager	1.0.0	07 Nov 2005, 23:39:36 PST
3.	☑	CiscoWorks IP Communications Service Monitor	1.0.0	07 Nov 2005, 23:39:37 PST

Rows per page: 10
Go to page: 1 of 1 Pages Go
Select an item then take an action -->
Download Updates
Select Updates

Click Product Name to see details about the installed versions

Select the product(s) to download from Cisco.com to the server file system

** Software Updates can be found at www.cisco.com/sgi-bin/tablebuild.pl/cw2000-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.

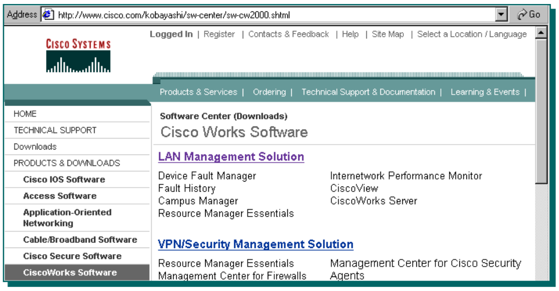
Note(s):

- 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 CiscoWorks GUI.

Periodic Maintenance

Cisco 1040 Image Updates

Step 1 - Download new image from Cisco.com



Address http://www.cisco.com/kobayashi/sw-center/sw-cw2000.shtml

Go
Cisco Systems
Logged In | Register | Contacts & Feedback | Help | Site Map | Select a Location / Language
Products & Services | Ordering | Technical Support & Documentation | Learning & Events |
HOME
TECHNICAL SUPPORT
Downloads
PRODUCTS & DOWNLOADS
Cisco IOS Software
Access Software
Application-Oriented Networking
Cable/Broadband Software
Cisco Secure Software
CiscoWorks Software

Software Center (Downloads)

Cisco Works Software

LAN Management Solution

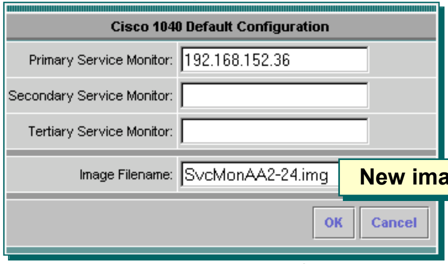
Device Fault Manager	Internetwork Performance Monitor
Fault History	CiscoView
Campus Manager	CiscoWorks Server
Resource Manager Essentials	

VPN/Security Management Solution

Resource Manager Essentials	Management Center for Cisco Security
Management Center for Firewalls	Agents

Service Monitor Operations > Default Configuration

Step 2 – Update the Cisco 1040 configuration



Cisco 1040 Default Configuration

Primary Service Monitor: 192.168.152.36

Secondary Service Monitor:

Tertiary Service Monitor:

Image Filename: SvcMonAA2-24.img

New image name

Depending on original 1040 configurations, may need to use Service Monitor Operations > Cisco 1040 Management to configure each individual 1040

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.

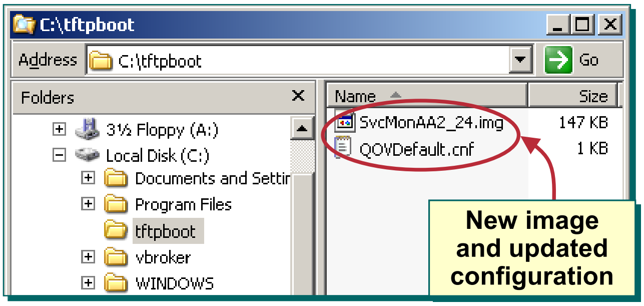
   If a specific configuration was generated for each Cisco 1040 ,then edit their configuration files individually using the ***IP Communications Service Monitor > Service Monitor Operations > Cisco 1040 Management*** task. Select the Cisco 1040 configuration to edit, select **Edit** and update the *Image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

Continued on next page…

Periodic Maintenance

Cisco 1040 Image Updates (Continued)

Step 3 - Copy image and updated configurations to the TFTP server

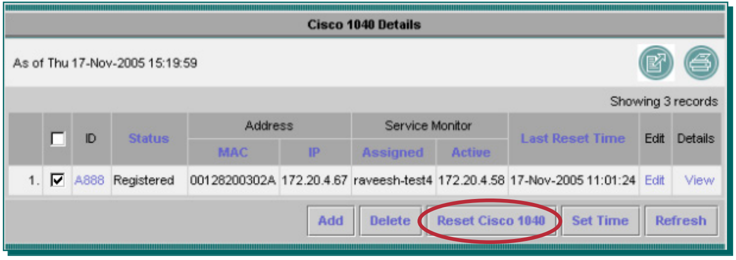


Name	Size
SvcMonAA2_24.img	147 KB
QOVDefault.cnf	1 KB

New image and updated configuration

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

Service Monitor Operations > Cisco 1040 Management


Cisco 1040 Details

As of Thu 17-Nov-2005 15:19:59

Showing 3 records

				Address		Service Monitor				
	□	ID	Status	MAC	IP	Assigned	Active	Last Reset Time	Edit	Details
1.	☑	A888	Registered	00128200302A	172.20.4.67	raveesh-test4	172.20.4.58	17-Nov-2005 11:01:24	Edit	View

Cisco 1040 Image Updates

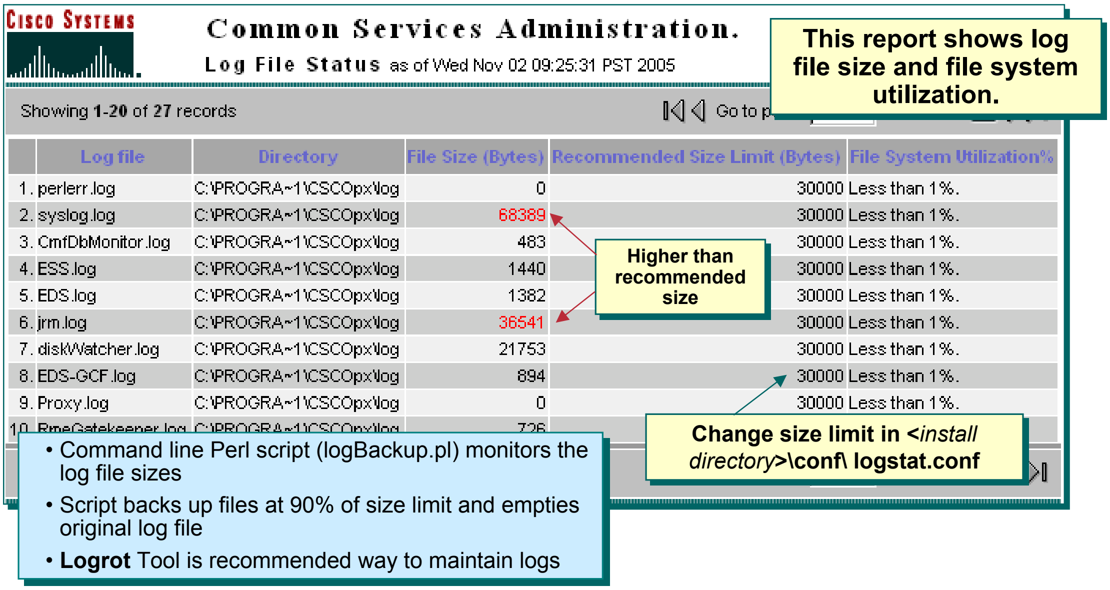
3. **Copy Image and Updated Configuration to TFTP Server** – The Cisco 1040 sensors retrieve their image and configuration files from the TFTP server. Therefore, the new image file and updated configuration(s) need to be copied to the TFTP server.

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 > Server > Reports > Log File Status



CISCO SYSTEMS

Common Services Administration.

Log File Status as of Wed Nov 02 09:25:31 PST 2005

Showing 1-20 of 27 records

	Log file	Directory	File Size (Bytes)	Recommended Size Limit (Bytes)	File System Utilization%
1.	perlerr.log	C:\PROGRA~1\CSCOpx\log	0	30000	Less than 1%.
2.	syslog.log	C:\PROGRA~1\CSCOpx\log	68389	30000	Less than 1%.
3.	CmfDbMonitor.log	C:\PROGRA~1\CSCOpx\log	483	30000	Less than 1%.
4.	ESS.log	C:\PROGRA~1\CSCOpx\log	1440	30000	Less than 1%.
5.	EDS.log	C:\PROGRA~1\CSCOpx\log	1382	30000	Less than 1%.
6.	jrm.log	C:\PROGRA~1\CSCOpx\log	36541	30000	Less than 1%.
7.	diskWatcher.log	C:\PROGRA~1\CSCOpx\log	21753	30000	Less than 1%.
8.	EDS-GCF.log	C:\PROGRA~1\CSCOpx\log	894	30000	Less than 1%.
9.	Proxy.log	C:\PROGRA~1\CSCOpx\log	0	30000	Less than 1%.
10.	RmeGatekeeper.log	C:\PROGRA~1\CSCOpx\log	726		

This report shows log file size and file system utilization.

Higher than recommended size

Change size limit in <*install directory*>\conf\ logstat.conf

- Command line Perl script (logBackup.pl) monitors the log file sizes
- Script backs up files at 90% of size limit and empties original log file
- **Logrot** Tool is recommended way to maintain logs

Log Files

CiscoWorks 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 ***Common Services > Server > Report > Log File Status*** task, you can view information on all the log files used by CiscoWorks.

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

To simplify the task of managing the log files there is a Perl script (logBackup.pl) that enables you to control their 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 CiscoWorks processes first before using the script (from command prompt ***net stop crmdmgtd***).

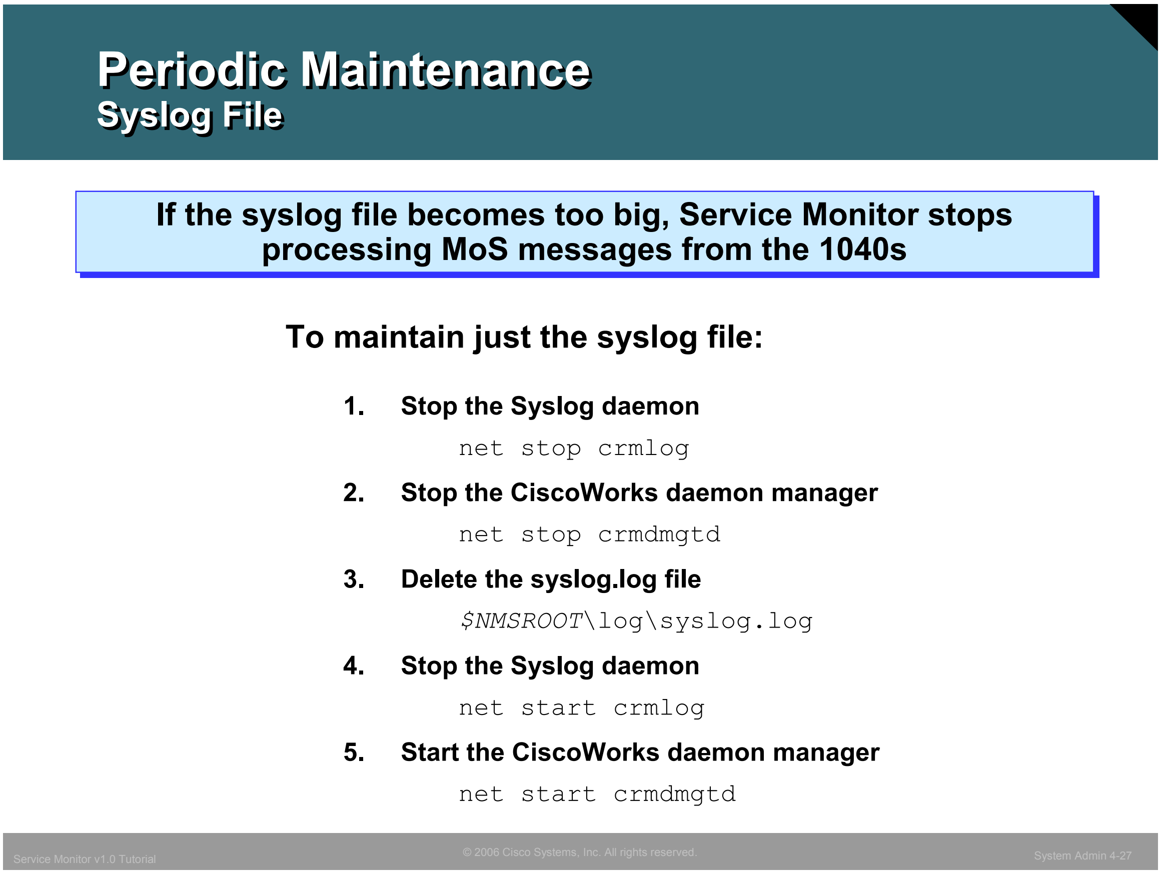
Files maintained by this script include the Daemon Manager and Daemon process log files. Most log files are located in directories in the PX_LOGDIR directory - %NMSROOT% /log.

Logrot Utility

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

- Rotate log when CiscoWorks 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. **Stop the Syslog daemon**

   `net start crmlog`

5. **Start the CiscoWorks daemon manager**

   `net start crmdmgtd`

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-27

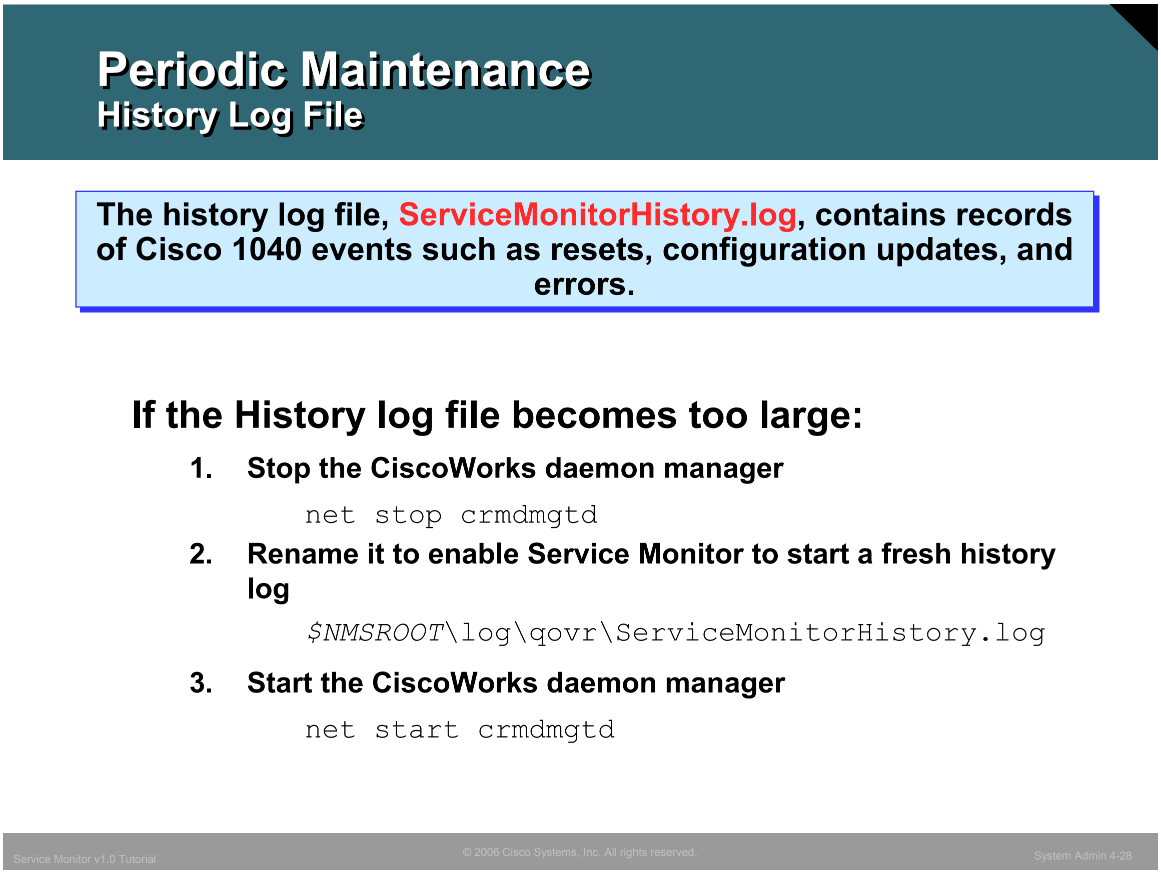
Syslog File

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
```

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-28

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

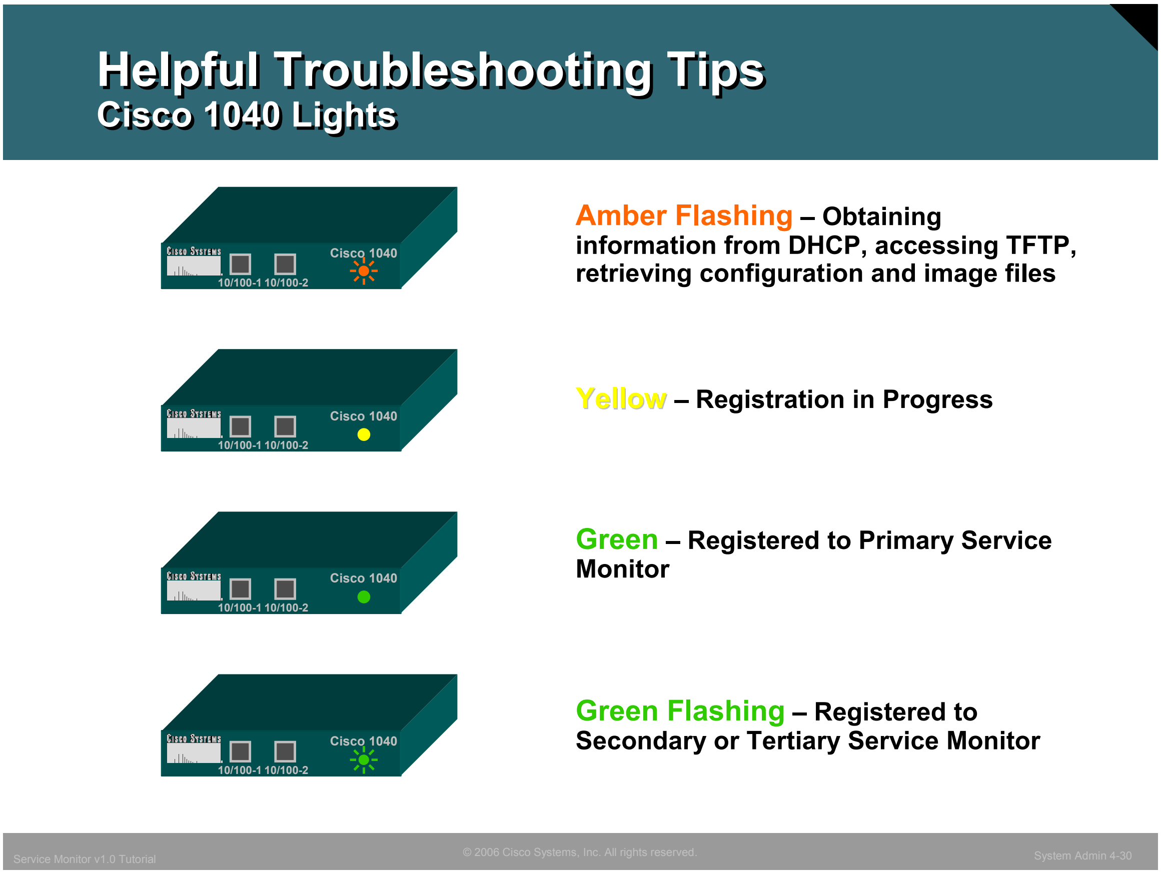
System Requirements

Installation Guidelines

User Security Administration

Periodic Maintenance

Helpful Troubleshooting Tips



Helpful Troubleshooting Tips

Cisco 1040 Lights

Cisco Systems
Cisco 1040
10/100-1 10/100-2

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 or Tertiary Service Monitor

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-30

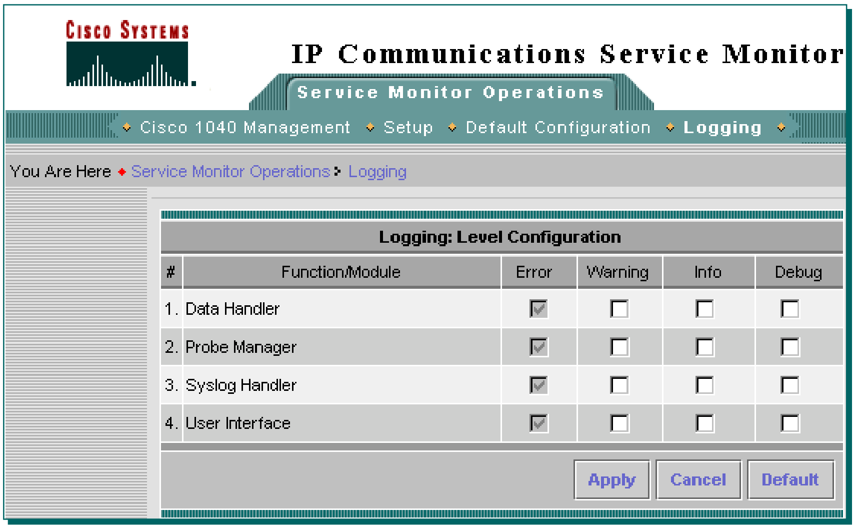
Cisco 1040 Lights

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
Service Monitor Log Files



Logging: Level Configuration

#	Function/Module	Error	Warning	Info	Debug
1.	Data Handler	☑	□	□	□
2.	Probe Manager	☑	□	□	□
3.	Syslog Handler	☑	□	□	□
4.	User Interface	☑	□	□	□

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

SM Log File Location:
$NMSROOT/log/qovr

Using Logging to Enable and Disable Debugging

Service Monitor writes application log files for all major functional modules. By default, Service Monitor writes only error and fatal messages to these log files. Logging cannot be disabled, but can be configured to collect more data when needed by increasing the logging level. The Service Monitor application log files can be found in the *$NMSROOT\log\qovr* directory.

To change logging levels use the following steps:

1. From the Service Monitor's desktop, select ***IP Service Monitor Operations > Logging***. The Logging Configuration page is displayed.

   Note: You cannot disable logging. Service Monitor will always write error and fatal messages to application log files.

2. For each Operations Manager functional module, select the level of information you wish to log.

   Warning--Log error messages and warning messages

   Info--Log error, warning, and informational messages

   Debug--Log error, warning, informational, and debug message

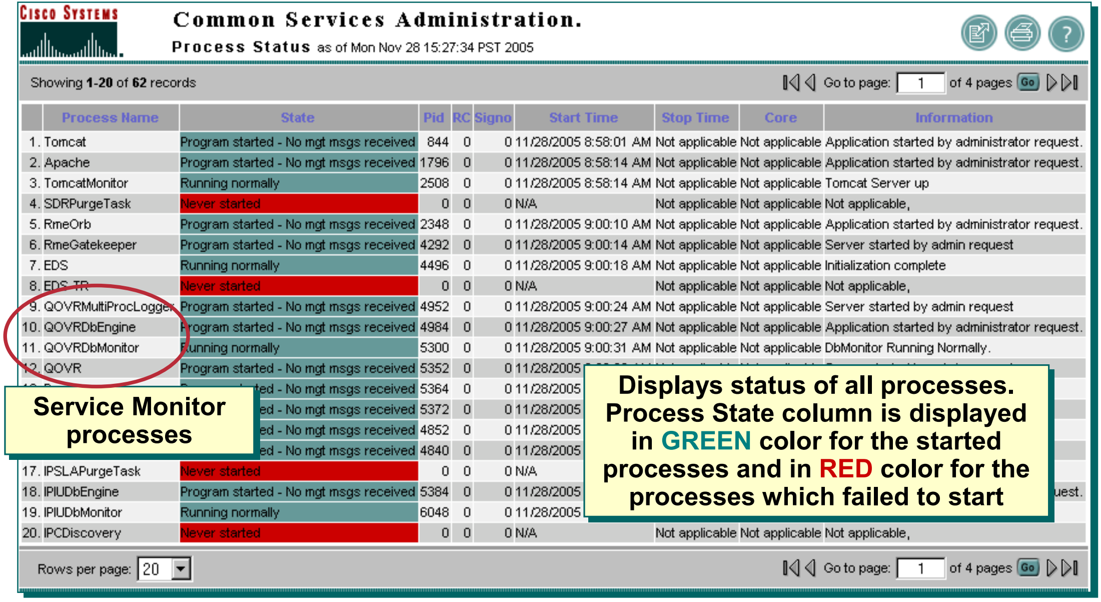
   Note: the Error check box is always selected; you cannot deselect it. Click the **Default** button to reset all functional modules to the error level only.

3. Click **Apply** for the changes to take effect.

Helpful Troubleshooting Tips

Process Status

Common Services > Server > Reports > Process Status



CISCO SYSTEMS

Common Services Administration.

Process Status as of Mon Nov 28 15:27:34 PST 2005

Showing **1-20** of **62** records

Go to page: 1 of 4 pages Go

	Process Name	State	Pid	RC	Signo	Start Time	Stop Time	Core	Information
1.	Tomcat	Program started - No mgt msgs received	844	0	0	11/28/2005 8:58:01 AM	Not applicable	Not applicable	Application started by administrator request.
2.	Apache	Program started - No mgt msgs received	1796	0	0	11/28/2005 8:58:14 AM	Not applicable	Not applicable	Application started by administrator request.
3.	TomcatMonitor	Running normally	2508	0	0	11/28/2005 8:58:14 AM	Not applicable	Not applicable	Tomcat Server up
4.	SDRPurgeTask	Never started	0	0	0	N/A	Not applicable	Not applicable	Not applicable,
5.	RmeOrb	Program started - No mgt msgs received	2348	0	0	11/28/2005 9:00:10 AM	Not applicable	Not applicable	Application started by administrator request.
6.	RmeGatekeeper	Program started - No mgt msgs received	4292	0	0	11/28/2005 9:00:14 AM	Not applicable	Not applicable	Server started by admin request
7.	EDS	Running normally	4496	0	0	11/28/2005 9:00:18 AM	Not applicable	Not applicable	Initialization complete
8.	EDS-TR	Never started	0	0	0	N/A	Not applicable	Not applicable	Not applicable,
9.	QOVRMultiProcLogger	Program started - No mgt msgs received	4952	0	0	11/28/2005 9:00:24 AM	Not applicable	Not applicable	Server started by admin request
10.	QOVRDbEngine	Program started - No mgt msgs received	4984	0	0	11/28/2005 9:00:27 AM	Not applicable	Not applicable	Application started by administrator request.
11.	QOVRDbMonitor	Running normally	5300	0	0	11/28/2005 9:00:31 AM	Not applicable	Not applicable	DbMonitor Running Normally.
12.	QOVR	Program started - No mgt msgs received	5352	0	0	11/28/2005			
		ted - No mgt msgs received	5364	0	0	11/28/2005			
		ed - No mgt msgs received	5372	0	0	11/28/2005			
		ed - No mgt msgs received	4852	0	0	11/28/2005			
		ed - No mgt msgs received	4840	0	0	11/28/2005			
17.	IPSLAPurgeTask	Never started	0	0	0	N/A			
18.	IPIUDbEngine	Program started - No mgt msgs received	5384	0	0	11/28/2005			uest.
19.	IPIUDbMonitor	Running normally	6048	0	0	11/28/2005			
20.	IPCDiscovery	Never started	0	0	0	N/A	Not applicable	Not applicable	Not applicable,

Rows per page: 20 ▼

Go to page: 1 of 4 pages Go

Service Monitor processes

Displays 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

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

Process Status

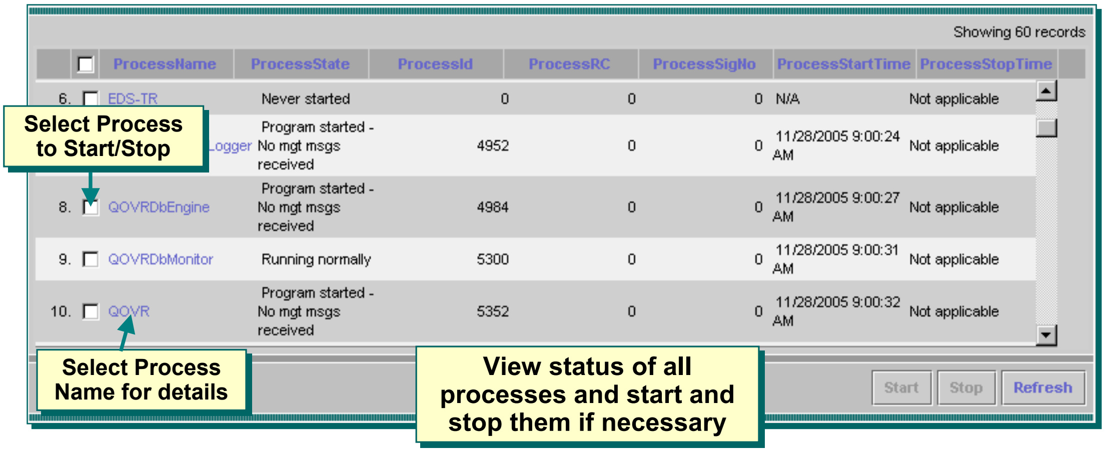
Process Status is a Common Services task used to manage all CiscoWorks processes. This report displays the status of all processes. Process State column is displayed in **GREEN** color for the started processes and in **RED** color for the processes which failed to start.

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



Showing 60 records

	☐	ProcessName	ProcessState	ProcessId	ProcessRC	ProcessSigNo	ProcessStartTime	ProcessStopTime
6.	☐	EDS-TR	Never started	0	0	0	N/A	Not applicable
		Logger	Program started - No mgt msgs received	4952	0	0	11/28/2005 9:00:24 AM	Not applicable
8.	☐	QOVRDbEngine	Program started - No mgt msgs received	4984	0	0	11/28/2005 9:00:27 AM	Not applicable
9.	☐	QOVRDbMonitor	Running normally	5300	0	0	11/28/2005 9:00:31 AM	Not applicable
10.	☐	QOVR	Program started - No mgt msgs received	5352	0	0	11/28/2005 9:00:32 AM	Not applicable

Select Process to Start/Stop

Select Process Name for details

View status of all processes and start and stop them if necessary

To "bounce" server – 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 processes. In the event something doesn't quite seem right with one of the applications, 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 processes, open a Command Prompt on the server and enter:

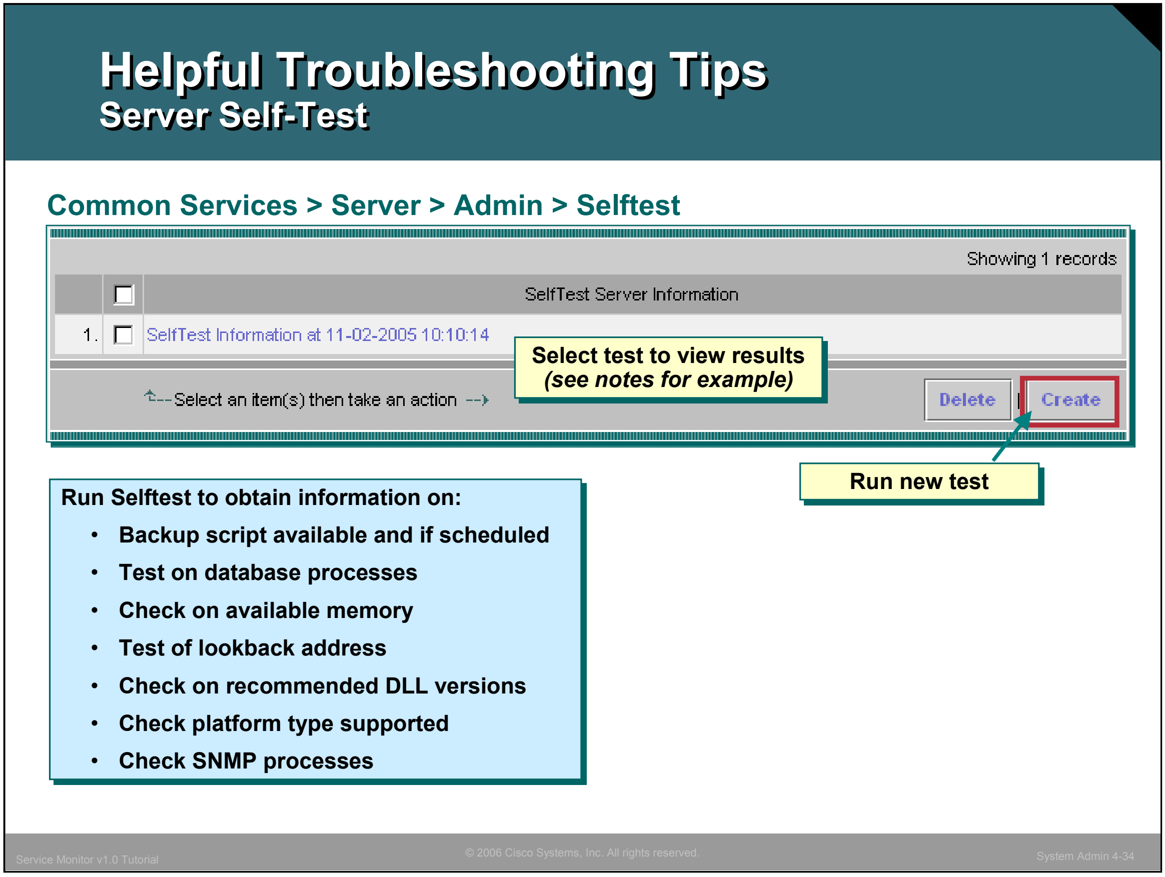
```
net stop crmdmgtd
```

To restart all the processes 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.)



Helpful Troubleshooting Tips

Server Self-Test

Common Services > Server > Admin > Selftest

Showing 1 records

	☐	SelfTest Server Information
1.	☐	SelfTest Information at 11-02-2005 10:10:14

Select test to view results
(see notes for example)

Run new test

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**

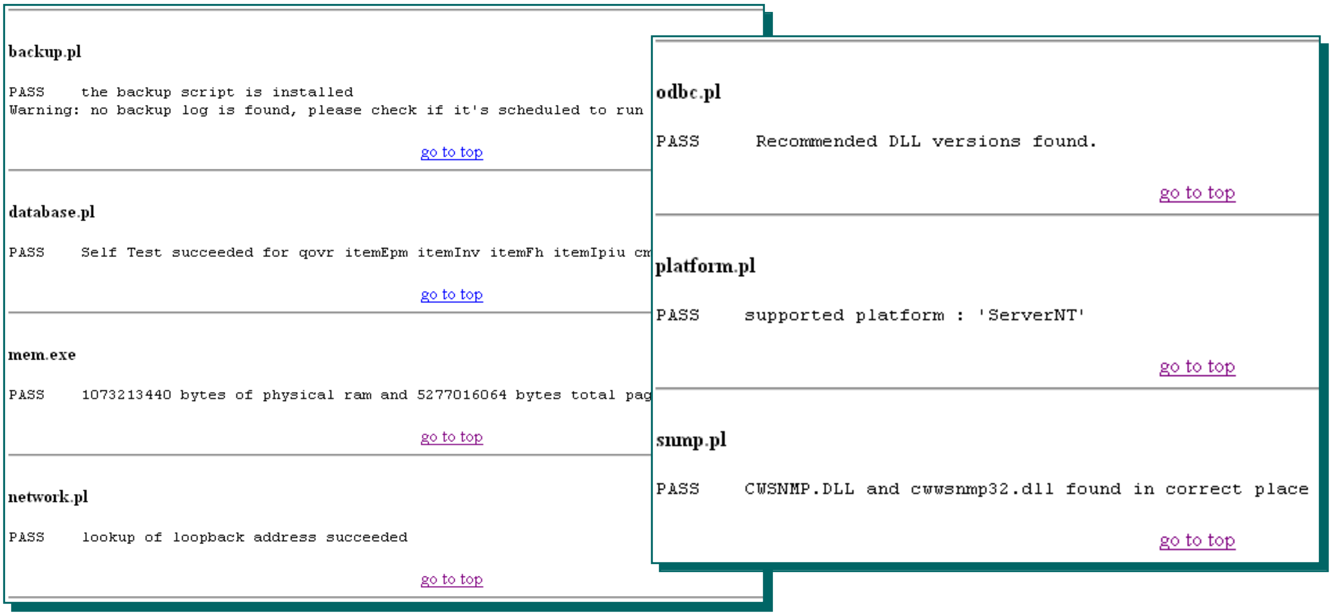
Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-34

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.



backup.pl

```
PASS    the backup script is installed
Warning: no backup log is found, please check if it's scheduled to run
```

go to top

database.pl

```
PASS    Self Test succeeded for qovr itemEpm itemInv itemFh itemIpiu cm
```

go to top

mem.exe

```
PASS    1073213440 bytes of physical ram and 5277016064 bytes total pag
```

go to top

network.pl

```
PASS    lookup of loopback address succeeded
```

go to top

odbc.pl

```
PASS     Recommended DLL versions found.
```

go to top

platform.pl

```
PASS    supported platform : 'ServerNT'
```

go to top

snmp.pl

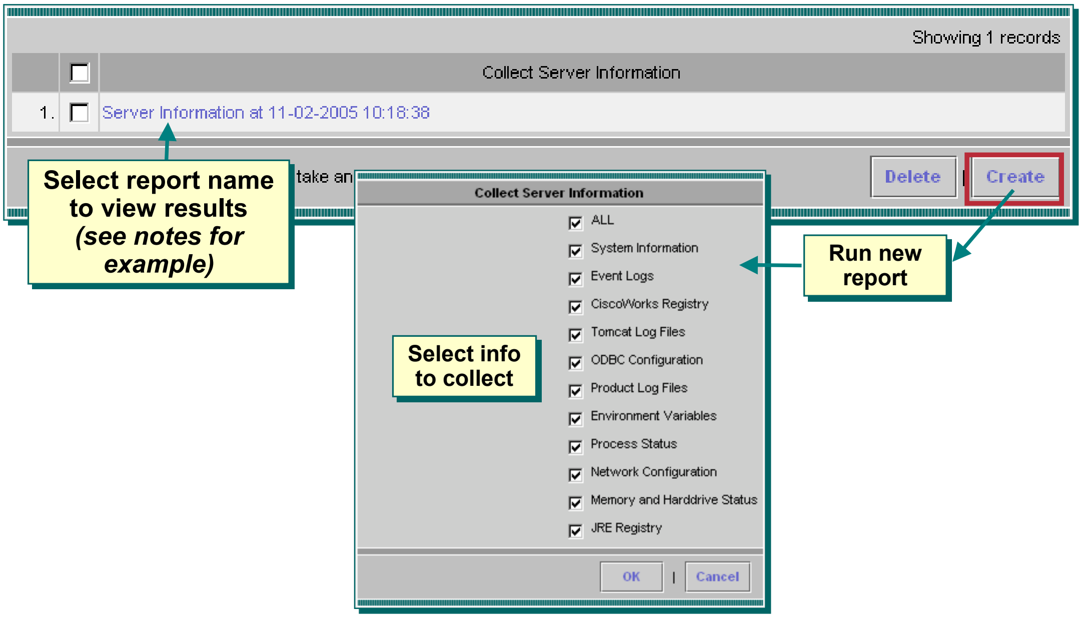
```
PASS    CWSNMP.DLL and cwwsnmp32.dll found in correct place
```

go to top

Helpful Troubleshooting Tips

Collect Server Information

Common Services > Server > Admin > Collect Server Information



Showing 1 records

	☐	Collect Server Information
1.	☐	Server Information at 11-02-2005 10:18:38

Collect Server Information

- ☑ ALL
- ☑ System Information
- ☑ Event Logs
- ☑ CiscoWorks Registry
- ☑ Tomcat Log Files
- ☑ ODBC Configuration
- ☑ Product Log Files
- ☑ Environment Variables
- ☑ Process Status
- ☑ Network Configuration
- ☑ Memory and Harddrive Status
- ☑ JRE Registry

Select report name to view results *(see notes for example)*

Select info to collect

Run new report

Service Monitor v1.0 Tutorial © 2006 Cisco Systems, Inc. All rights reserved. System Admin 4-35

Collect Server Information

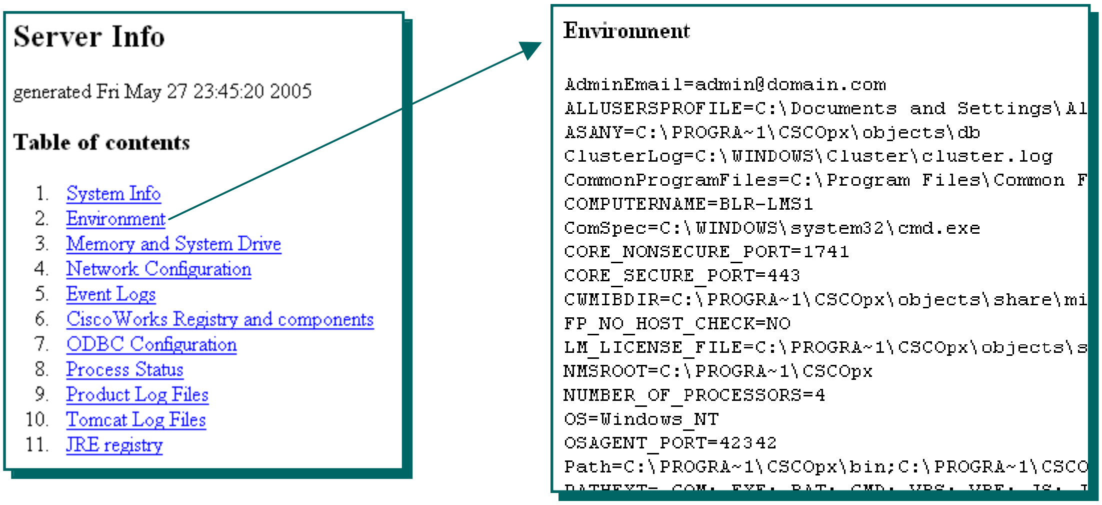
The System Administrator can gather troubleshooting information about the status of the server using this option. (*A command line script is also available at …/CSCOpx/bin/collect.info*). If you collect server information through the user interface, data is stored in …/CSCOpx/htdocs/collect.

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.



Server Info

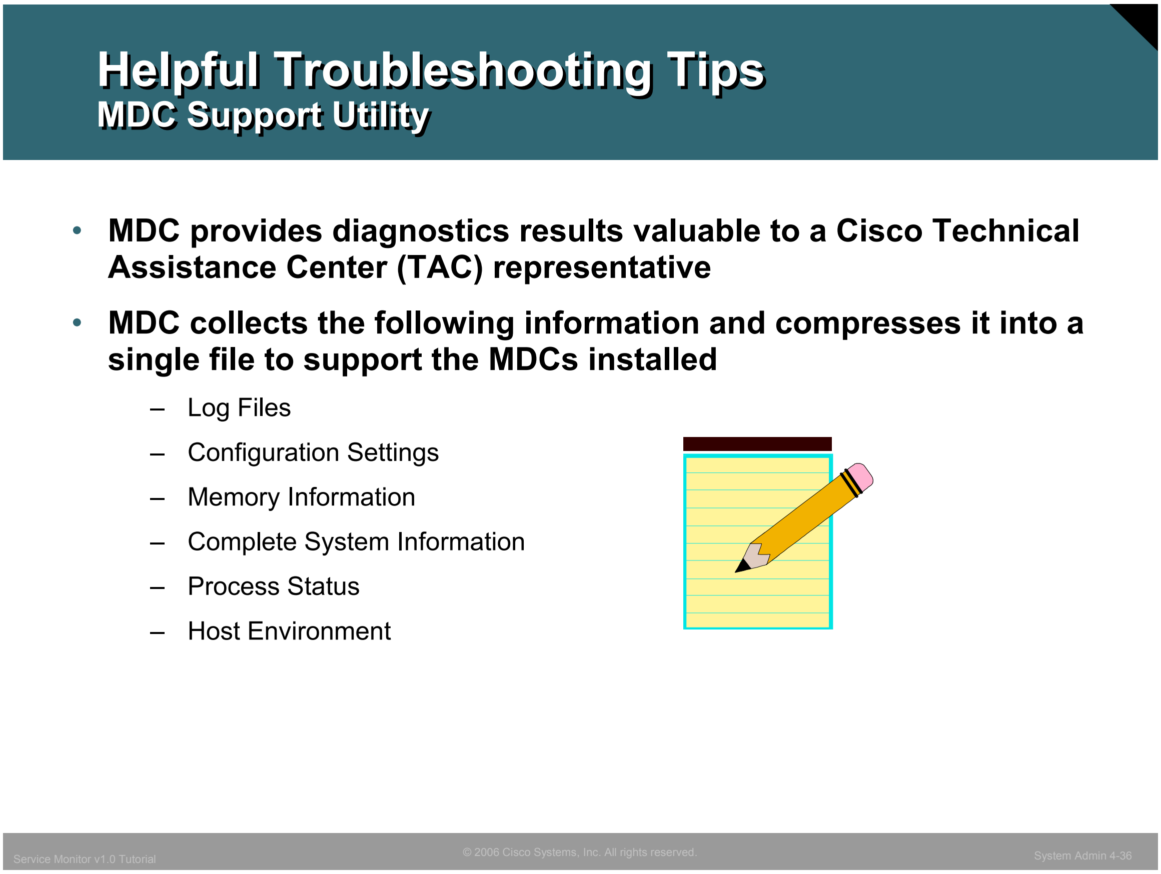
generated Fri May 27 23:45:20 2005

Table of contents

1. System Info
2. Environment
3. Memory and System Drive
4. Network Configuration
5. Event Logs
6. CiscoWorks Registry and components
7. ODBC Configuration
8. Process Status
9. Product Log Files
10. Tomcat Log Files
11. JRE registry

Environment

```
AdminEmail=admin@domain.com
ALLUSERSPROFILE=C:\Documents and Settings\Al
ASANY=C:\PROGRA~1\CSCOpx\objects\db
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common F
COMPUTERNAME=BLR-LMS1
ComSpec=C:\WINDOWS\system32\cmd.exe
CORE_NONSECURE_PORT=1741
CORE_SECURE_PORT=443
CWMIBDIR=C:\PROGRA~1\CSCOpx\objects\share\mi
FP_NO_HOST_CHECK=NO
LM_LICENSE_FILE=C:\PROGRA~1\CSCOpx\objects\s
NMSROOT=C:\PROGRA~1\CSCOpx
NUMBER_OF_PROCESSORS=4
OS=Windows_NT
OSAGENT_PORT=42342
Path=C:\PROGRA~1\CSCOpx\bin;C:\PROGRA~1\CSCO
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.J
```



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.

Cisco Systems

Empowering the Internet Generation^{SM}

Thank You!

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

Cisco Systems

<Intentionally Left Blank>

CISCO SYSTEMS

Service Monitor References

Chapter 5

<Intentionally Left Blank>

Reference Materials

Many Cisco reference documents have been created to help users understand the use of 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 Service Monitor.

- **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)**

    TBS

- ## Other Related Material

  - **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).