Cisco Unified Operations Manager Tutorial

Cisco Unified Communications Management Suite

About This Tutorial

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

About This Tutorial

This tutorial on Cisco Unified Operations Manager (OM) provides self-paced training focused on using the key features of the OM application.

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 OM product as well as its interaction with other related products.

How the Tutorial Is Organized

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

How This Tutorial Is Organized

The tutorial is divided into five chapters:

Chapter 1: Introduction

This chapter describes Unified Communications and highlights both the need for management and the challenges often encountered when managing Unified Communications devices and services.

Chapter 2: Operations Manager Product Features

This chapter discusses the key features of the Operations Manager (OM) application. The product is presented through both discussions of the major functional components and screen shots of many key features.

Chapter 3: Operations Manager Scenarios

This chapter walks you through step-by-step examples to provide hands-on experience using the Operations Manager application. The case studies begin with steps on how to get started, followed by using various features to manage the Unified Communications devices and services.

Chapter 4: System Administration Guidelines

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

Chapter 5: References

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

<Intentionally Left Blank>

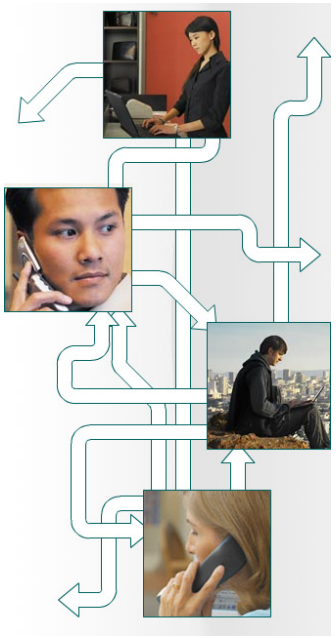
Cisco Unified Operations Manager

Introduction

Chapter 1

Chapter 1 Outline

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



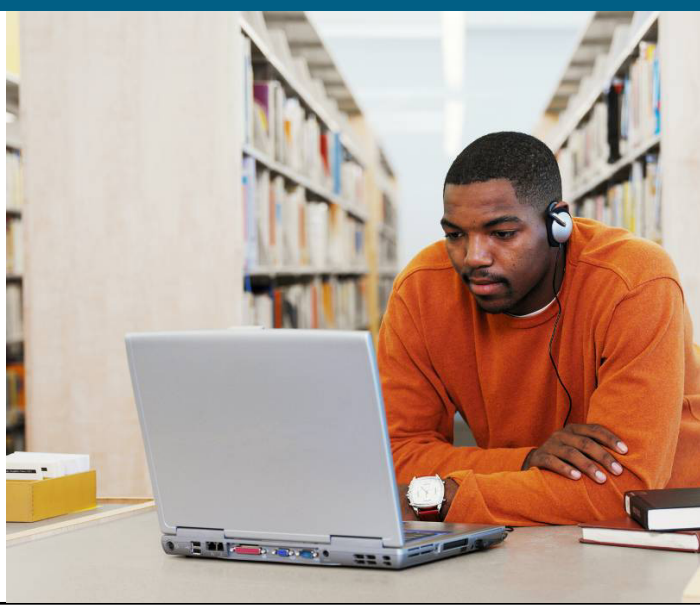
Chapter 1 Outline

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

Chapter 2 will then focus on all the features provided specifically by Operations Manager, followed by several scenarios in Chapter 3 that illustrate how to deploy and use some of the key features of the product. 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 Unified Communications, Operations Manager, and other related topics.

Managing Unified Communications

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



What is Unified Communications?

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

Unified Communications that ….

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

What is Unified Communications?

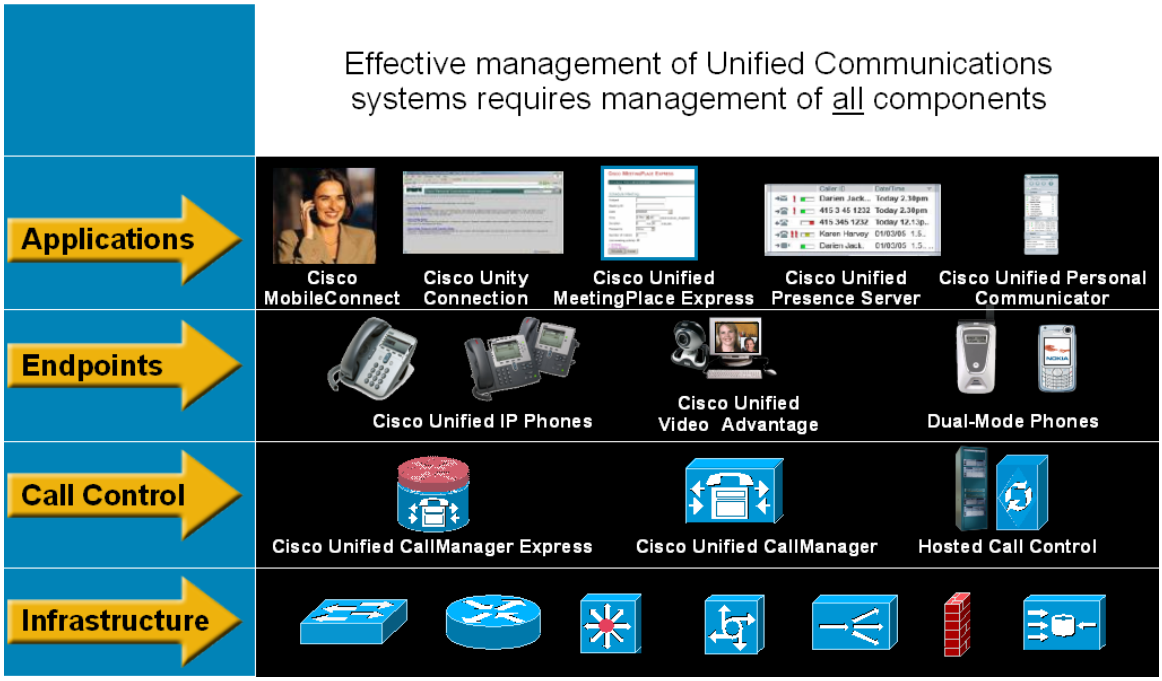
Today's organizations must contend with increasingly complex communication environments featuring a wide array of communication methods. Employees, business partners, and customers communicate with one another through infinite combinations of phones, voice messaging, e-mail, fax, mobile clients, and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

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

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

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

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



Managing Unified Communications

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

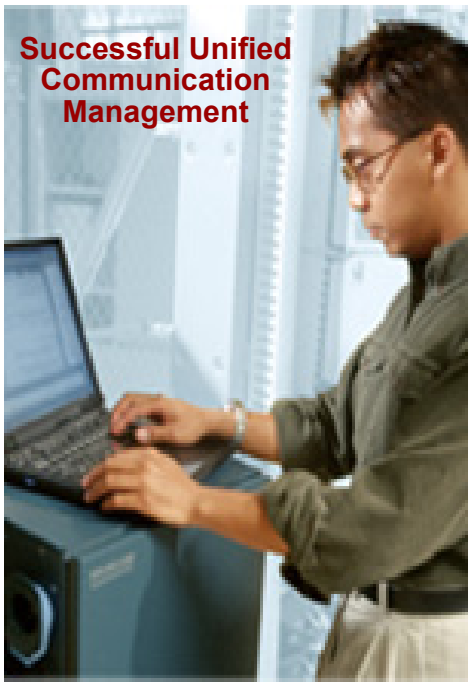
The Unified Communications environment consists of the IP transport devices and the IP communications intelligence built into the Unified Communications application services. It is a comprehensive system of powerful enterprise-class solutions which include:

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

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

Managing Unified Communications
Management Focus

1. Ensure infrastructure is rock solid and working properly
2. Implement QoS techniques and gather measurable metrics
3. Regularly monitor Unified Communications applications for availability of services
4. Monitor and test various end points (I.e. IP phones) across different boundaries



Management Focus

Unified Communications and network management begins with visibility into the network infrastructure, its performance, the applications used across the network, and the end points – the users and their computers or IP phones. Your job is to understand how to obtain visibility into these components, gather information about the components and their performance, and understand your network and how it can work for you. Cisco's infrastructure and network management tools are the starting points. The upcoming pages will highlight these areas of focus in more detail.

Managing Unified Communications
Managing The Infrastructure

IP infrastructure is used to transport voice, video, and data traffic

- Provide details about devices, connectivity, and Unified Communications applications, services, and relationships
- Monitor devices for conditions that could lead to service degradation
- Monitor network paths to verify compliance with acceptable latency / jitter
- Provide device and telephony-related metrics and details

Cisco Voice Enabled Routers & Switches

Managing the Infrastructure

The first area of focus in Unified Communications management should start with the infrastructure, ensuring that the foundation is rock solid and properly configured to handle Unified Communications. Routers and switches comprise the IP transport devices in your Unified Communications environment. There are few important factors when choosing a router or switch for Unified 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.

Secondly, focus on quality of service (QoS) for Unified Communications by monitoring performance using QoS metrics and implementing QoS techniques where needed. Next, let's look at various service quality and voice quality metrics.

Managing Unified Communications
Measurable Service Quality Metrics

Response Time / Latency	The elapsed time between the end of a query on one end of a conversation pair and the beginning of a response from the other end of a pair. Latency, a function of response time, is any characteristic of a network or system that increases the response time.
Availability / Outages	Critical to IP Communications is the availability of the network and the 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

Measurable Service Quality Metrics

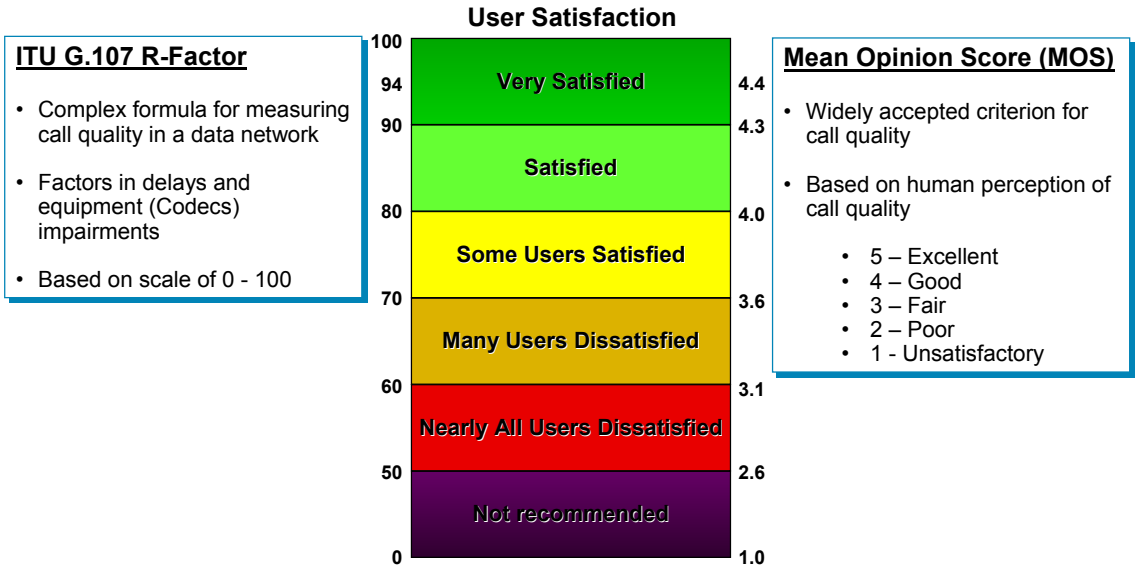
Network managers look for measurable statistics such as jitter, packet loss, and end-to-end network latency, in order to ensure acceptable service levels. Familiarize yourself with these metrics and what they mean in terms of absolute value, or when comparing or trending over time.

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

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

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

Managing Unified Communications
Measurable Voice Quality Metrics



Measurable Voice Quality Metrics

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

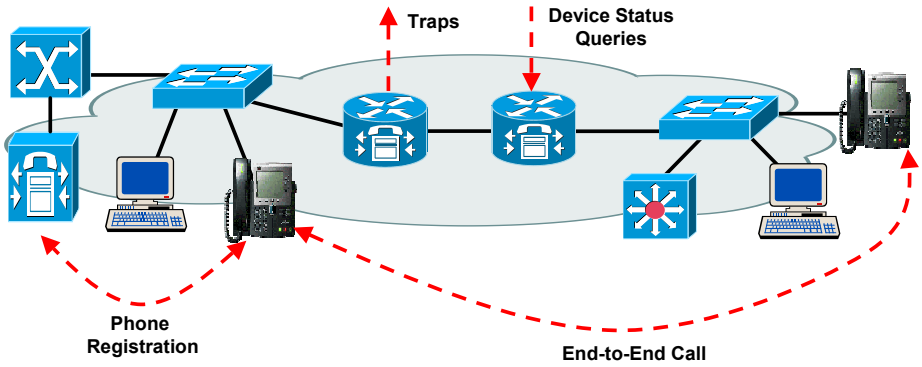
Traditionally, measuring call quality has been very subjective: a human picks up the phone and listens to the voice and provides his or her perception on the quality of the call. In fact, this is the basis for the widely accepted criterion for call quality, the *Mean Opinion Score (MOS).*

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

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

Managing Unified Communications
Managing Call Control Services and Applications

- Real-time monitoring and alerting on the availability of services
  - Are voice gateways and CallManagers reachable?
  - Are call conferencing and messaging available?
  - Can IP phones obtain a dial tone, register, or complete calls?
- Proactive testing to detect potential impacts to service early on

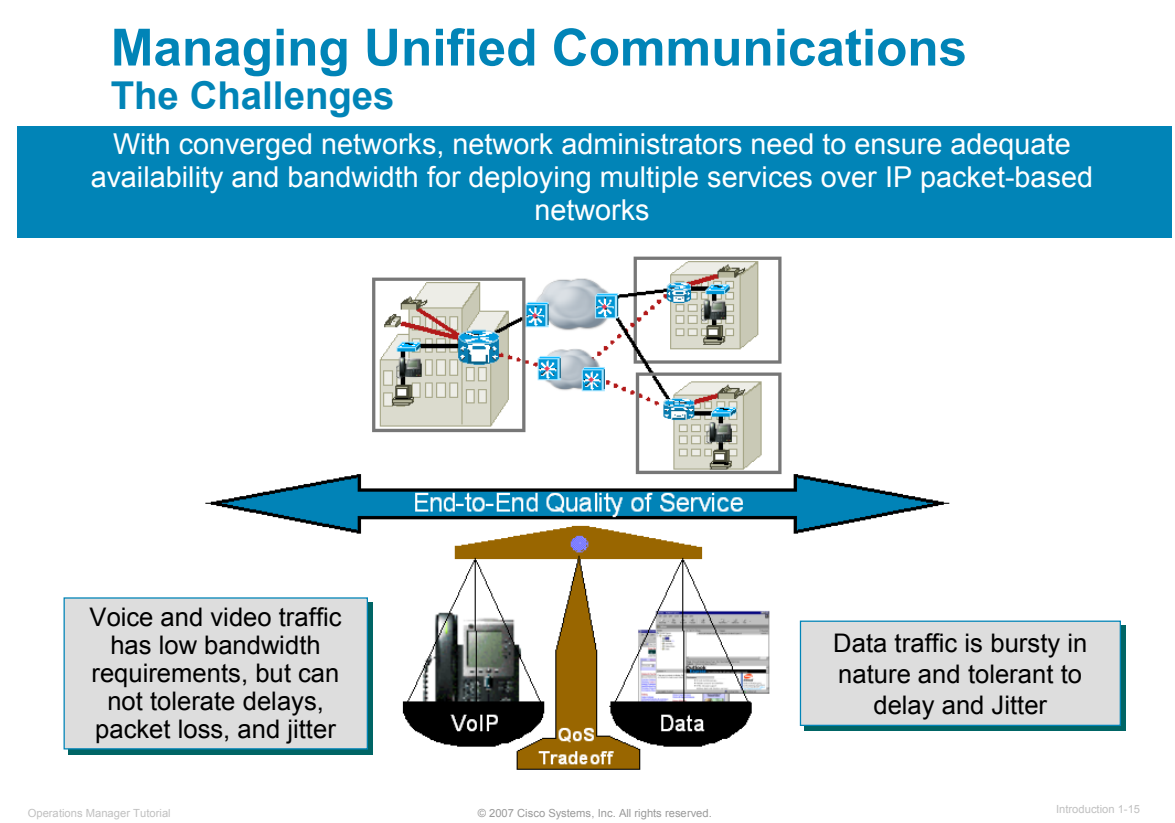


Managing Call Control Services and Applications

Other areas of focus are the Unified Communications applications and the end points in the network – users and their computers or IP phones. Unified Communications is dependent on CallManagers and gateways working properly. These Unified Communications services provided by both the transport devices and the Unified Communications applications are critical to successful operations. Therefore, it is critical to monitor these services for availability. The following represents a sampling of monitoring functions available to the network manager:

- Diagnostic Tests – Run tests to determine the state of the services provided by an Unified Communications application. This can be done by generating synthetic tests or monitoring actual transactions. Results can be compared against pre-defined thresholds and used to trend overall behavior.
- Polling – Use SNMP queries to retrieve transport device status to determine overall health.
- Traps – Forward SNMP traps (alerts of conditions) from transport devices to receive real-time indication of potential problems.

And finally, monitoring and testing the end points (I.e. IP phones) in the network will ensure continuous communication across different boundaries.



The Challenges

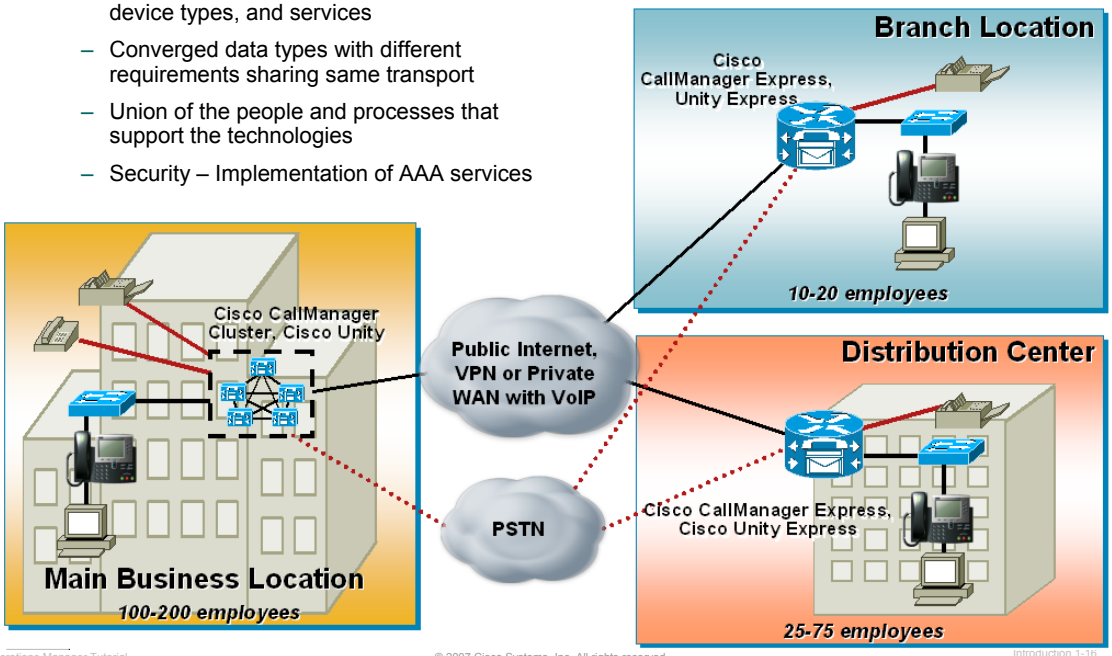
Businesses are constantly searching for methods to increase their effectiveness while attempting to cut costs. One cost savings step was the convergence of their voice, video, and data networks. Converged networks present businesses with a new communications paradigm, which has the potential to create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

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

Managing Unified Communications

The Complexity

- Growing number and complexity of devices, device types, and services
- Converged data types with different requirements sharing same transport
- Union of the people and processes that support the technologies
- Security – Implementation of AAA services



The Complexity

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

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

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

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

Managing Unified Communications
The Questions

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

The Questions

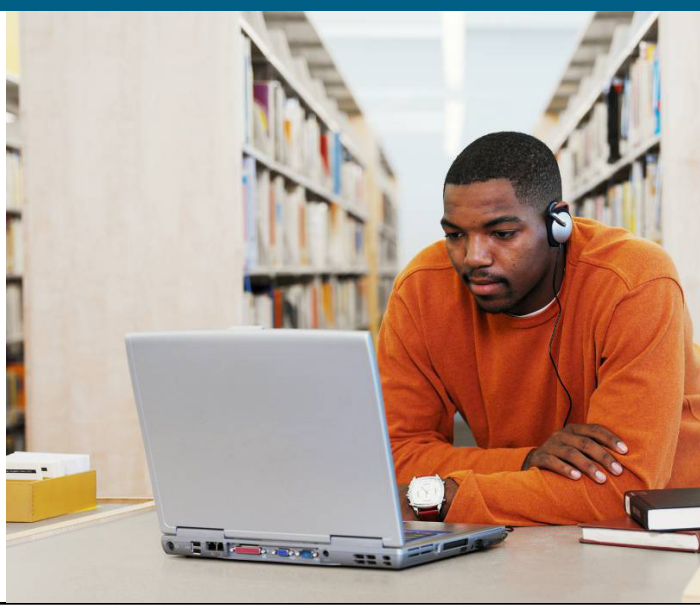
So the decision was made a long time ago to deploy IP telephony and now that has expanded to more than just voice calls over your IP network. Your role as a network manager is ever changing and now you are asking questions like these above.

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

<Intentionally Left Blank>

Cisco's Solution

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



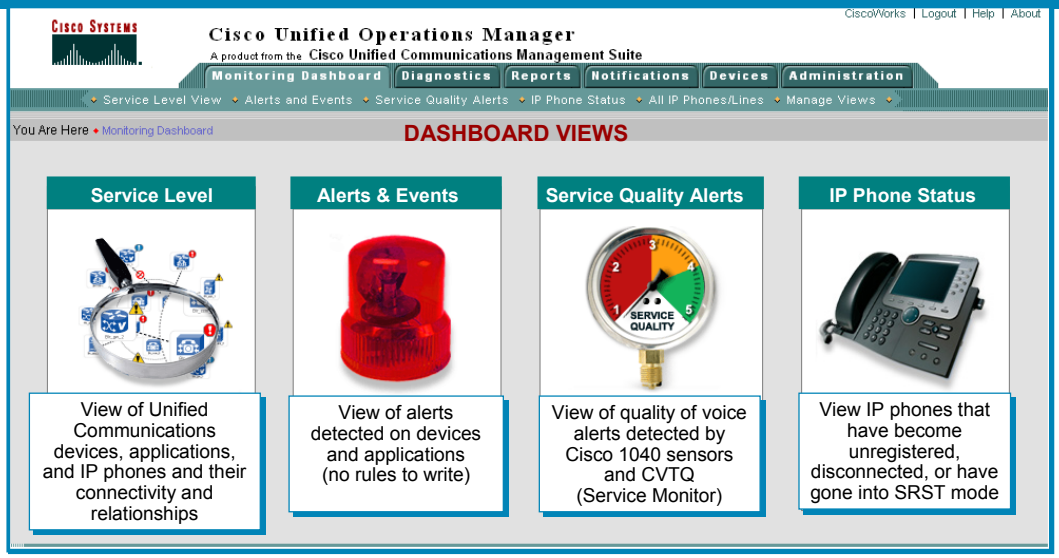
Cisco's Solution
Unified Communications Management Suite

Unified Communications Management Suite

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

Cisco's Solution
Unified Operations Manager (OM)

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



Cisco Unified Operations Manager

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

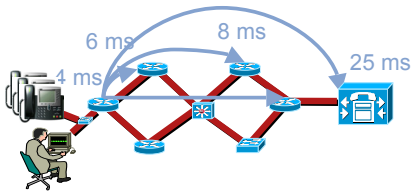
Information is presented by a series of 4 dashboards (representing different service-level views of the network), providing the network manager with a comprehensive view of the Unified Communications infrastructure and its current operational status.

The remaining chapters in this tutorial will look at each of these dashboard views (Chapter 2) and how to use these views in various scenarios (Chapter 3).

Cisco's Solution
Unified Operations Manager, (Cont.)

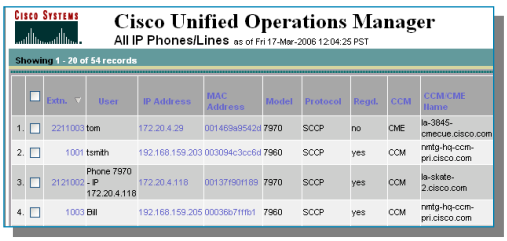
Diagnostic Tests

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



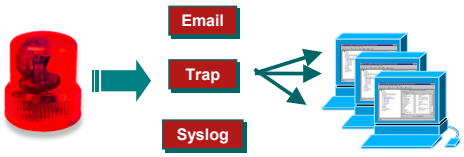
Report Generation

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



Notification Services

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



Cisco Unified Operations Manager, (Cont.)

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

Diagnostic Tests

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

Report Generation

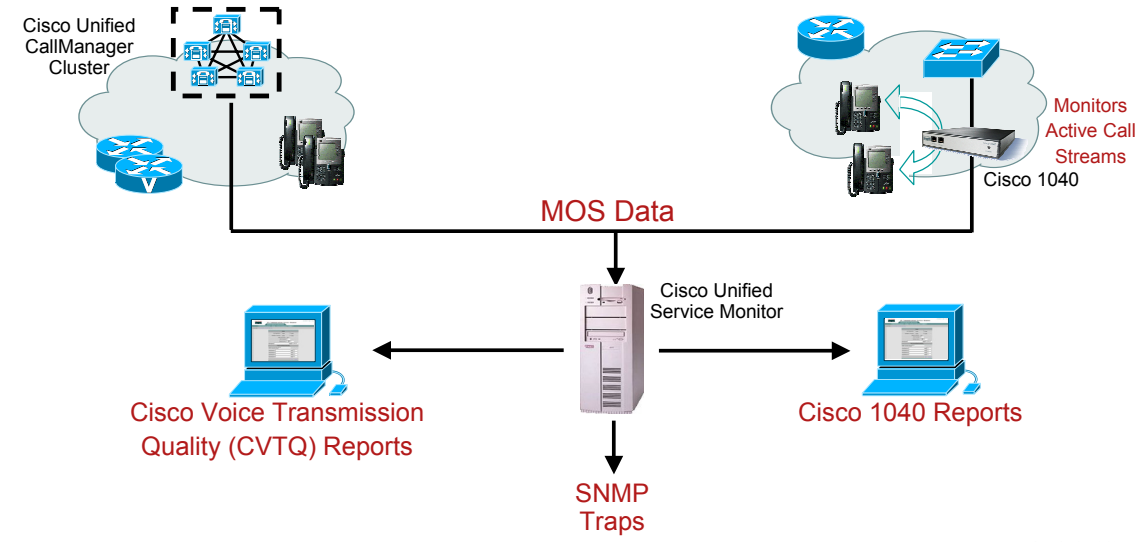
Operations Manager provides an extensive set of reports that help network managers maintain information about their Cisco Unified Communications deployment. The historical alert, event, and service-quality reports maintain information about all the alerts and events reported by Operations Manager for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

Notification Services

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

Cisco's Solution
Unified Service Monitor (SM) / Cisco 1040 Sensors

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



Cisco Unified Service Monitor / Cisco 1040 Sensors

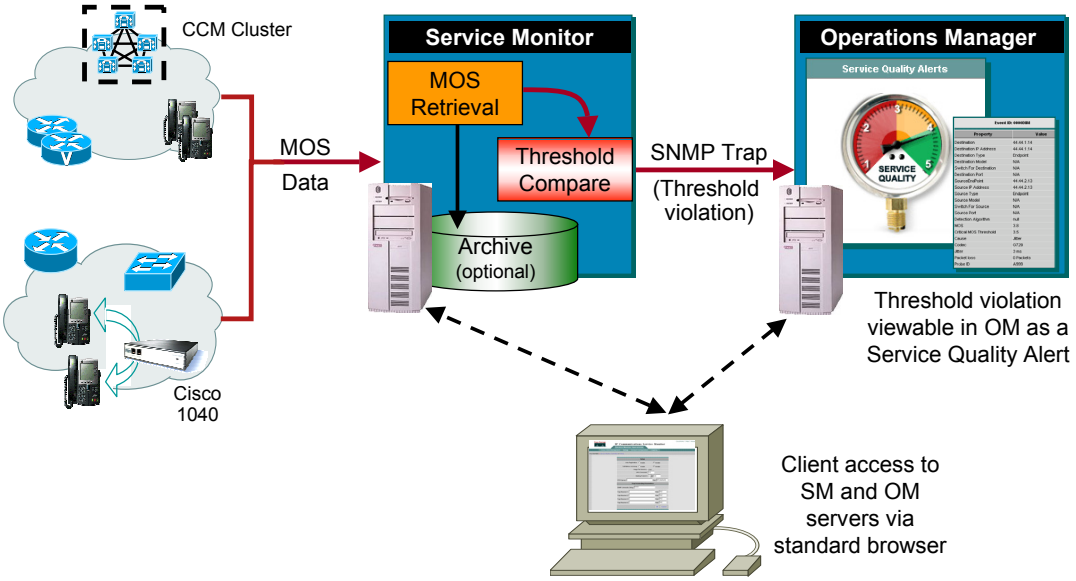
Cisco Unified Service Monitor is another application in the Cisco Unified Communications Management Suite. Service Monitor (SM), Cisco 1040 sensors, and the Cisco Unified CallManager clusters provide a reliable method of monitoring and evaluating voice quality for IP phones. The Cisco 1040 sensor continuously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

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

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

(Refer to the Cisco Unified Service Monitor Tutorial and Chapter 5 of this tutorial for more information on Service Monitor and the Cisco 1040 Sensors.)

Cisco's Solution
Product Integration



Product Integration

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

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

How to configure the integration is describe within this tutorial.

Cisco's Solution
Product Compatibility

Cisco Unified Communications Operations Manager and Cisco Unified Communications Service Monitor supports deployments consisting of:

- Cisco CallManager
- Cisco CallManager Express
- Cisco Unity
- Cisco Unity Express
- Cisco Meeting Place Express
- Cisco Conference Connection
- Cisco Unified Presence Server
- Cisco Unity Connection
- Cisco Unified Contact Center
- Cisco Unified Contact Center Express
- Cisco Telepresence Stations (CTS series)
- Cisco Emergency Responder
- Cisco Personal Assistant
- Routers, Gateways, Switches, IP Phones, and Video Phones

Product Compatibility

The Cisco Unified Communications Management Suite is compatible with the Unified Communications products highlighted above.

Thank You!

Continue on to Chapter 2 to discover the many features of Operations Manager.

Cisco Systems

Cisco Unified Operations Manager

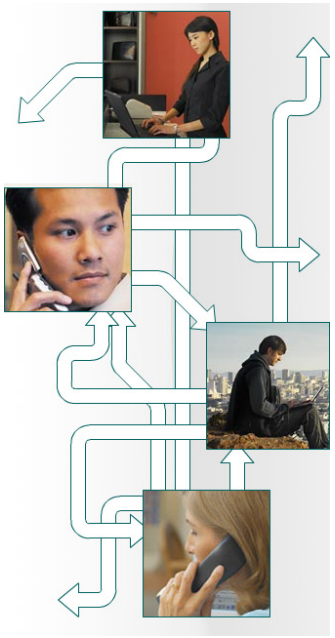
Product Features

Chapter 2

Chapter 2 Outline

Operations Manager Product Features

- Operational Status Views
- Diagnostic Tests
- Inventory Management
- Reports
- Event Notification
- Customization / Advanced Features



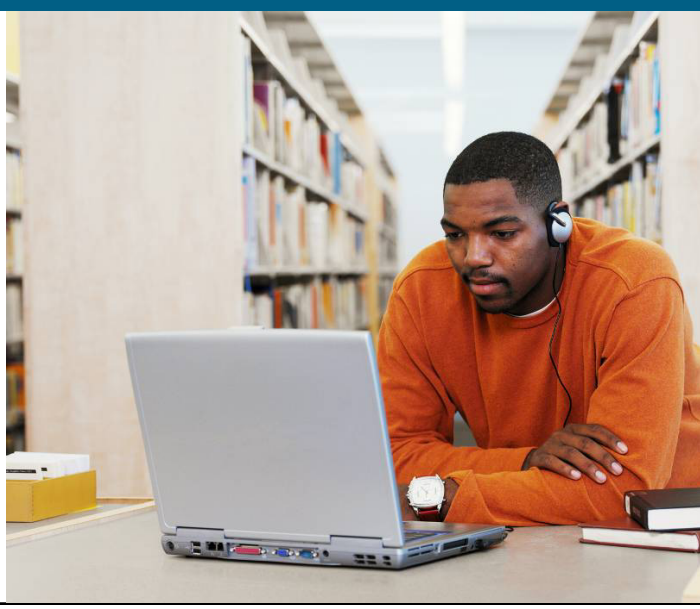
Chapter 2 Outline

Hopefully Chapter 1 has excited you to the possibilities of using Operations Manager to help manage your Unified Communications devices and services. This chapter discusses the key features and services provided by Unified Operations Manager (OM).

By the conclusion of this chapter, the reader should have a good understanding of the services provided by Operations Manager. Chapter 3 will then provide the jump start to using Operations Manager through a series of scenarios that detail some common network management situations.

Operational Status Views

- **Operational Status Views**
- Diagnostic Tests
- Inventory Management
- Reports
- Event Notification
- Customization / Advanced Features



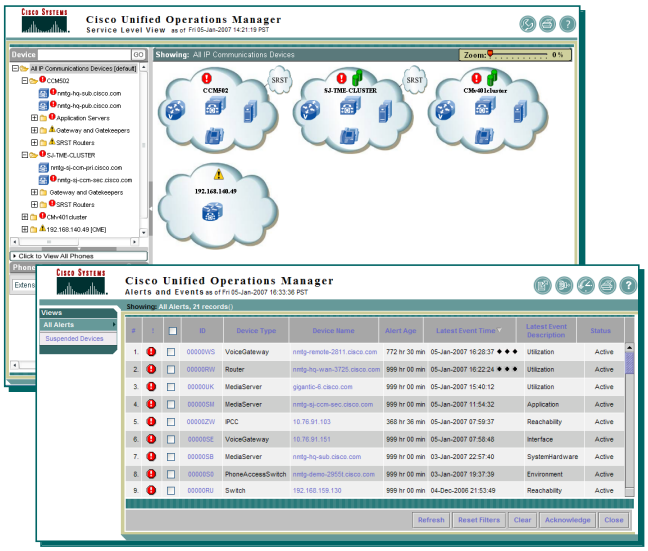
Operational Status Views
Overview

Dashboards (4)

- Service Level View
- Alerts and Events
- Service Quality Alerts
- IP Phone Status

Views in Dashboards

- Device Groups limit / control the amount of information in a view
- Default Views (2)
  - All Alerts
  - Suspended Devices
- Customize Views - Select the devices seen in a view
- Filter controls - Limit devices seen in a view



Tip: All dashboards can be bookmarked in browser for quick access

Operational Status Views – Overview

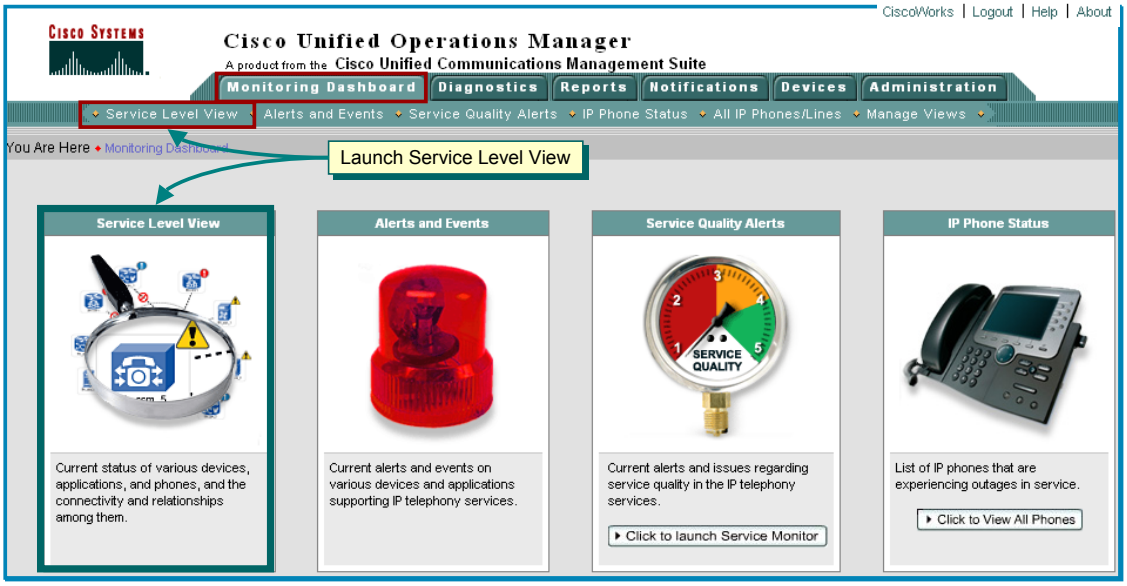
Operations Manager provides you with four monitoring dashboards: Service Level View, Alerts and Events, Service Quality Alerts, and IP Phone Status. The launch point to these dashboards are the first screen that the user will see when launching Operations Manager. On a day-to-day basis, operations personnel are likely to use these monitoring dashboard displays to monitor the Unified Communications environment. Network administrators and operators might similarly use the monitoring dashboard displays and Alert and Event History reports to assess network health and the IP phone reports to solve IP phone problems.

Because the Unified Communications network can be large, organization of information is key to network management. Thus, "Views" are used within Operations Manager to organize or limit and control the amount of information displayed at one time. Views are logical groupings of devices that appear in the Monitoring Dashboard displays. By default, the Alerts and Events, Phone Activities, and Service Quality Alerts displays contain two default views: All Alerts and Suspended Devices. These views are static and cannot be edited, deactivated, or deleted. The Service Level View display contains the All IP Communications Devices view, which is a default view that cannot be edited, deactivated, or deleted. Once you decide how you want to cluster your devices into a logical set, you can create and activate a view of these groups so they are shown in the Monitoring Dashboard displays.

Even a view can have a wealth of information. Thus, filter controls are available within the Monitoring Dashboards to further limit the information displayed or can help you locate the information that you are looking for. (*An example of creating new views is illustrated in Chapter 3, Scenarios*.)

Now, let's look at the content within each of these Monitoring Dashboards!

Operational Status Views
Service Level View Dashboard

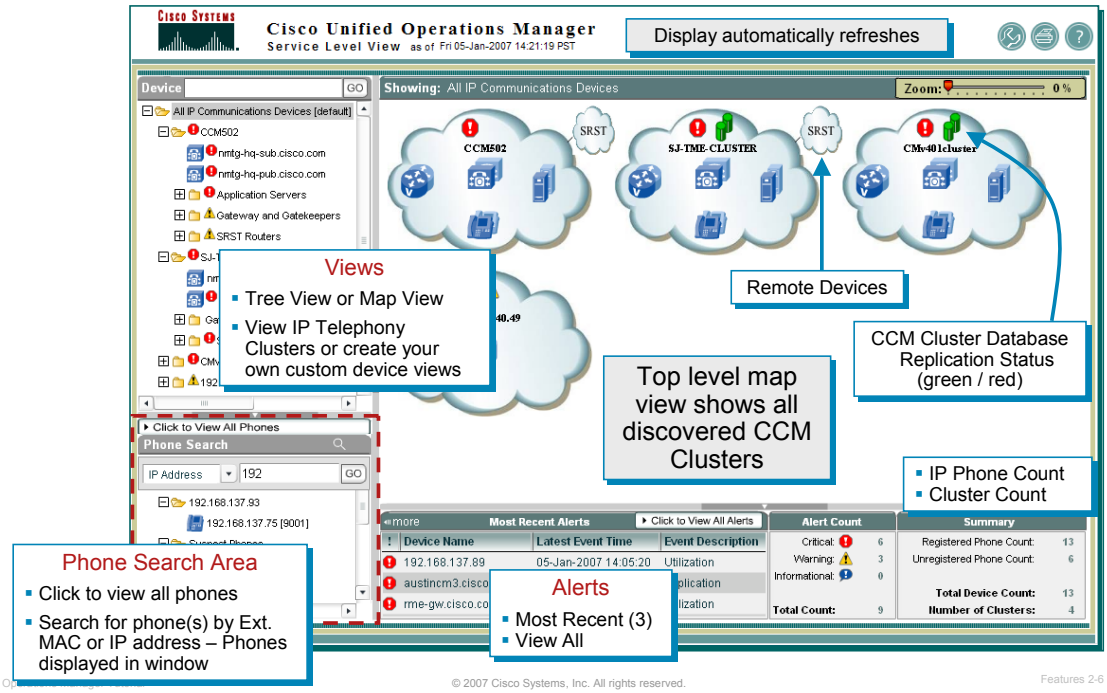


Service Level View Dashboard

One of the four Monitoring Dashboards in Operations Manager is the **Service Level View**. This view allows network managers to visualize their Unified Communications deployment. This view is a real-time auto-refresh display that provides summary and status information about all the Unified Communications clusters and the elements of the clusters in the deployment. The view displays a logical topology view of your Unified Communications implementation and focuses on the call control relationships.

The Service Level View is accessible under the Operations Manager Monitoring Dashboard tab. Either select the menu under the Monitoring Dashboard tab or click on the ***Service Level View*** picture (*notice that the icon changes when the cursor is placed over the top of it*).

Service Level View Dashboard
Overview



Service Level View – Dashboard Overview

Cisco Unified Operations Manager's Service Level View display a logical topology view and allows network managers to visualize their entire Cisco Unified Communications deployment.

This logical view focuses on call control relationships. The Service Level View shows all the Cisco Unified CallManager clusters and all route groups and route lists in the clusters; all instances of Cisco Unified CallManager Express (and their logical groupings); associated gateways, gatekeepers, application servers, and Cisco IP Contact Centers (and their logical groupings); and SRST-enabled devices; as well as each component's registration status with Cisco Unified CallManager.

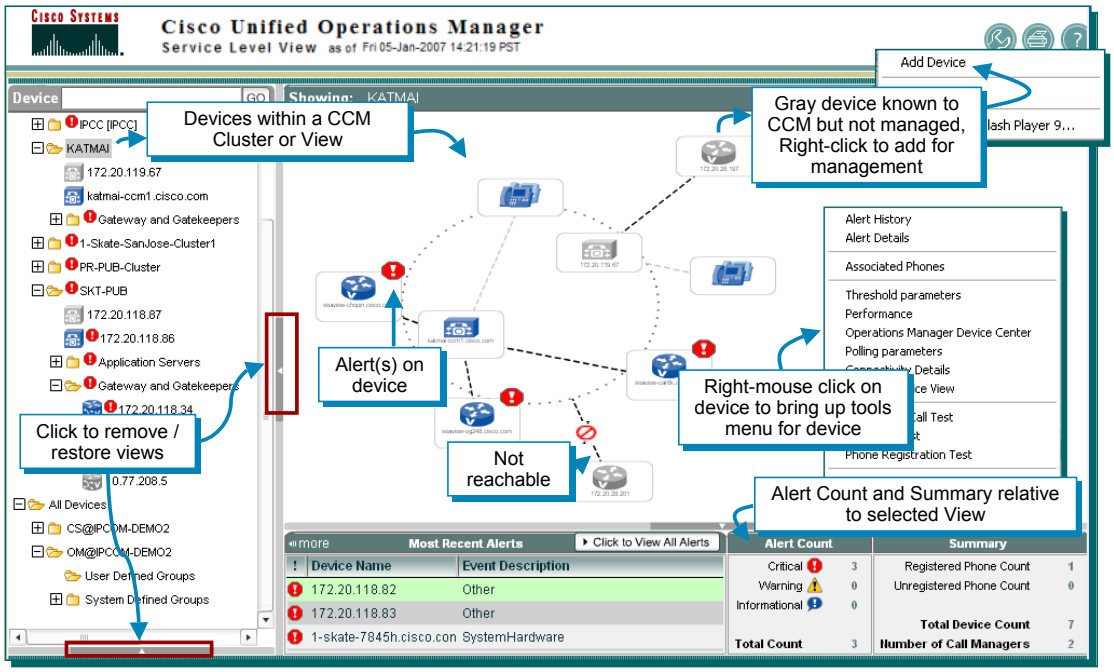
The Service Level View is designed so that it can be setup and left running, providing an ongoing monitoring tool that signals you when something needs attention. When a fault occurs in the network, Operations Manager generates an event or events that are rolled up into an alert. If the alert occurs on an element it is shown on the Service Level View.

The Service Level View is a tree based and map based display. It displays all the IP Telephony clusters present in your network. The display uses views (a logical grouping of device groups) to organize what you want to see. There is one default view called ***All IP Communications Devices*** and your own views can also be created. The ***All IP Communications Devices*** view contains all the Cisco CallManager clusters and all the devices associated with the clusters in your network.

You can use the Service Level View to:

- Display a logical or neighbor topology view of your Unified Communications deployment
- View most recent alerts, severity levels, and historical view
- Launch other Operations Manager tools
- Depending on the device type, launch other tools outside of Operations Manager or administration pages for devices, such as CCM Administration or Serviceability pages, Unity Administration, or Gateway Administration
- View IP Phone count (registered or unregistered), device count, and CCM count in the Summary view
- View latest changes
- Drill down into CCM cluster to view service level topology (next page)

Service Level View Dashboard
Device Group or Cluster Details



Service Level View – Device Group or Cluster Details

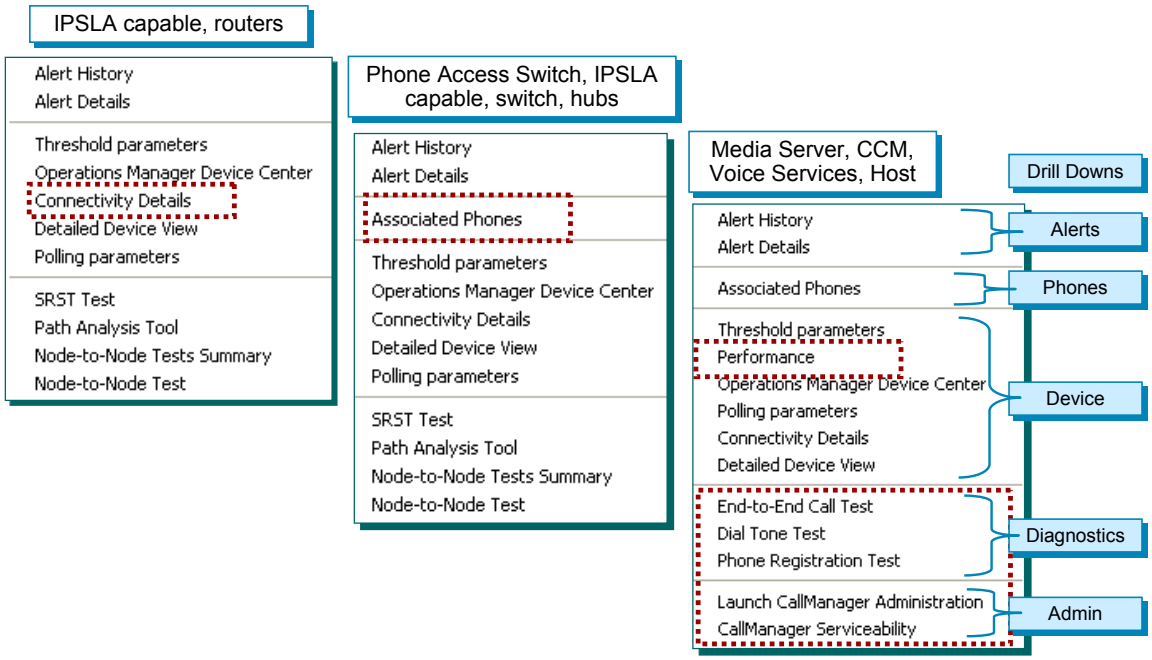
Drill down views show the operational status of each element of the Unified Communications cluster and its interrelationships with other elements. This display serves as the central point to initiate different functions that are available in Operations Manager.

A context-sensitive right-click menu is provided through which network managers can get detailed status as well as historical information about the alerts on each of the elements.

It is also possible to select different devices and initiate a variety of diagnostic tests, get access to performance-monitoring and capacity-monitoring information by way of graphs, or get IP connectivity details for a device by launching a neighbor topology view that shows Layer 2 physical connectivity for up to five hops from the selected device.

Operations Manager also makes available a set of context-sensitive tools outside of Operations Manager that can aid in further troubleshooting or diagnostics. The figure above shows the Service Level view for a multi-cluster Unified Communications deployment and its drill down details.

Service Level View Dashboard
Drill Downs Based on Device Capabilities



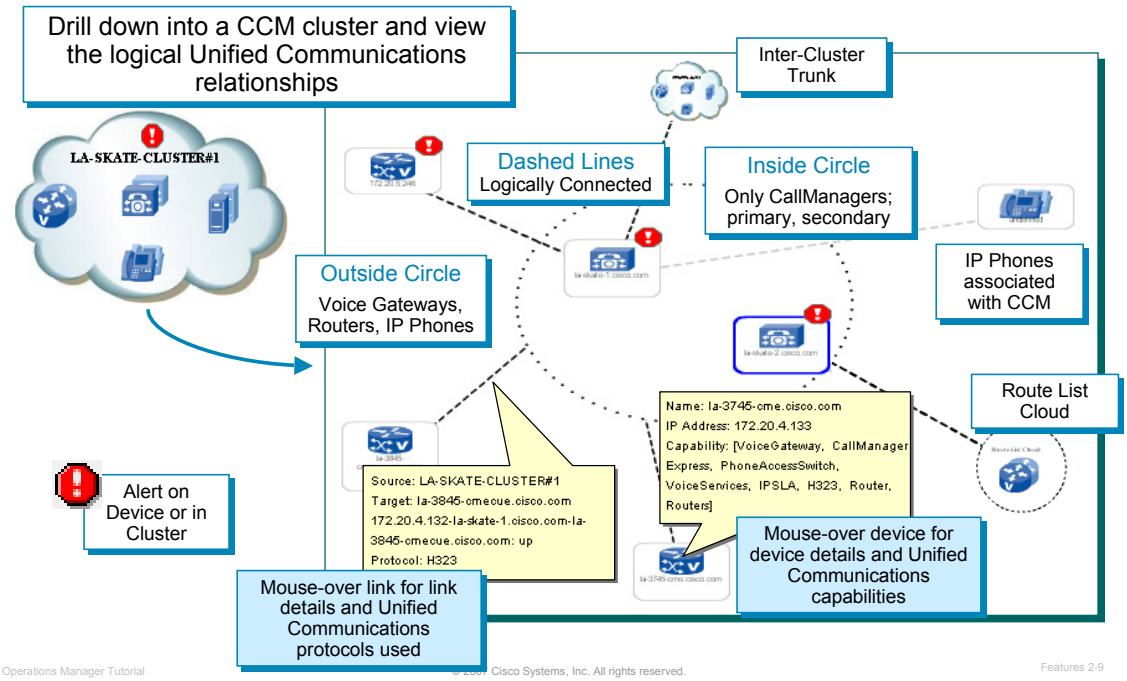
Service Level View – Drill Downs

Drill downs provide the next step for the user to take and are a great way to view more information or easily launch other tools on a selected device. For example, let's say a device is marked with a critical alerts in the Service Level View. By simply using the right mouse click on the device, the user is presented with available drill downs for more information (I.e. Look at the alert details, run a diagnostic test, or generate a report).

A context-sensitive right-click menu is provided as access to these drill down menus. The reports and tools available for selection differ based on the device selected. Operations Manager provides the appropriate drill down capabilities by first evaluating the device type and its capabilities. Illustrated above are different drill downs for various devices. The available drill down types are illustrated below. Remember, not all drill downs are applicable to every device; it will depend upon the device capabilities and services installed on the device.

- Alert
  - Alert Details
  - Alert History
- Device
  - Detail Device View
  - Performance, Polling, Thresholds
  - Connectivity Details (Physical Topology)
- IP Phone
  - Associated IP Phones
- Diagnostic Tests
  - Synthetic (End-to-End Call, Dial Tone, Phone Registration)
  - IP SLA (Node-to-Node)
  - SRST
- Administration (Cisco CallManager Administration / Serviceability)
- Other tools
  - Common Services
  - CiscoWorks Device Center

Service Level View Dashboard
Logical Relationships



Service Level View – Logical Relationships

Service Level View can be used to illustrate logical device connectivity. When drilling down into the CCM clusters using the map-based view, the signaling and Unified Communications solution relationships between devices is illustrated.

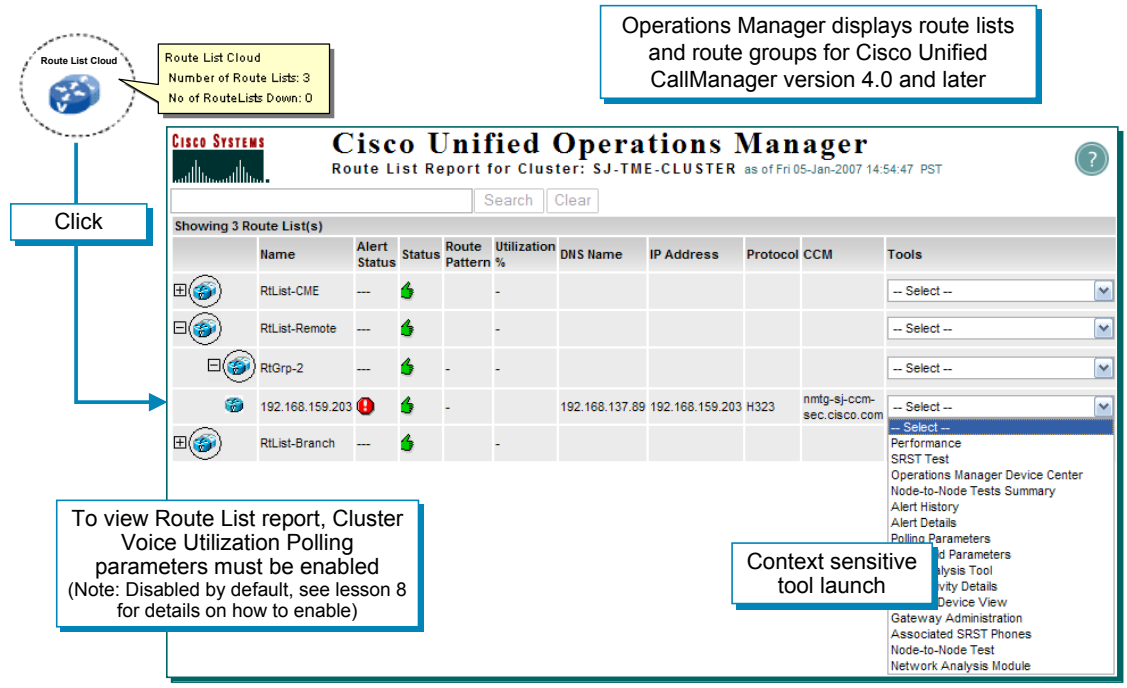
This logical view focuses on the call control relationships. All dashed lines represent logical connectivity. Inside the circle are the Cisco CallManagers for the cluster. From this view, it is easy to visualize the IP phones associated with the Cisco CallManagers and the associated call control relationships, as well as visualize the alerts that have occurred on the devices.

As illustrated above, some devices may be grayed out. This occurs when the device is not responding to OM using SNMP queries or is outside the discovery boundaries, but was discovered originally from the CCM discovery.

Also illustrated is the use of tool tips. Simply hold the cursor over a logical link and more information on the connection is displayed. This is not the physical connection, but the protocol connecting the two endpoints.

When the CCM cluster is marked with an alert, then one or more devices in the cluster has an alert. By drilling down into the CCM cluster, the devices with alerts are displayed. The alert icons can be one of the following severity levels:

Service Level View Dashboard
Route List Report



Service Level View – Route List Report

A Route List Cloud icon can be seen in the Service Level View. To generate a route list report, click the Route List Cloud icon in the view. The leftmost column contains various icons:

- Route List--Expand to view the route groups in the route list
- Route Group--Expand to view the gateways in the route group
- Voice Gateway--View the data for the gateway

The route pattern field describes the route pattern that is associated with the route list. It comprises one or more digits and wildcards (such as X which indicates a single digit) that represent a range of directory numbers that are either routed or blocked by the pattern.

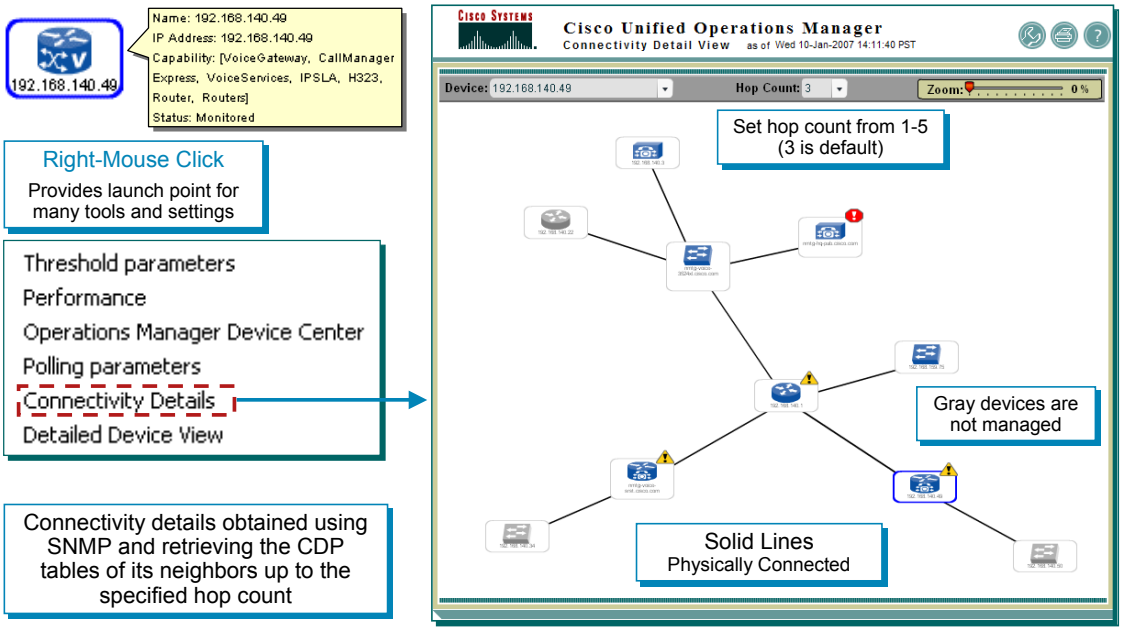
The utilization field has either one of the following:

- Percentage utilization for the route list, route group, or gateway. Note**:** For Operations Manager to obtain this data, polling for Cluster Utilization Settings must be enabled; it is disabled by default.
- N/A or dash (-)-move cursor over this column to view a tool tip with an explanation.

Note(s):

- Operations Manager displays route lists and route groups for Cisco Unified CallManager version 4.0 and later.
- For Operations Manager to obtain utilization data or route group data, polling for Cluster Utilization Settings must be enabled; it is disabled by default. To enable this setting, use **Administration> Polling and Thresholds**.

Service Level View Dashboard
Physical Relationships



Service Level View – Physical Relationships

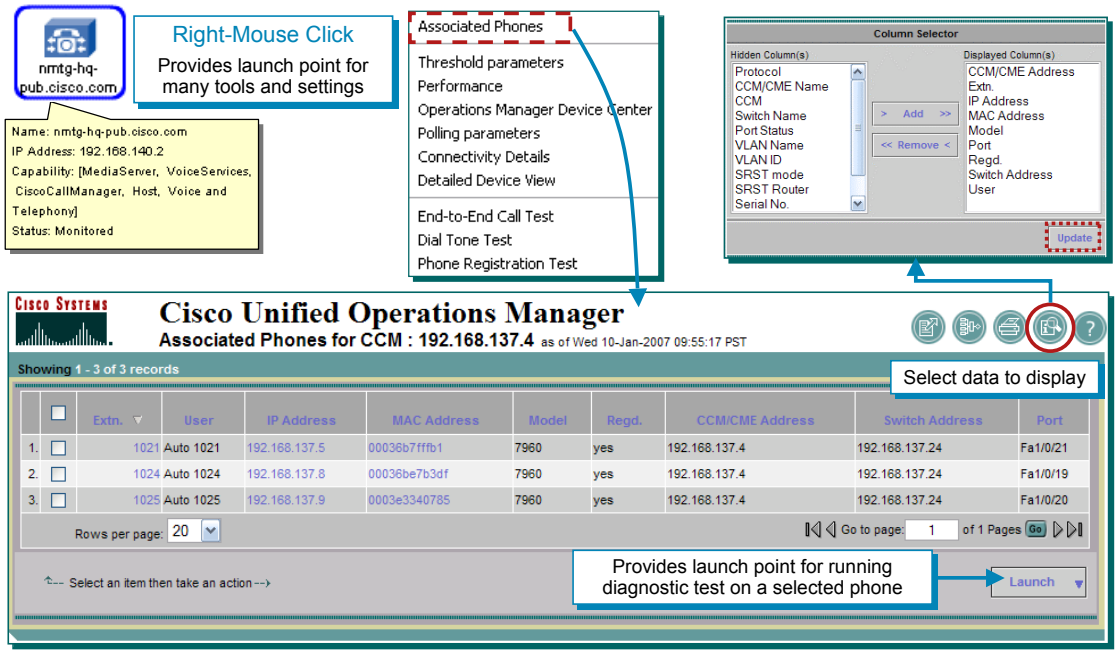
The Service Level View can also be used to illustrate physical device connectivity. Simply select a device that you want to view, right-mouse click, and select **Connectivity Details**.

The physical connectivity is obtained by using the access credentials (SNMP) defined in Operations Manager to retrieve the CDP (Cisco Discovery Protocol) table, containing port connectivity to neighboring devices. Once the neighbor device is known, its neighbors can be retrieved, if CDP is enabled and the access credentials allow to information to be viewed. If CDP is enabled on its neighboring devices, this continues up to the defined **Hop Count**, illustrated above. You can change the number of hops you want displayed (between one and five).

Operations Manager will gray-out devices that it is not communicating with; therefore, the devices could not be managed. This could occur due to the following:

- The device is not responding to OM using SNMP queries. The credentials either don't match between OM and the device, SNMP is not enabled on the device, or the protocol may be blocked by a firewall.
- The device is outside the discovery boundaries. The device could have been discovered originally from the CCM discovery.

Service Level View Dashboard
Associated IP Phones



Service Level View – Associated IP Phones

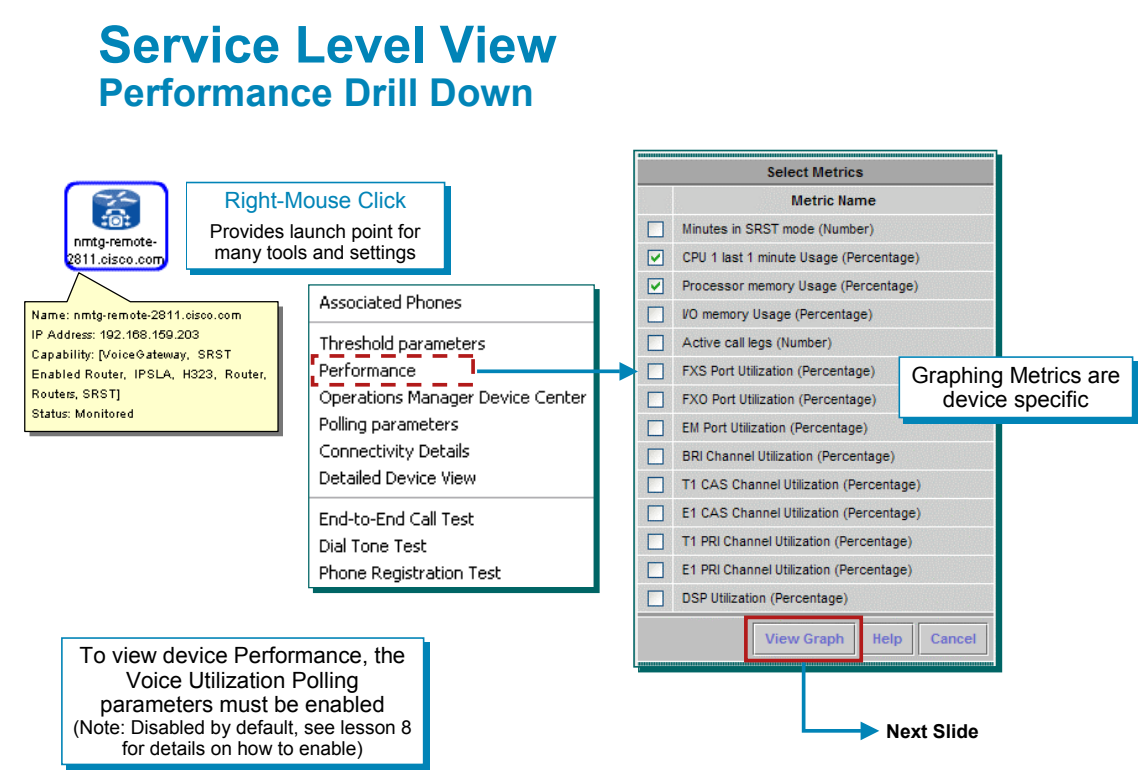
The Service Level View can also be used to display IP Phones associated with a selected Cisco CallManager. Simply select a CallManager that you want to view, right-mouse click, and select **Associated Phones**.

Tip: You can also get a report on *ALL* IP phones in several ways: The "**Click to View All IP Phones**" button on either the OM Home Page or the Service Level View dashboard (lower left corner; you may need to expand view), or from the OM Home Page, **Monitoring Dashboard> All IP Phones / Lines** menu.

As illustrated above, information such as the phone's extension, registered user, IP and MAC addresses, protocol, and associated CallManager can be obtained. If the phone is also connected to a managed switch that information is also provided.

Note(s):

- *The user name is available using one of two ways:*
  - *Using LDAP and a LDAP server is configured / defined in Operations Manager. (Chapter 3 describes how to configure a LDAP server in Operations Manager.)*
  - *Or, when a description for the phone has been entered in CCM*
  - *If both ways are available, LDAP takes precedence.*
- *The protocol illustrated is the protocol used between the phone and CCM.*
- *Registration status of the IP phone is with respect to Cisco CallManager or Cisco CallManager Express. The field displays **yes** if the IP phone is registered or **no** if the IP phone is not registered.*
- *SRST (Secure Survivable Remote Site Telephony) fields provide information if the phone is configured to fail over to an SRST router in case of a WAN link failure.*
- *The launch point links can be used to quickly configure diagnostics tests (SRST test, Synthetic Test, IP Phone Status Test) on a selected phone. More information on these tests is available in the Diagnostics Testing section of this chapter.*



Service Level View – Performance Drill Down

A user can select a device and examine changes in network performance metrics. The network performance data can be selected, displayed, and charted in real time. Performance graphs can be created from the data that is collected when either:

- Voice utilization polling is enabled for devices. Voice utilization polling is disabled by default. To enable this setting, use **Administration> Polling and Thresholds**.
- Data is available on disk from node-to-node tests that you have configured.

Service Level View
Performance Graph

Service Level View – Performance Graph

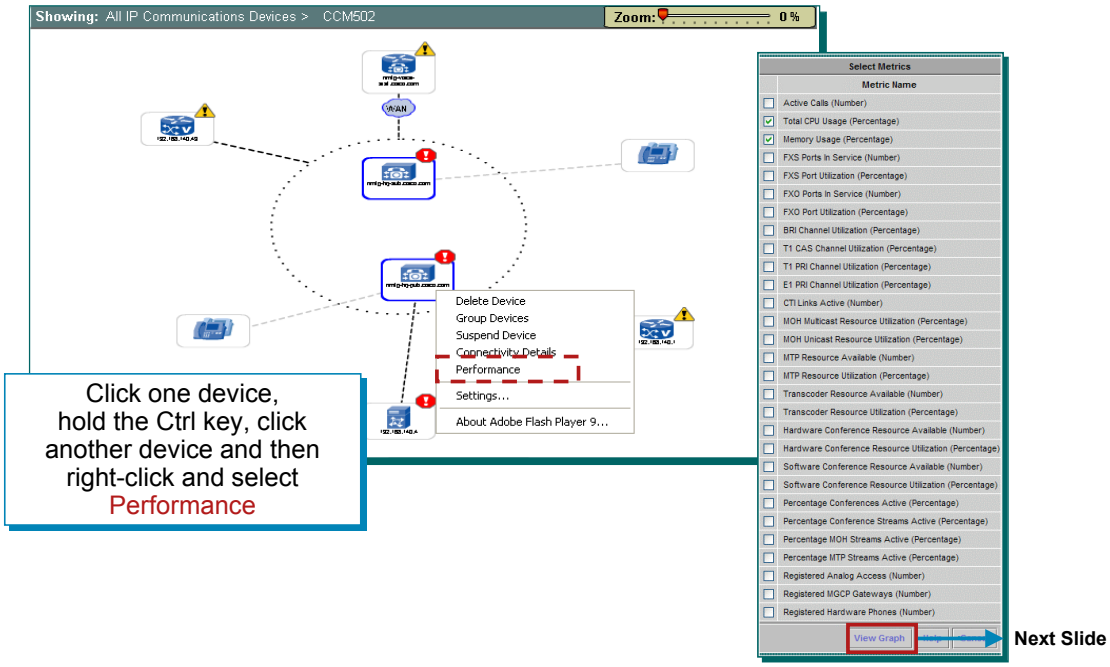
Performance graphs provide real-time information and historical information. When you launch a performance graph, one line graph is displayed for each metric that you select. Each line graph contains 16 data points displayed in real time.

The graph menus allow you to change the display:

- Time line: Real Time (default) or select the number of hours of data to graph, up to a maximum of 72 hours. If you select a device that does not have data available for the selected time interval, a message appears stating such. An empty graph appears and refreshes periodically automatically. At any time, you can change the time interval to get historical information, if there is any.
- Graph Type: Line Graphs (default) or select Bar Chart or Area Chart.
- Data Points: 16 data points (default) or select up to a maximum of 240 data points.

Additionally, you can **show all graphs or merge all graphs** regardless of the unit of measure. When you select the **Merge** radio button, the merged graph is scaled to show all the metrics in the single graph.

Service Level View
Performance Graphing Multiple Devices

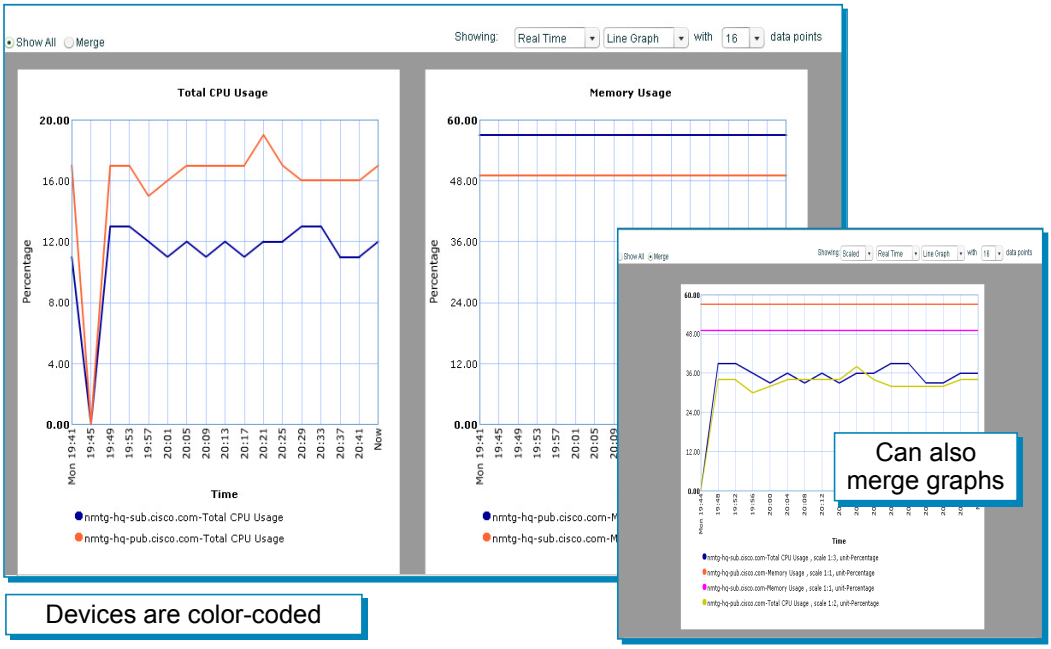


Next Slide

Service Level View – Performance Graphing Multiple Devices

To graph data for more than one device together, click one device, hold the Ctrl key, click another device, and then right-click and select **Performance** from the menu. Let's look at an example on the next page.

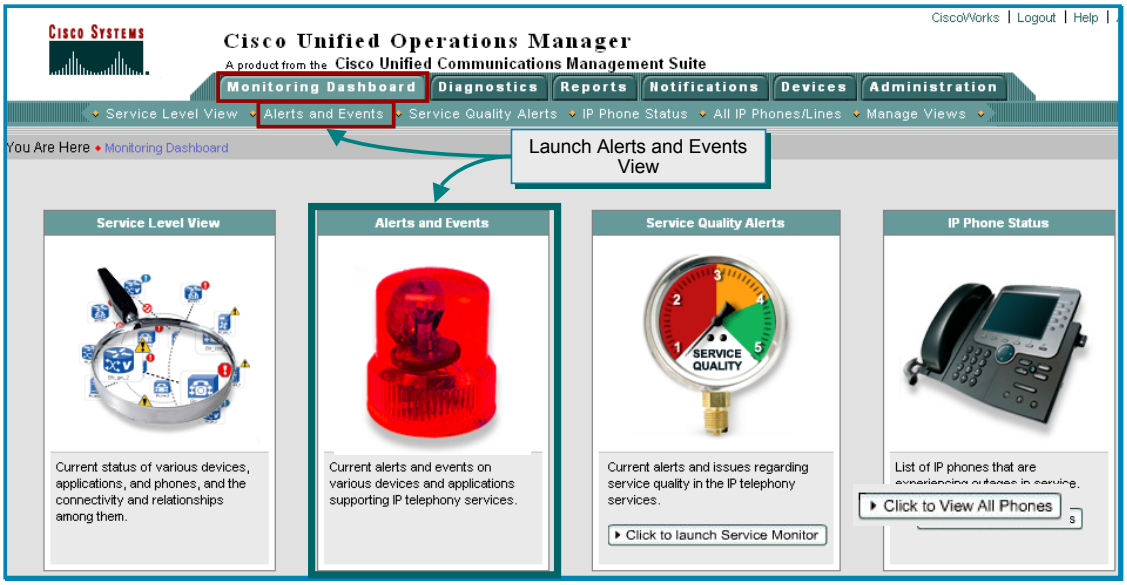
Service Level View
Multiple Devices Performance Graph



Service Level View – Multiple Devices Performance Graph

Above is an example of the network performance data graphed for multiple devices.

Operational Status Views
Alerts and Events Dashboard



Alerts and Events View Dashboard

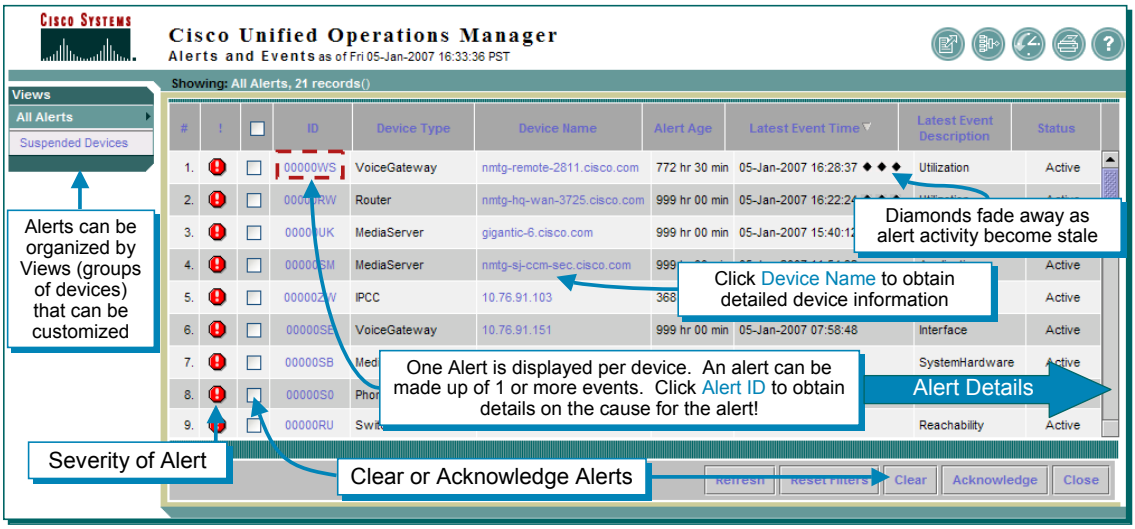
The second of the four Monitoring Dashboards in Operations Manager is the ***Alerts and Events*** View. This view provides real-time information about the operational status of your network.

The view is accessible under the Operations Manager Monitoring Dashboard tab. Either select the menu under the Monitoring Dashboard tab or click on the ***Alerts and Events*** picture (*notice that the icon changes when the cursor is placed over the top of it*).

Alerts and Events Dashboard
Overview

Alert and Events View

A device is monitored for many conditions. When one or more of these conditions is problematic, a single alert on the device is displayed in the Alert and Events View.



Alerts and Events – Dashboard Overview

The **Alerts and Events** view is illustrated above. These alerts are per device and are caused by one or more events detected by monitoring the device with Operations Manager. Operations Manager comes with built-in intelligence that can understand the role of every device in an IP deployment, and it appropriately monitors those devices for any kind of faults or outages. There is no need to write any rules to start monitoring the Unified Communications deployment; all the rules are built into the product. It also comes with factory-defined thresholds (which can be further tuned by network administrators) and an analysis engine that can detect the violation of any of these thresholds and immediately alert network managers through multiple means.

Alerts are presented to the user through the Alerts and Events Display, which refreshes periodically to present the most up-to-date status of the Unified Communications deployment being monitored. A separate display called the IP Phone Status Display, discussed later in this section, provides instant access to IP phone outage information.

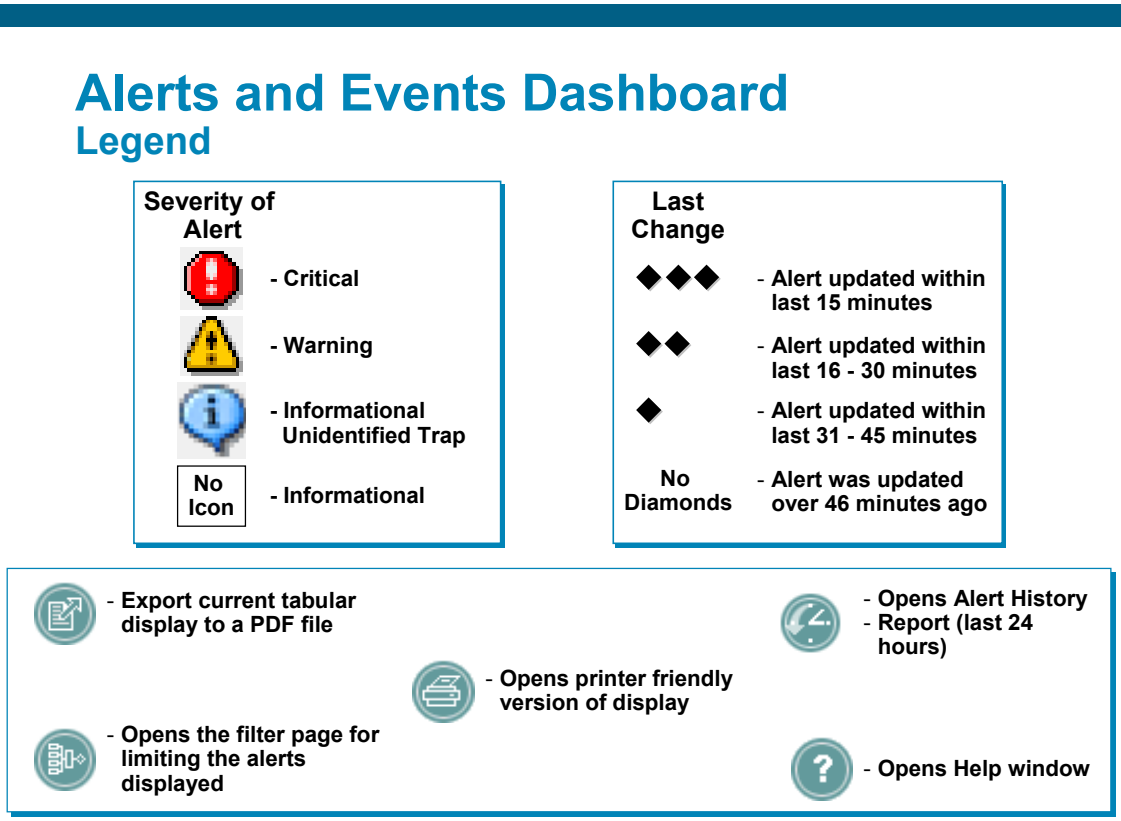
The display is designed so that you can have Alert views for all devices or customized device groups (views), providing an ongoing monitoring tool that signals you when something needs attention. (*Creating customized device views is discussed later in this chapter.*)

When a condition occurs in the network (i.e. monitored parameters exceed a threshold or a service/interface is down), Operations Manager generates an event, and events for a single device are rolled up into an alert on the device. If the alert occurs on an element in your active *view* (a logical grouping of device groups), it is shown on the Alerts and Events display.

To view the event(s) that triggered an alert on the device, simply click the ***Alert ID***.

Note(s):

- *For a device to be monitored by Operations Manager, it must be supported by Operations Manager and added to the OM Inventory (refer to the Device Management section discussed later).*



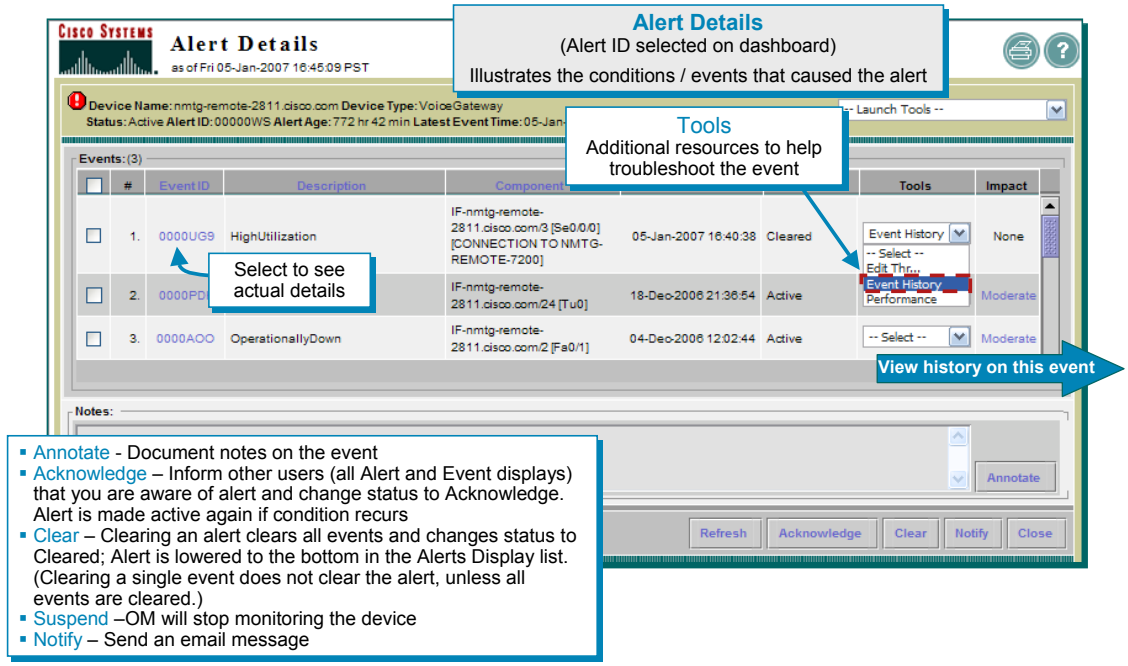
Alerts and Events - Dashboard Legend

As shown in the graphic above, the Alerts and Events display uses icons as a means of quick glance status (severity and Last Change), and as launch points for additional tools.

Note(s):

- *The diamond symbols in the **Last Change** column indicate which alerts have experienced recent activity. When no icon appears in the Last Change column, the alert is older than 45 minutes. The Status field will indicate if the alert is still active or otherwise.*

Alerts and Events Dashboard
Alert Details



Alerts and Events –Alert Details

Upon selecting the **Alert ID** in the Alerts and Events view, the event(s) which triggered an alert on the device is/are listed. The events with the most recent change are listed first.

Events remain in the Alert Details report until the parent alert expires. If you suspend the monitoring of a device, all the events are cleared, but the *alert* remains active. (This way, important information is not lost from the display, and you can easily resume monitoring of the device.)

If an event recurs, the existing event is not updated. Instead, the recurrence is shown as a new event with a new event ID.

Acknowledging an active alert signals other users that you are aware of the alert. When you click the **Acknowledge** button in the Alert Details window, this status change is populated to all Alert displays. If an event on the alert recurs, the status reverts to Active.

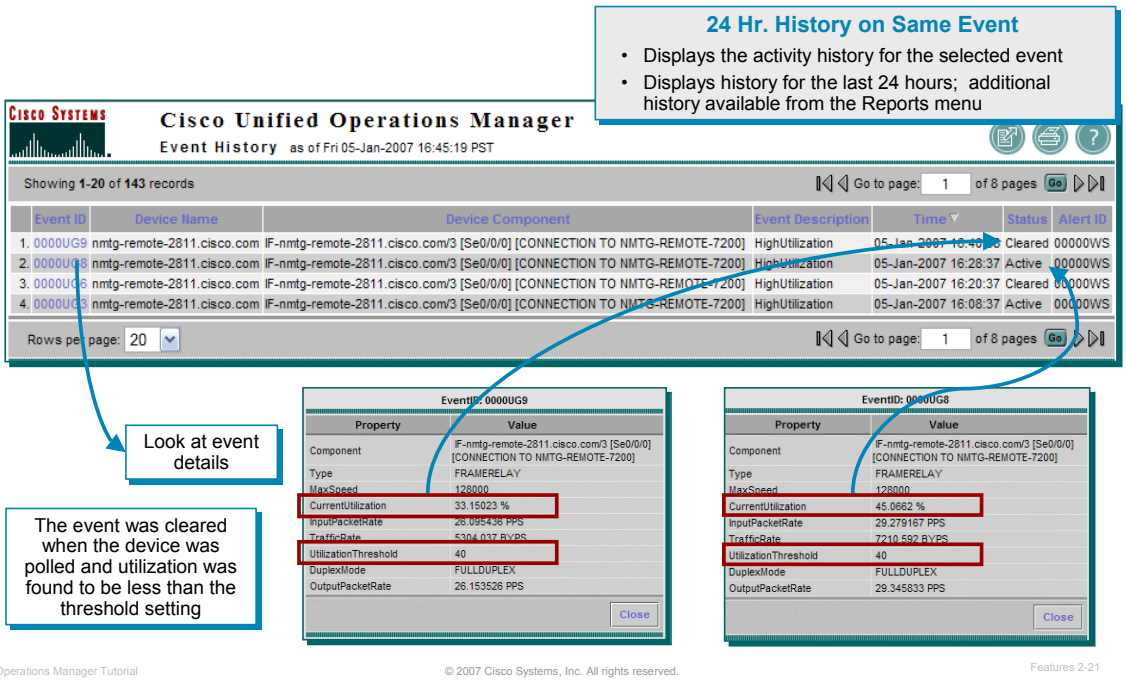
Clearing an Alert: This changes the state of the alert in the Alerts and Events display to cleared. You may want to clear an alert when you are aware of the condition or if you are receiving erroneous events and don't want to receive alerts on. When you click the **Clear** button in the Alert Details page, this status change is populated to all Alerts and Events displays. Once an Alert is cleared, the status cannot be changed back. In order to get the existing state of the device, you must manually delete and re-add the device into Operations Manager. The cleared Alert will be remove from the Alerts and Events display after Operations Manager performs its normal polling and determines that the alarm has been in the Cleared state for 30 minutes or longer (from the time of polling). If an event on the alert recurs, the status reverts to Active. *Also, clearing an alert will clear all the events associated with the alert.*

To view the details of the event, click the ***Event ID*** or go to the ***Event History*** tool to view the history of the same event over the last 24 hours and get the same details.

Note(s):

- *This report is refreshed every 30 seconds.*
- *The names of events can be changed to names that are more meaningful to you. These customized names will be reflected in both the Alerts and Events display and any Alert History reports you generate. For information on changing the event names, refer to the Event Notification section in this chapter.*

Alerts and Events Dashboard
Event History / Details



Alerts and Events – Event History / Details

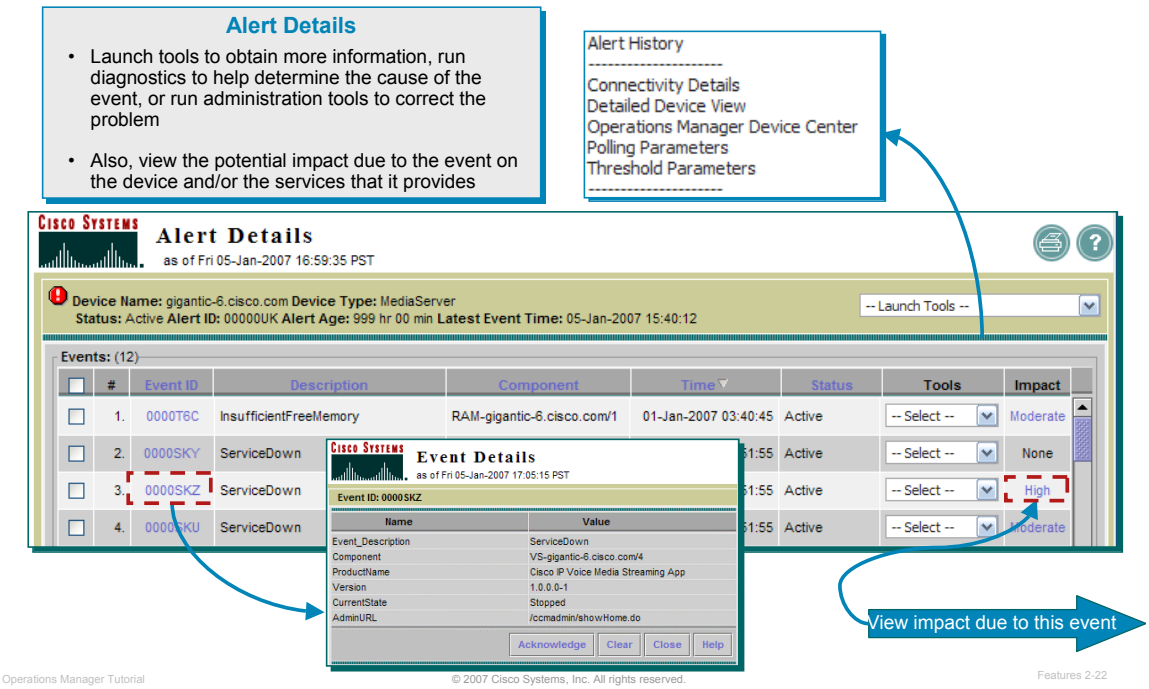
To view the details of the event, click the ***Event ID*** or go to the ***Event History*** tool to view the history of the same event over the last 24 hours and get the same details. The figure above illustrates the details of several events: first when the CCM was stopped and then a second event when the event was cleared when the CCM was polled by Operations Manager and found to be back online. All these events are tied to the same Alert ID since it is related to the same device.

Clearing an Event: Clearing an event will not clear the alert, unless this is the only event for the alert. It is not until all events for the alert are cleared, that the alert will also clear. Also, if you clear the alert on the device, the associated events will be cleared.

Note(s):

- *All Alert History reports generated from within the Alerts and Events display provide information from the past 24 hours.*
- *To generate an Alert History report on time spans beyond the last 24 hours, use Alert History from the Reports tab by selecting **Reports > Alert and Event History**. For more information, see 24-Hour Context-Based Alert and Event History Reports.*

Alerts and Events Dashboard
Launch Point for Other Tools / Reports

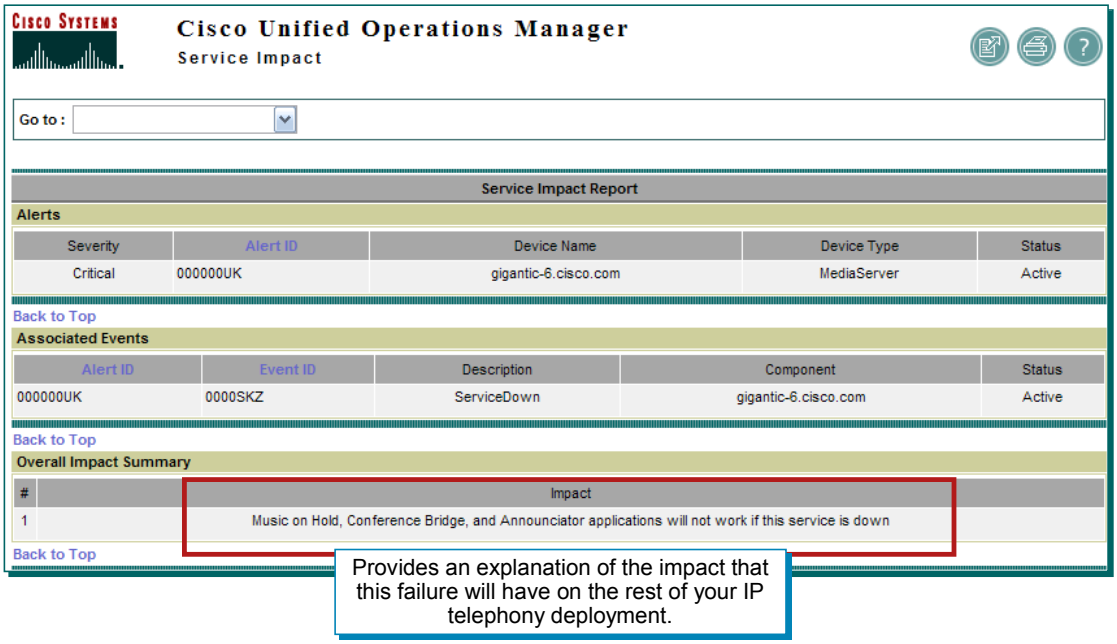


Alerts and Events –Alert Details, continue …

In addition to viewing the event details and history, you can launch other tools to obtain more information or data as to why the event was generated. The reason for the event may be easy to determine or you may need to run additional diagnostic tests. The various tools available for selection will vary depending upon the device type.

This view also provides information on the impact of the event on the device and its services that it provides. To view the impact information, click on the Impact value (i.e. High, Medium, Low).

Alerts and Events Dashboard
Impact of Event on Services Provided by Device



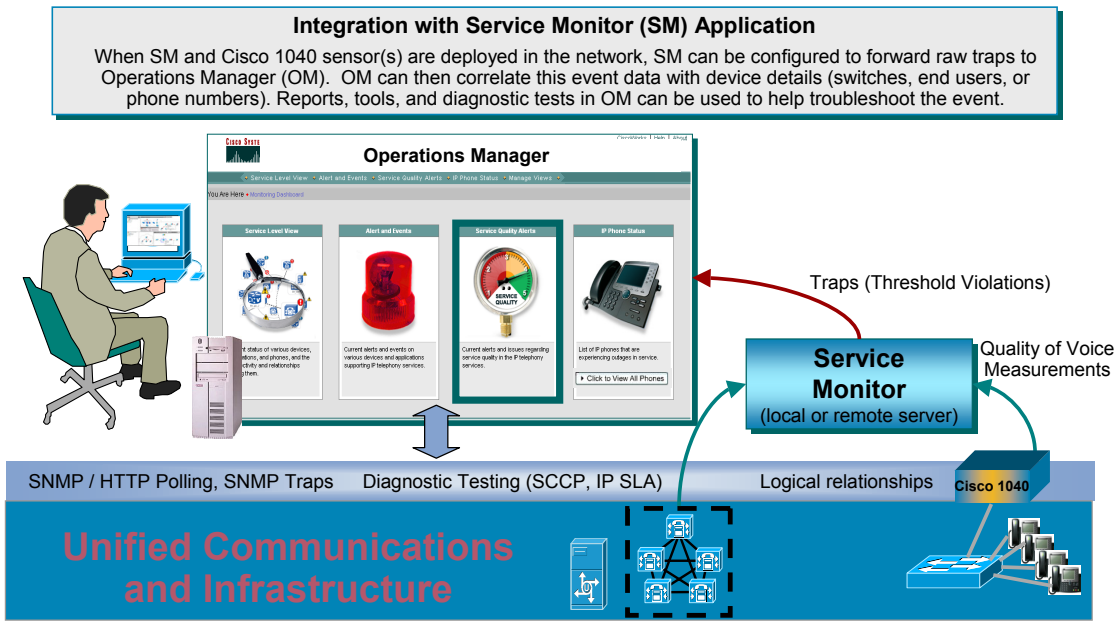
Provides an explanation of the impact that this failure will have on the rest of your IP telephony deployment.

Alerts and Events –Impact of Event on Services Provided

Cisco has established severity definitions and has also determined the impact of certain conditions occurring or exceeding pre-defined thresholds. The Service Impact Report can be used to help the network manager get more details on the event and the possible impact that it may have on the Unified Communications services.

In this example, the event is marked critical and is a result of polling the available free virtual memory on the media server. The amount of virtual memory has fallen below the specified threshold. As a result, the server may experience increased page faults and thrashing, which results in poor server performance.

Operational Status Views
Service Quality Alerts Dashboard



Service Quality Alerts Dashboard

The third (of four) Monitoring Dashboard in Operations Manager is the Service Quality Alerts View. The Service Quality Alerts dashboard will display alerts that Operations Manager has received from the Cisco Unified Service Monitor (SM) application. SM generates SNMP traps when it detects poor quality of voice measurements collected by a Cisco 1040 sensor or Cisco CallManager cluster. (CallManagers collected their measurements from gateways and phones that utilize the CVTQ algorithm.) Operations Manager will read the raw SNMP trap sent by SM, create an alert, and mark the alert with a severity level based on the quality of voice alert value.

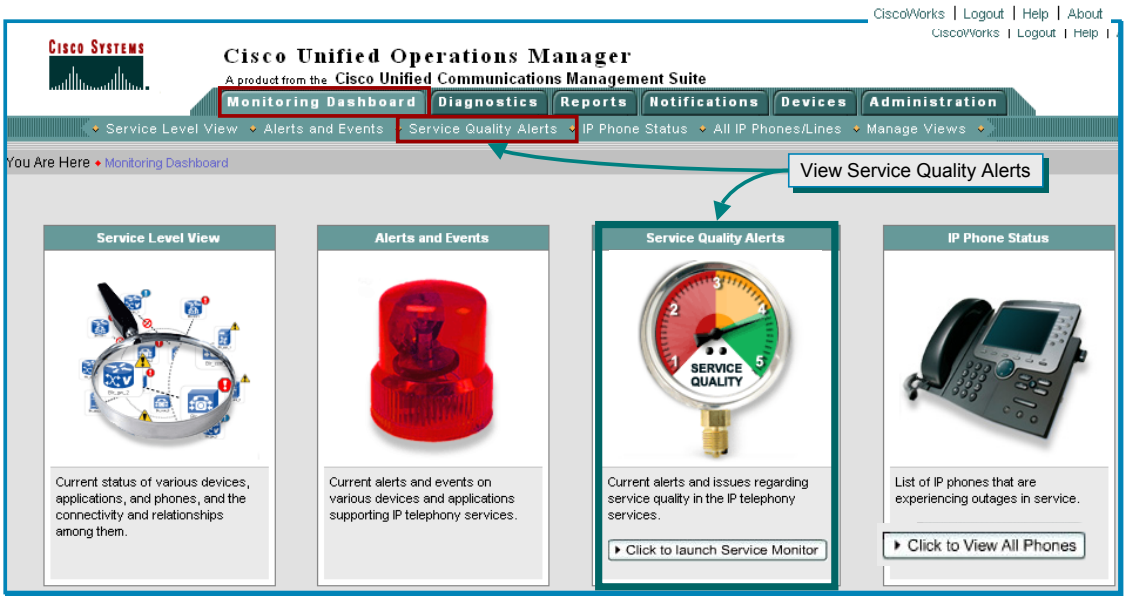
The integration of SM with OM provides the user with tremendous value. Now, instead of receiving a raw SNMP trap containing the IP addresses of the RTP call stream, the network manager can view within OM device details. OM correlates the IP addresses with the connecting switches, end users, and phone numbers of the managed device. Additionally, the network manager can use drill down reports and tools to identify the two end IP phones, determine the operational status, and run a path trace or IP SLA test.

Note(s):

- *To use the Service Quality alerts display, you must have a licensed copy of Service Monitor configured to send traps to the Operations Manager server.*
- *You must also add the Service Monitor definition to Operations Manager using the* ***Administration > Service Quality Settings > Service Monitors*** *menu option.*

Refer to the Service Monitor tutorial for more information on monitoring quality of voice.

Operational Status Views
Service Quality Alerts Dashboard



Service Quality Alerts Dashboard

The ***Service Quality Alerts*** view is accessible under the Operations Manager Monitoring Dashboard tab. Either select the menu under the Monitoring Dashboard tab or click on the ***Service Quality Alerts*** picture (*notice that the icon changes when the cursor is placed over the top of it*).

Remember that service quality alerts are only displayed in this view if the following conditions are met:

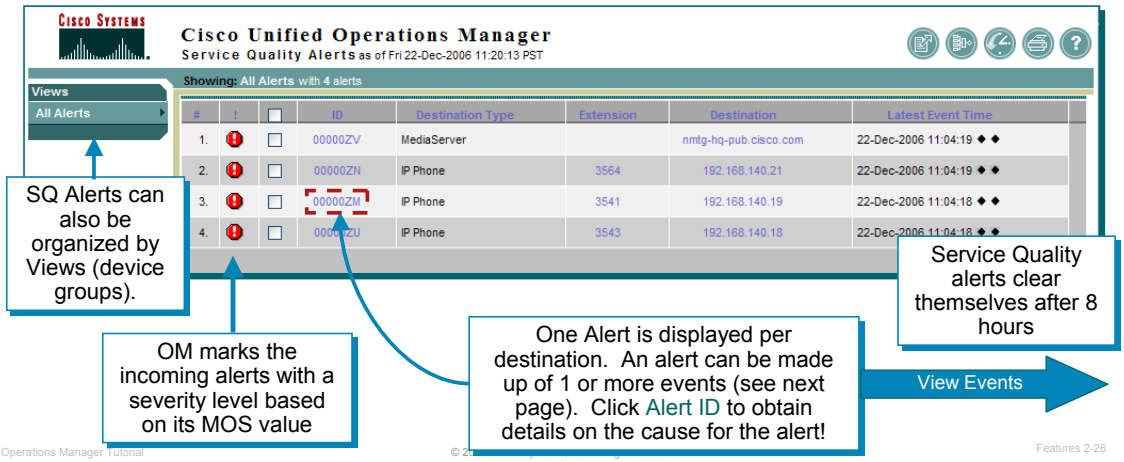
- Cisco 1040 Sensors are monitoring RTP call streams
- Cisco 1040 Sensors forward call metrics to the Service Monitor application
- Gateways or IP phones with the CVTQ (Cisco Voice Transmission Quality) algorithm are deployed and managed by Cisco CallManagers, which are managed by SM
- Service Monitor (locally or remotely installed with OM) must be configured to forward poor quality of voice alerts to Operations Manager
- The Service Monitor server information must also be defined within Operations Manager

Service Quality Alerts Dashboard
Overview

Service Quality Alert Views

Similar to the Alerts and Events View, except these alerts come from the optional Service Monitor application which gathers service quality data from the Cisco 1040 sensors and Cisco CallManager clusters

- Cisco 1040 Sensors monitor real-time RTP call streams
- Cisco CallManagers provide data collected from gateways and phones that use the Cisco Voice Transmission Quality (CVTQ) algorithm



Service Quality Alerts – Dashboard Overview

While the Cisco 1040 sensors are busy monitoring a SPAN port of a switch and analyzing each RTP data stream, it sends Mean Opinion Scores (MOS) values via Syslog messages to the Service Monitor application every 60 seconds. Service Monitor analyzes the incoming MOS values against a user-defined threshold and forwards any violations to Operations Manager.

Operations Manager is configured to listen for SNMP traps from Service Monitor. Operations Manager is also configured to mark the alerts with a Severity Level based on the value of the MOS.

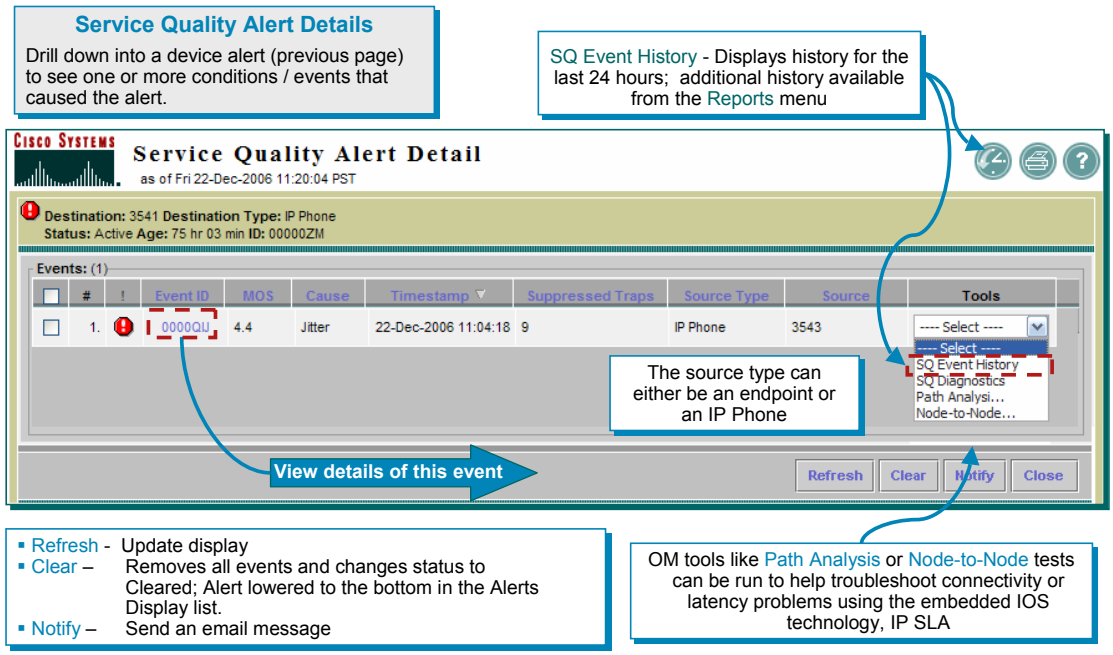
The Service Quality Alerts display in Operations Manager shows the alerts received from Service Monitor that are occurring in your current view. Alerts are grouped by their severity: critical, warning, or informational. Within these severity groupings, alerts with the latest change are listed first.

When an alert is generated, it remains in the Service Quality Alerts display until it expires. Operations Manager sets an alert state to Expired when Operations Manager determines that the alarm has been in the *Cleared* state for 30 minutes or longer (from the time of polling). While the alert is in the display, if any of its events recur, the alert is updated. If an expired alert recurs, a new alert with a new ID is shown. This display is refreshed every 30 seconds.

Note(s):

- *Service Quality alerts clear themselves after 8 hours, but are available for viewing in the historical report.*
- *You can generate a 24-hour Service Quality Event History report on all events that occurred on devices in your view by clicking the History button in the upper right-hand corner of the window.*
- *The view pane lists the currently available views, or user-defined device groups, available for Service Quality Alerts. By default, two views--All Alerts and Suspended Devices--are always shown, and cannot be deleted from your Service Quality Alerts display.*

Service Quality Alerts Dashboard
Alerts Details



Service Quality Alerts – Alert Details

Upon selecting the Alert ID in the Service Quality Alerts View, the *Service Quality Alerts Details* dashboard is displayed in a new window listing the individual service quality events that caused the alert.

From the Service Quality Alert Details window, the user can view more information including the MOS value and primary cause for that MOS value. The user also has the option to launch several Operations Manager (OM) tools to help in troubleshooting efforts.

In the example above, you can also quickly see the MOS values. The event(s) which triggered the alert on the destination IP Phone or Endpoint is/are listed. The events with the latest change are listed first. Operations Manager was configured to marked MOS values below 3.5 as critical events. These settings for Service Quality alerts can be defined under the main Operations Manager menu, **Administration > Service Quality Settings > Event Settings**.

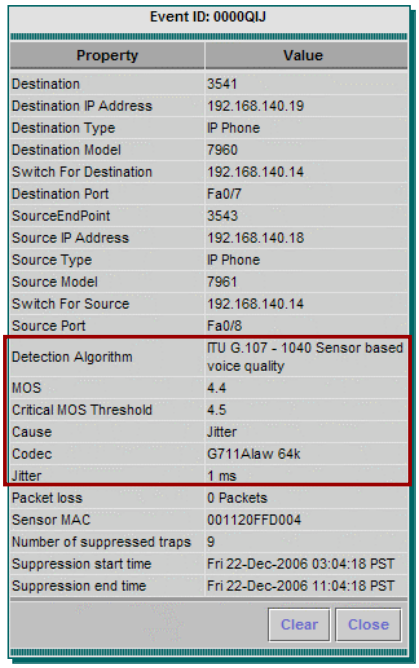
To view the details of the event, click the **Event ID** or go to the **Service Quality Alert History** tool to view the history of the same event over the last 24 hours and get the same details.

Additionally, Operations Manager tools like Path Analysis or Node-to-Node Tests can be run to help troubleshoot connectivity or latency problems using the embedded IOS technology, IP SLA. (Refer to the Diagnostics Tests features of Operations Manager for more information.)

Note(s):

- *This report is refreshed every 30 seconds.*

Service Quality Alerts Dashboard
Event Details



Service Quality Event Details

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

Service Quality Alerts – Event Details

If the **Event ID** was selected in the Alert Details window, 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 SM user-defined threshold of 3.5, and the primary cause of the low MOS was jitter which was reported at 40 msec for the 60 sec reporting period.

Operational Status Views
IP Phone Status Dashboard

IP Phone Status Dashboard

The last of the four Monitoring Dashboards in Operations Manager is the ***IP Phone Status*** view. Different from the Alerts and Events display, this Monitoring Dashboard provides instant access to IP phone outage information.

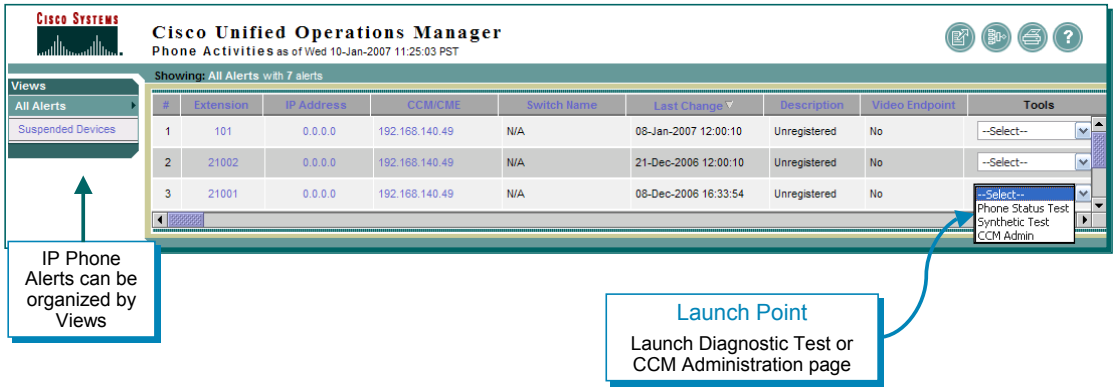
The ***Phone Activities*** view is accessible under the Operations Manager Monitoring Dashboard tab. Either select the menu under the Monitoring Dashboard tab or click on the ***IP Phone Status*** picture (*notice that the icon changes when the cursor is placed over the top of it*).

Quick access to a report on *all IP Phones* detected in the network is available by selecting "***Click to View All Phones***"; this report is illustrated in the Reports section of this chapter.

IP Phone Status Dashboard
Overview

Phone Activities Display

Contains information about the IP phones in the network that have become disconnected from the switch, are no longer registered to a Cisco CallManager, or have gone into SRST mode



IP Phone Alerts can be organized by Views

Launch Point

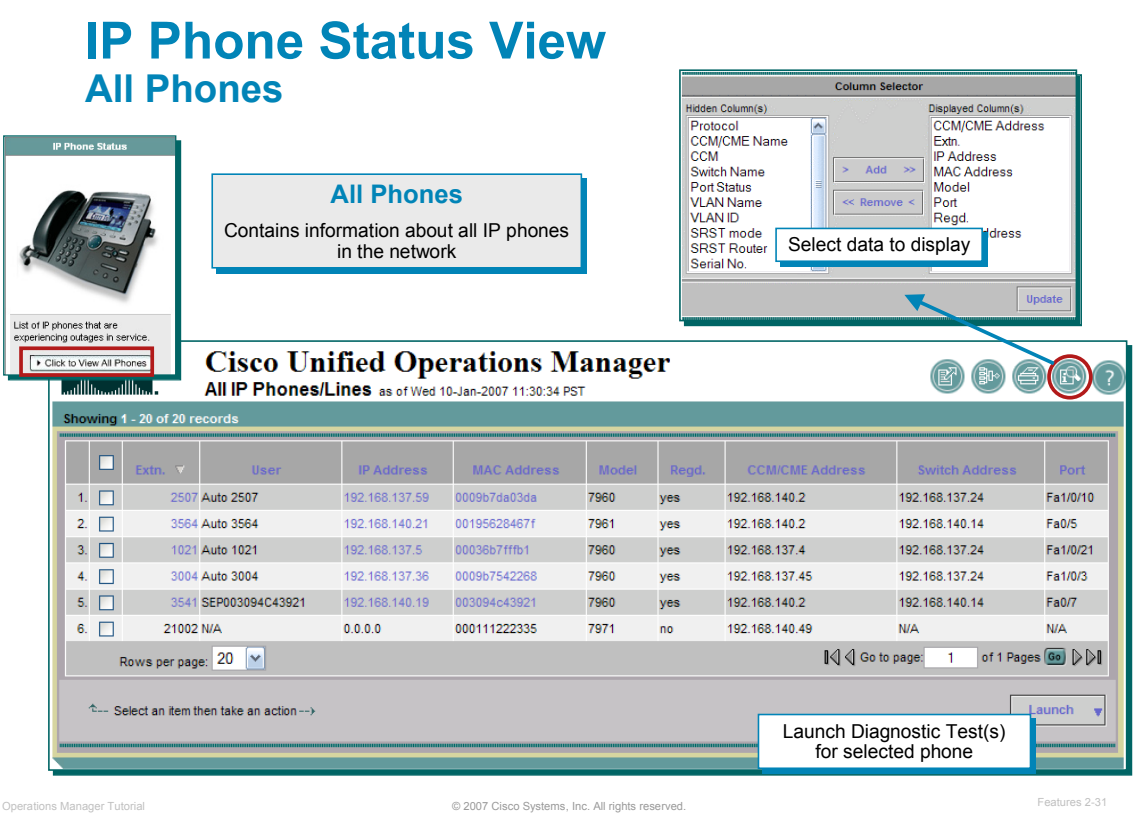
Launch Diagnostic Test or CCM Administration page

IP Phone Status – Dashboard Overview

Two types of outages are monitored: signaling-related outages and IP connectivity-related outages. It is also possible to get information about an IP phone's switch and port or launch diagnostic test or the CCM administration page, allowing administrators to troubleshoot problems that may have wider scope (at the switch level) than just the IP phone.

The Phone Activities display shows information about the IP Phones in your network that have become disconnected from the switch, are no longer registered to a Cisco CallManager, or have gone into SRST (Secure Survivable Remote Site Telephony) mode. The following events cause activity to be displayed on the Phone Activities display:

- Phone Removed
- SRST Entered
- SRST Suspected
- Suspect Phone Detected



IP Phone Status – All Phones

Quick links are available to view all IP phones associated with the managed Cisco CallManagers.

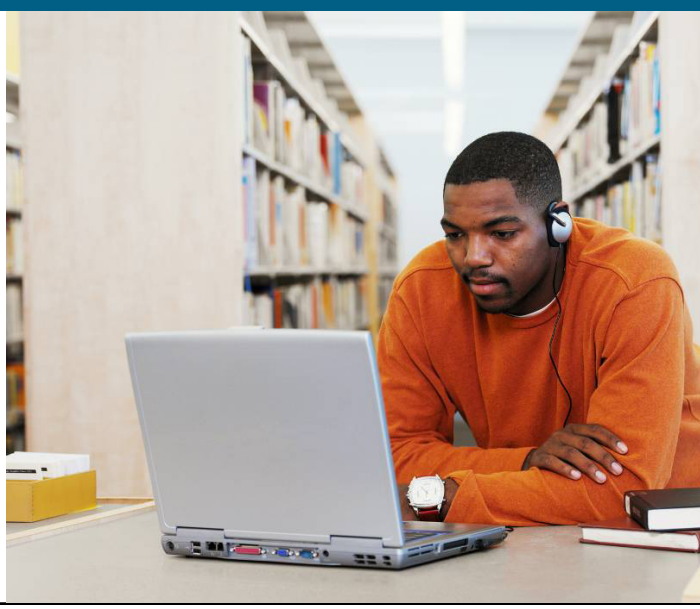
Quick access to a report on *all IP Phones* detected in the network is available by selecting the "***Click to View All Phones***" button located within the IP Phone Status View icon.

This report provides all information available for the IP phones in the network. From this report, you can launch selective diagnostic tests for selected phones.

<*Intentionally Blank*>

Diagnostic Tests

- Operational Status Views
- **Diagnostic Tests**
- Inventory Management
- Reports
- Event Notification
- Customization / Advanced Features



Diagnostic Tests
Overview

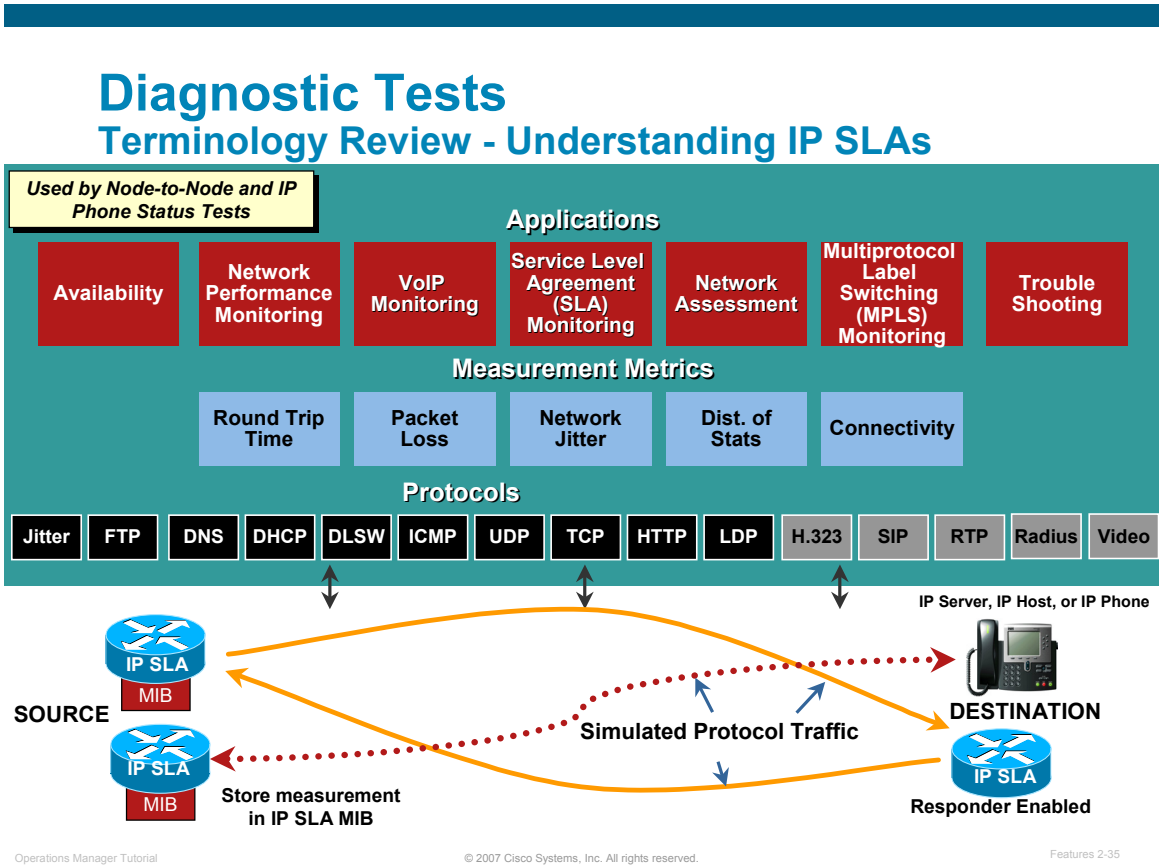
- IP Phone Status Tests
  - Use to determine the reachability of one or more phones; Test sends a ping to the IP phone from either both the OM server or just from an IP SLA-capable Cisco IOS device
- SRST (Survivable Remote Site Telephony) Tests
  - Test reachability to local SRST router; when IP Phones go into SRST mode, they rely on local SRST router for call processing
- Synthetic Tests
  - Use to test the availability of voice services; OM can simulate synthetic IP phones to request services
- Batch Tests
  - Acceptance tests, check-out tests, site inventory and status
- Node-to-Node Tests
  - Use to ensure QoS by measuring response time, latency, and jitter from a source to a destination

Diagnostic Tests - Overview

Operations Manager comes with a rich set of diagnostic tests that can be used to aid in trouble isolation and resolution. There are primarily five types of tests:

- **IP Phone Status Tests** - The IP phone status tests can be used to determine the current operational status of the IP phones in terms of signaling and IP connectivity. These tests also utilize the IP SLA feature in IOS devices to test the reachability of IP phones in the network. Users can supply a list of phones to test and configure when to run the tests (on-demand or scheduled).
- **SRST (Survivable Remote Site Telephony) Tests** – The SRST tests can be used to test the IP phones reachability to the local SRST router. When an IP phone goes into SRST mode (access to their Cisco CallManager is down), they rely on the locally configured SRST router for continued call processing.
- **Synthetic Tests** - The synthetic tests serve to replicate user activity (receiving a dial tone, making an end-to-end phone calls, leaving voice mail, and creating/joining conference calls). These tests can verify the functional availability of the supporting infrastructure and validate different configuration aspects such as route patterns, route lists, inter-cluster trunks, and gateway dial peers.
- **Batch Tests** - Batch tests can be used to test the health and connectivity of a branch office. Batch tests consist of a set of synthetic tests that are run on voice applications (for example, Cisco Unified CallManager Express or Cisco Unity Express) that are deployed in a branch office and a set of phone tests that are run on real phones (running SCCP) in the branch office.
- **Node-to-Node Tests -** The node-to-node tests use the services of IP Service Level Agreements (IP SLA) feature, formerly known as Service Assurance Agent (SAA), in Cisco IOS devices to simulate traffic in the network and then determine network characteristics such as reachability, response time, latency, jitter, packet loss, and network quality. Each of these tests can be run in a continuous monitoring mode as well as in either a scheduled or on-demand mode. The results are presented through a variety of reports.

Each of these will be discussed in more detail in the upcoming pages. But first, let's review the IP SLA feature embedded in IOS devices since it is used in both the IP phone status tests and node-to-node tests.



Terminology Review - Understanding IP SLAs

A quick overview of IP SLA is provided here since it is used in both the IP phone status tests and the node-to-node tests.

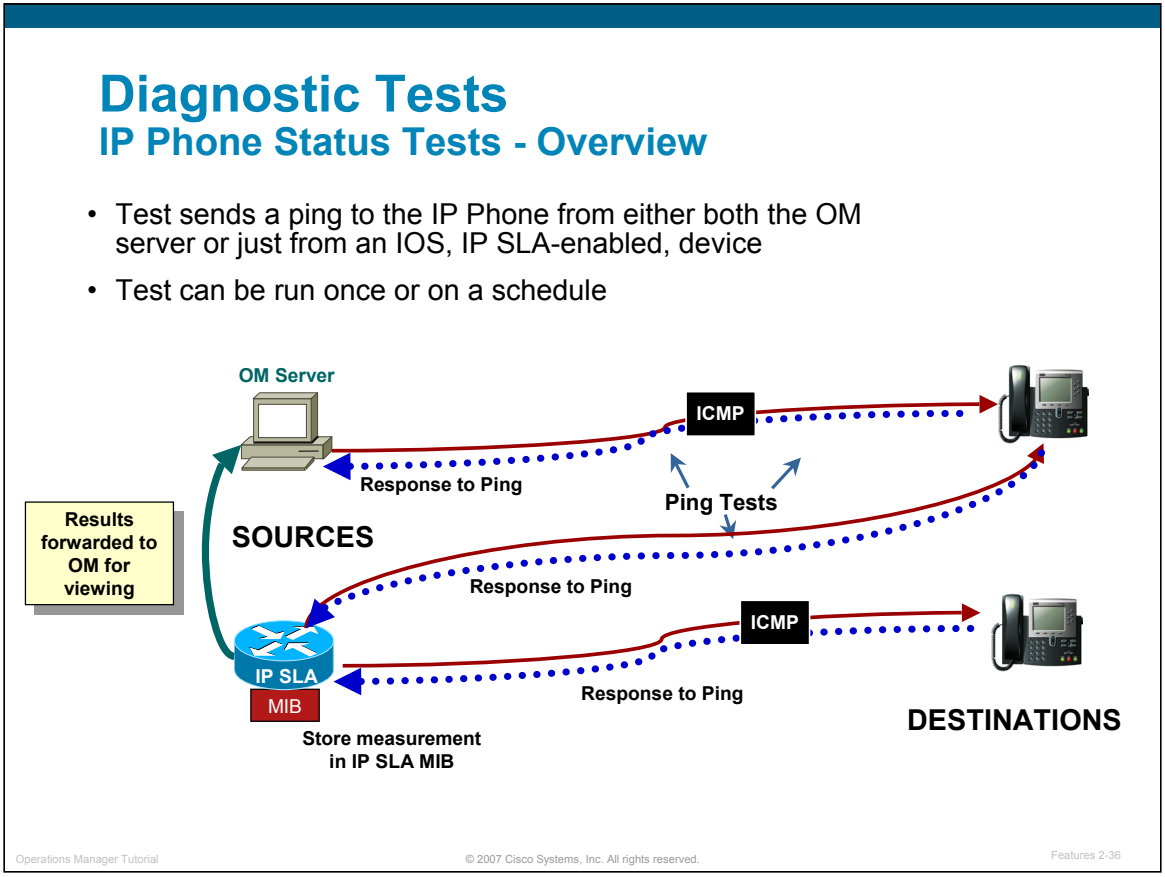
IP SLA stands for IP Service Level Agreements and is a feature in most Cisco IOS devices (see appropriate versions below). Since IP SLAs are embedded into IOS devices, there is no need to deploy other diagnostic devices into the network to run tests.

Cisco IOS IP SLA measures network performance by sending one or more simulated protocol test packets to a destination IP device or a Cisco router. Cisco IOS IP SLA uses the timestamp information to calculate performance metrics such as jitter, latency, network and server response times, packet loss, Mean Opinion Score (MOS) voice quality scores, and other network statistics. The “Source” IP SLA device generates the simulated protocol traffic and stores the test measurements in its IP SLA MIB. The results can easily be retrieved for viewing using SNMP and tools like CiscoWorks.

With IP SLAs, the user can continuously, reliably, and predictably measure network performance and proactively monitor network health or run-time diagnostic tests to aid with troubleshooting.

Note(s):

- *IP SLAs was previously known as the Response Time Reporter (RTR) and Service Assurance Agents (SAAs) in earlier IOS versions.*
- *Depending on the version of IOS, different protocols can be simulated. IP SLA v2.1 is supported in IOS version 12.0(5)T, 12.1(1), and higher. IP SLA v2.1 is supported in IOS version 12.3(4)T and higher.*
- *Configuring the IP SLA is simplified by using Cisco tools (Operations Manager or Internetwork Performance Monitor (IPM) or by using the Command Line Interface of the IP SLA device.*



Diagnostic Tests – IP Phone Status Tests

The Phone Status Test determines if an IP Phone is *reachable* using a ping test from the Operations Manager server and/or from a specified IOS device that is IP SLA-capable.

A phone status test consists of the following:

- A list of IP phones to test, selected by you.
- A testing schedule that you configure.
- IP SLA-based pings from an IP SLA-capable device (for example, a switch, a router, or a voice router) to the IP phones and, optionally, pings from the Operations Manager server to the IP phones.

The figure above illustrates two IP Phone status tests configured on an IP SLA-capable voice router, with one of the tests also having the Operations Manager server testing reachability to the destination IP Phone.

Using Operations Manager, it is easy to configure an IP SLA echo test on the IP SLA-capable IOS device, provided that the device has enough memory provisioned to allow Operations Manager to do so. The results of the test are then forwarded to the Operations Manager server for viewing. A phone is considered unreachable after no response to either an IP SLA-based ping or an Operations Manager ping, if enabled. If the IP phone is unreachable, Operations Manager generates the PhoneReachabilityTestFailed event.

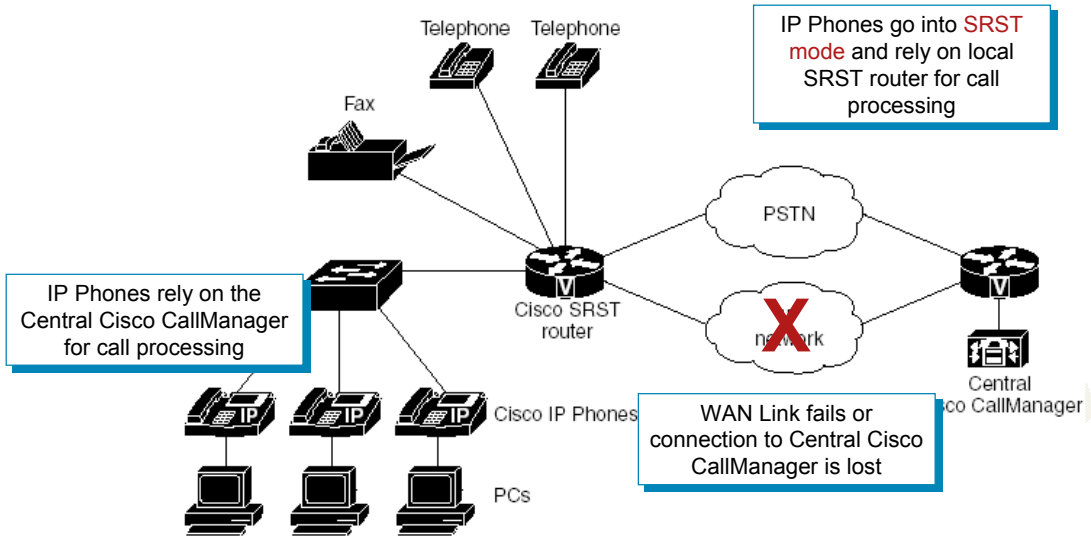
Below is an example of the IP Phone status test results. (SAA Result is the ping test from the IP-SLA device. NMS Result is the ping test from the Operations Manager server.)

Phone Status Test Results

Test Results

PhoneIP	SAA Result	NMS Ping Result	Registration Status
172.20.5.57	Passed	Passed	Unregistered
44.44.1.3	Passed	Passed	Unregistered
44.44.1.2	Passed	Passed	Unregistered

Diagnostic Tests
SRST Tests - Overview



Diagnostic Tests – SRST Tests

Remote branch offices may be configured for Survivable Remote Site Telephony (SRST) in case the Cisco Unified CallManager becomes inaccessible. A branch office normally relies on a central CallManager for call processing. If the Cisco Unified CallManager becomes inaccessible, phones can use a Cisco voice router for call processing. Phones go into SRST mode when either of the following happens:

- The WAN link to the Cisco Unified CallManager at the central site goes down
- The connection to the Cisco Unified CallManager is lost

SRST allows phones in branch offices to continue to function until the WAN link comes up or until the phones can register with a Cisco Unified CallManager again.

The SRST test runs IP SLA Jitter tests from the source router (near Central Cisco CallManager) to detect the reachability of the target SRST router (at the branch office). Use OM to configure the IP SLA test on the source router.

Diagnostic Tests
Synthetic Transactions Tests - Overview

- Tests the Availability of Voice Services
  - Cisco CallManager (CCM) and Express (CME)
  - TFTP Server
  - Cisco Emergency Response (CER)
  - Cisco Conference Connection (CCC)
  - Cisco Unity™ and Unity Express
- 7 Different Voice Application Tests
  - OM simulates a Cisco 7960 IP phone requesting services for most tests
  - Two real IP phones can be used for an end-to-end call test
- OM compares actual results against expected results
  - Skinny Client Control Protocol (SCCP)
  - TFTP server
- Events generated based on results
  - 20 second timeout is considered a test failure
  - Incorrect response

> - Do not create more than 100 end-to-end call tests that run at one-minute intervals.
> - No more than 250 synthetic tests can be defined.

Diagnostic Tests - Synthetic Transactions Tests

Synthetic Transactions are tests that can be used to measure the availability of voice applications in the network. These tests verify whether the voice application can service requests from a user, such as verifying that phones can register with a Cisco CallManager (CCM). Operations Manager supports synthetic testing for the following applications:

- Cisco CallManager and Cisco CallManager Express
- Cisco TFTP Server
- Cisco Emergency Responder
- Cisco Conference Connection
- Cisco Unity and Cisco Unity Express

Seven different synthetic transactions, within Operations Manager, can be used to create a test of voice services. Multiple tests can be configured against a single CCM. In most cases, the synthetic tests can use synthetic phones, simulated by Operations Manager, to measure the availability of voice applications by emulating your actions. For example, a synthetic test places a call between clusters and then checks to see if the call is successful. If a synthetic test fails, Operations Manager generates a critical event. Such events are displayed in the Alerts and Events display

To perform the synthetic transactions, the user configures the necessary number of simulated Cisco 7960 phones in the CCM database; however, if auto registration is enabled in CCM, this step is not necessary. Each synthetic transaction requires a unique phone number and MAC address. Using the Operations Manager graphical user interface (GUI), the user uses the simulated phones to configure the set of transactions to run for a test against the CCM. Operations Manager then acts as a simulated IP phone using the SIP or Skinny Client Control Protocol (SCCP) signaling protocols to request the voice services.

For each test, Operations Manager expects a certain response. If an unexpected response or no response (20 second timeout) is received, the test fails. A failed test could indicate that the services are down, the network is slow or mis-configured, or the transactions themselves were mis-configured.

Let's now take a closer look at the seven different types of synthetic transactions configurable with Operations Manager.

Diagnostic Tests
Synthetic Transactions Tests

Test Name	Test Description
Phone Registration	Checks if a phone can register with the CallManager
Off-Hook	Checks if a phone gets dial tone
End-to-End Call	Checks if a phone can call another phone (real or simulated)
Conference Connection	Creates a conference and connects to it
Unity Message Waiting Indicator	Checks if the message waiting indicator light goes on after a message is left
Cisco Emergency Responder (CER)	Checks if CER is able to route calls based on a 911 call
TFTP download	Checks if the phone configuration is downloadable

- *OM simulates a Cisco 7960 IP Phone requesting call services for most tests*
- *OM simulates a Cisco 7960 IP Phone calling another simulated, real, or analog phone (end-to-end call)*

Diagnostic Tests - Synthetic Transactions Tests

The synthetic tests available within Operations Manager and the results that each test must produce to pass are listed here.

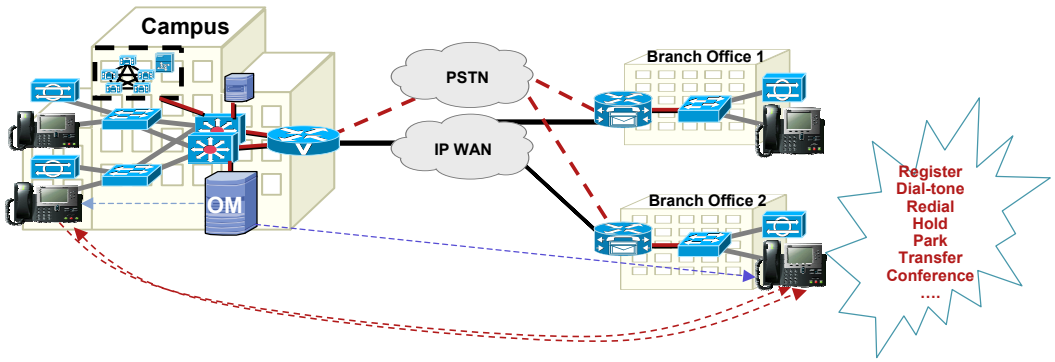
- **Phone Registration Test** - This test opens a connection with the CCM and registers a simulated IP phone. The test passes if the registration of the phone is successful.
- **Off-Hook Test** – This test simulates an off-hook state to the CCM and checks for receipt of a dial tone. The test passes if it receives a dial tone signal from the CCM.
- **End-to-End Call Test** – This test initiates a call to a second simulated or real IP phone. The test passes if it registers, goes off-hook, and places the call; and there is a ring indication; and the destination phone goes off-hook to accept the call.

  Note: If *call progress tones* and *announcements* are configured on the gateway for your end-to-end call, the test may succeed even before the phone rings or after a couple of rings. This indicates that your gateway is working correctly.
- **Cisco Conference Connection Test** – This test creates a conference (meeting) in the Conference Center and connects to the meeting. This test passes if a conference is created with the specified meeting ID and the call is initiated; and the first person and second person (if configured) successfully connects to the conference.
- **Message Waiting Indicator Test** – This test calls the target phone and leaves a voice message in the voice mail box. This test passes if there is activation of the phone's message waiting indicator. The message is then deleted and the message waiting indicator is deactivated.
- **Emergency Call Test** – This test initiates a call to the emergency number to test the dynamic routing of emergency calls. This test passes if all calls initiated and if a ring indication on Public Safety Answering Point (PSAP) and On Site Alert Number (OSAN), if configured.
- **TFTP Download Test** – This test performs a TFTP get-file operation on the TFTP server. The test passes if it successfully downloads a configuration file from the TFTP server.

Note: The phones in all of these synthetic tests, except for Phone Registration, remain registered with the CCM unless there is a failure.

Diagnostic Tests
Batch Tests Overview

- Batch tests enable you to test the health and connectivity of a branch office using multiple synthetic tests and IP phone tests defined in an XML file
- Comprehensive phone-to-phone tests: End-to-End calls (remote site, PSTN, DID), Phone registration, Off-hook, Conference, Hold, Park, Transfer…
- Dial plan tests: Verify class of restriction and gateway availability
- Acceptance tests, check-out tests, site inventory, and status



Diagnostic Tests – Batch Tests

Batch tests provide a means to test the health and connectivity of a branch office. Batch tests consist of a set of synthetic tests (previously discussed) that are run on voice applications (for example, Cisco Unified CallManager Express or Cisco Unity Express) that are deployed in a branch office and a set of phone tests that are run on real SCCP IP phones in the branch office. Batch tests can be run once a day to verify the health of the voice network in the branch office.

Create Batch Tests to conduct:

- Comprehensive phone-to-phone tests such as: End-to-End calls (remote site, PSTN, DID), Phone registration, Off-hook, Conference, Hold, Park, Transfer, etc.
- Dial plan tests: Verify class of restriction and gateway availability
- Acceptance tests, check-out tests, site inventory, and status

Diagnostic Tests
Node-to-Node Tests - Overview

- Tests the UC Infrastructure for QoS
- Use Node-to-Node tests to ensure Quality-of-Service (QoS) for the end users
- Evaluate protocol response times, network latency, and jitter
  - Response times are the most direct measurement of the user's experience
  - Latency is the delay that components in a path add to the overall response time
  - Jitter is the amount of variance in interpacket delay of voice packets

Up to 250 Node-to-Node tests can exist at a time

Diagnostic Tests - Node-to-Node Tests

Node-To-Node tests monitor the response time and availability of multi-protocol networks on both an end-to-end and a hop-by-hop basis.

After collecting this data you can use the graphing function in Operations Manager to examine changes in network performance metrics in real time.

The next few pages look at the different Node-to-Node tests available in Operations Manager. Node-To-Node tests can be created one at a time, or imported from a file to add more than one test at a time. Up to 64 Node-To-Node tests can exist at a time.

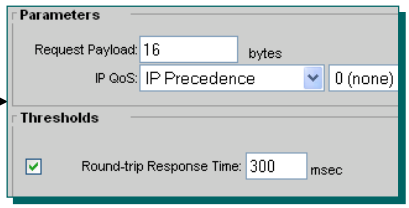
Below is a table that specifies the appropriate IOS version and IP SLA version that supports these tests.

Test	Required Versions	
	IP SLA	Cisco IOS
Ping Echo	2.1.0 and higher	12.0(5)T, 12.1(1), and higher
Ping Path Echo		
UDP Echo		
Data Jitter **Note:** Without ICPIF/MOS values.		
Data Jitter **Note:** With ICPIF/MOS values.	2.2.0 and higher	12.3(4)T and higher
Gatekeeper Registration Delay		12.3(14)T and higher
VoIP Post Dial Delay		

Diagnostic Tests
Node-to-Node Tests

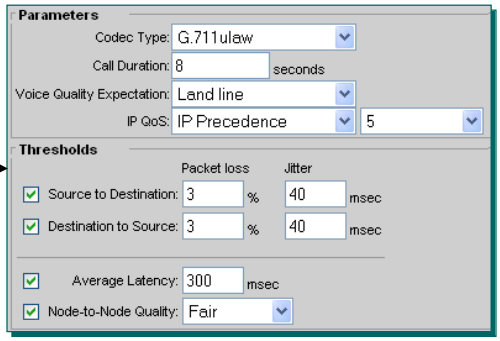
UDP Echo Tests

- Measure round-trip response time between source and endpoint (UDP Server) using a specified UDP port
- Specify test traffic's payload size and priority (IP Precedence or DSCP value)
- Optionally use an IP SLA-capable device (with the responder enabled) as the destination device to remove processing delay at the destination



Data Jitter Tests

- Measures the variance of the delay (jitter) of the UDP test packets, packet loss, and round-trip latency statistics
- Requires an IP SLA-capable device (with the responder enabled) as the destination device



Note: With an IP SLA device as the test endpoint, the IP SLA responder can improve accuracy of the test by responding to IP SLA packets, and use user-defined UDP/TCP ports

Node-to-Node Test Descriptions

Let's look closer at some of the available node-to-node diagnostic tests.

UDP Echo Tests

This test measures UDP server latency. The UDP echo test sends a packet with the configured number of bytes to the destination with the specified port number and measures the response time. The user can specify the payload size of the test and the priority of the test packets using IP Precedence or DSCP (Differentiated Services Code Point) values.

There are two destination device types for the UDP Echo operation: RTR Responders, which use IP SLA, and UDP servers, which do not. If the destination is a Cisco router, the user has an option to enable the IP SLA responder in the destination router. The responder would either listen to the default UDP echo port or to the port that the user specifies. Using the IP SLA responder feature can increase accuracy as the process delay in the destination router is assessed.

UDP Data Jitter Tests

With the addition of real-time traffic like voice traffic over IP networks, the focus shifts not just in the reliability of the network, but also on the delays involved in transmitting the data. Real-time traffic is delay sensitive. In the case of voice data, packet loss up to some extent is manageable, but frequent losses impair communication between endpoints.

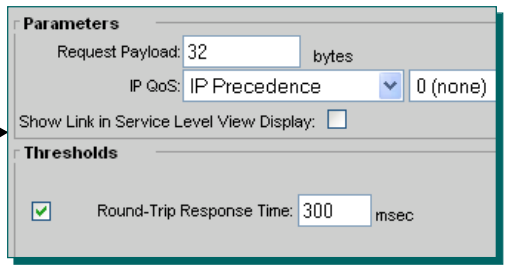
The UDP Jitter operation was designed to measure the delay, delay variance and packet loss in IP networks by generating UDP test traffic. The Jitter operation sends N packets, each of size S, from source device to a destination router (which requires IP SLAs responder enabled) each T milliseconds apart. All these parameters are user configurable. In Cisco's encoding implementation, if G.729 CODEC is used, then frames are generated every 10 ms and an RTP payload size of 10 bytes. Cisco gateway combines two such frames and transmits them every 20ms. So, the Jitter operation defaults values are set to these values to simulate voice traffic. By default 10 packets are sent for each operation.

The packets sent out to measure Jitter carry packet sequence (sending sequence and receiving sequence) information, as well as sending and receiving timestamps from the source and the responder. Based on this information, Jitter operation is capable of measuring: per-direction inter-packet delay variance (jitter), per-direction packet-loss, average round trip time, and one-way delay.

Diagnostic Tests
Node-to-Node Tests, (Cont.)

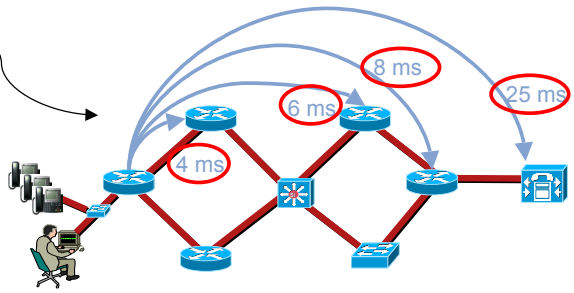
ICMP Ping Echo Tests

- Measure end-to-end round-trip response time – time to send ICMP request and receive ICMP reply; able to specify path using LSR option
- Generate tests to any IP address; Does not require IP SLAs Responder



ICMP Ping Path Echo Tests

- For each possible path, measure hop-by-hop response time between source device and any IP device
- Discovers the paths using traceroute and then measures response time between source device and each hop in the path



Node-to-Node Test Descriptions, continue …

ICMP Echo Tests

The ICMP Echo operation measures end-to-end response time between a Cisco router and any IP-enabled device. Response time is computed by measuring the time taken between sending an ICMP echo request message to the destination and receiving an ICMP echo reply. The test operation provides an option to compute response time on a specific path with LSR option in IP packet.

If there are multiple equal cost routes between source and destination devices, Echo operation has the capability to identify a specific path by using LSR option (if enabled on intermediate devices). This feature enables IP SLAs to discover paths more accurately, as compared to a typical traceroute.

Additionally, the tests also allow a user to measure Quality of Service (QoS) between endpoints by setting IP Precedence or DSCP bits on an IP packet.

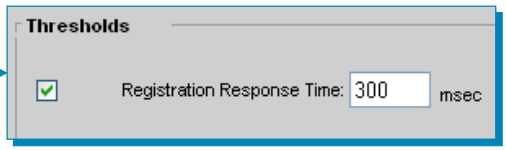
ICMP Path Echo Tests

The ICMP Path Echo operation computes hop-by-hop response time between a Cisco router and an IP device on the network. It discovers the path using traceroute and then measures response time between the source device and each intermittent hop in the path.

Diagnostic Tests
Node-to-Node Tests, (Cont.)

Gatekeeper Registration Delay

– Measure the response time required for a gateway to register with a gatekeeper



Note: The source gateway must have SIP or H323 configured on it.

Node-to-Node Test Descriptions, continue …

Gatekeeper Registration Delay Tests

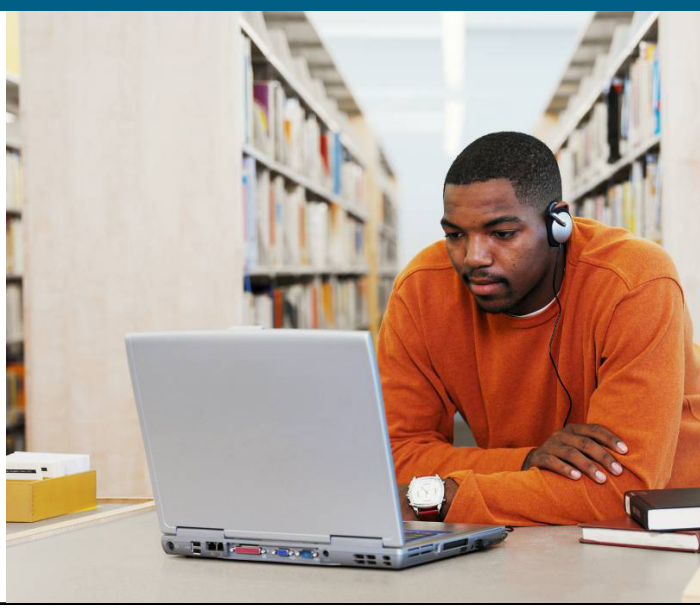
This test measures the time required for a gateway to register with a gatekeeper. The test sends a lightweight Registration Request (RRQ) from an H.323 gateway to an H.323 gatekeeper and receives a Registration Confirmation (RCF) from the gatekeeper. The test then measures the response time.

Note(s):

- *For the Gatekeeper Registration Delay test to run, the source gateway must have SIP or H323 configured on it.*

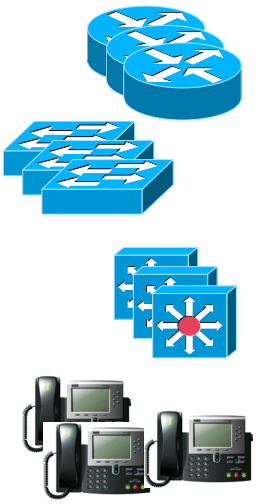
Inventory Management

- Operational Status Views
- Diagnostic Tests
- **Inventory Management**
- Reports
- Event Notification
- Customization / Advanced Features



Inventory Management
Overview

- Device Management Features
  - ☑ Populate the OM Inventory so that the devices can be managed by Operations Manager
  - ☑ Manage device credentials (username, passwords, etc.)
  - ☑ Schedule the inventory collection
  - ☑ Group devices for easier task execution
  - ☑ Generate Reports
- IP Phone Management Features
  - ☑ Generate Reports



Inventory Management - Overview

All network management products have one common configuration required before any management task can commence - configuring the tool to tell it which devices it needs to manage. The CiscoWorks solutions are not just one tool, but a collection of tools; all needing to be told which devices to manage. The adding of devices to a tool along with any necessary credentials (passwords, SNMP strings) can be a time consuming process. Fortunately, rather than perform this task for each CiscoWorks application, the CiscoWorks Common Services software provides a centralized Device and Credentials Repository (DCR) that each application can then pull the desired subset of devices and credentials from in which to manage. This assists in the maintenance of the tools – for example, if a device credential is changed, rather than updating a number of tools, only the DCR needs to be updated ensuring that all CiscoWorks applications are using the most up-to-date information.

For Operations Manager to monitor a device, you must first add the device to the DCR). Once a device is added to the DCR, you can then add it to the OM inventory, which is separate from the DCR, so that it can be managed. Once the devices are in the OM inventory, you can then schedule the Operations Manager monitoring collection.

CiscoWorks tasks are often run against a set of devices. Selecting the desired devices from a list of possibly thousands of devices could be time consuming and frustrating. Therefore, devices can be grouped using rules based on device attributes. Now, a group can simply be selected as the input for a task, saving time. As you will see, each CiscoWorks application has a number of pre-defined System Groups and a user can also create their own groups. These groups can be shared between applications.

And finally, Inventory Management does not only support the management of routers, switches, media servers, and gateways, but it also includes the endpoints, such as the IP phones connected to these devices.

Inventory Management
Understanding Device Credentials

- Device credentials are needed to allow Operations Manager to gather details / data from the devices
- Device credentials include:
  - Device properties (Hostname, IP address, Cluster)
  - Telnet / Enable / Rx-Boot mode / Auto Update server username and passwords
  - SNMP v1, v2, or v3 settings
  - HTTP / HTTPS settings
  - WMI (Windows Management Instrumentation) Credentials - MCS-based application servers only (I.e. Cisco Unified Contact Center and Cisco Unity)
  - User defined fields
- Device credentials are maintained in Cisco Works Common Services DCR (Device Credential Repository)
  - Operations Manager runs on the Cisco Works Common Services (CS) v3.0.5;
  - CS provides background services for communications, security, scheduling, etc.
- Devices can be added to Operations Manager using:
  - Automatic device discovery / Manual device addition / Import
  - Synchronize with other DCRs in the network

Inventory Management – Understanding Device Credentials

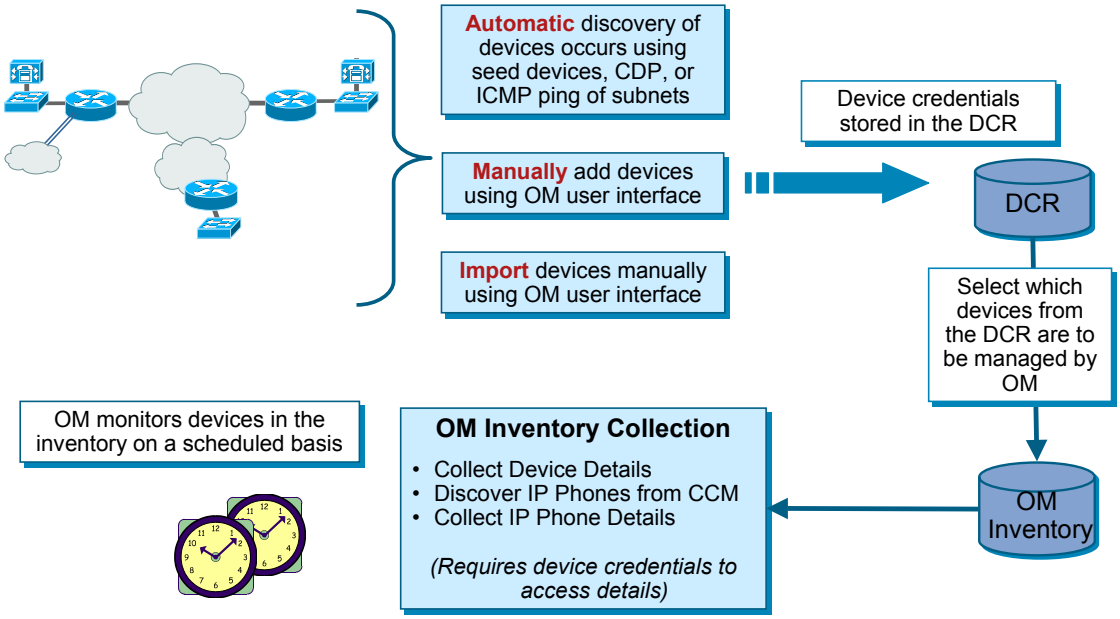
Device credentials are needed to allow Operations Manager to gather details / data from the devices. These credentials include information, such as:

- Device properties (Hostname, IP address, Cluster)
- Telnet / Enable / Rx-Boot mode / Auto Update server username and passwords
- SNMP v1, v2, or v3 settings
- HTTP / HTTPS settings
- WMI (Windows Management Instrumentation) credentials
- And optional user-defined fields

Operations Manager (OM) actually maintains two databases of device information: the Device and Credentials Repository (DCR) and the Operations Manager Inventory. The DCR provides a common database of devices and their access credentials for all installed Common Services based applications. This greatly simplifies the updating of devices and their credentials when used by more than one application. The Operations Manager Inventory is the collection of devices actually being managed by OM. It is a user-defined subset of the devices in the DCR.

Therefore, the first step is to populate the DCR, followed by selecting the devices in the DCR which should be added to the OM Inventory for management by OM. Devices can be added to the DCR in the following ways:

- Automatically through discovery using CDP information and SNMP queries or ICMP pings
- Manually - user provides device information
- Imported from a file or NMS system



Populating the OM Inventory

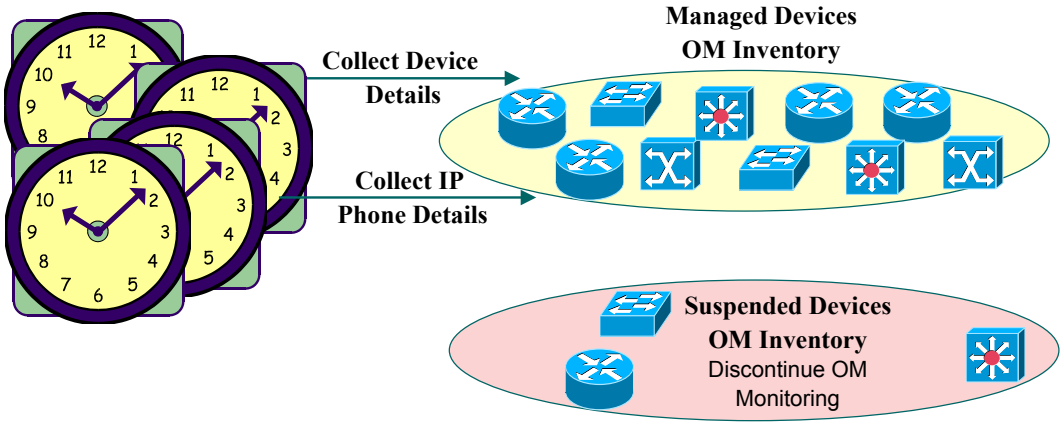
The administrator can select which devices are to be added to the OM Inventory for management. So when the DCR is populated, the OM inventory can be populated with the selected devices. The Inventory Collection process then accesses each device using the access credentials from the DCR to collect the management information needed. The administrator can schedule the inventory collection to reoccur on a periodic basis to keep the information up-to-date.

This entire process of inventory or device management is depicted above. Briefly summarizing, the device credential must be populated in the DCR either by discovery, manual add, or by importing them. Once in the DCR, the devices that the network manager wants to be managed by OM needed to be added to the OM inventory. Either all the devices from the DCR can be managed or the user can selected them. Once in the OM inventory, the collection schedules are defined and OM monitors these managed devices.

Inventory Management
Scheduling Inventory Collection

User can specify how often to collection information about the devices that are managed in the OM Inventory

- ☑ Specify how often to collect Device Details
- ☑ Specify how often to collect IP Phone Details



Scheduling Inventory Collection

Operations Manager collects data from monitored devices and updates the information about the devices themselves and the phones registered with managed devices. With Operations Manager, you can schedule inventory collection of devices and phones, configure Simple Network Management Protocol (SNMP) parameters, and access parameters for Lightweight Directory Access Protocol (LDAP) servers for obtaining assigned user names to IP Phones.

The collection of information is performed for all devices in the OM inventory. If at some point you do not want a device monitored, but still want to keep the device in the inventory, the device can be suspended from monitoring. A separate View is available for all suspended devices. As you see next, other views or device groups can be configured.

Inventory Management
Grouping of Devices for Easier Management

- View is a Logical Grouping of Devices or Device Group - Use to simplify the selection of devices for various operations and reports
- System (predefined) Device Groups
  - Pre-defined collection of devices (i.e. MDF device types)
  - Operations Manager has predefined System Groups related to Unified Communications components (I.e. Cisco CallManagers, Gatekeepers, 78xx Media Servers, IP SLA devices, and more)
- User Defined Device Groups
  - Membership based on set of rules or criteria
  - Membership can be Static (manually changed only) or Dynamic (automatically changed when membership rules are applied)
  - Groups can be Private (available to creator only) or Public (usable by all)

Grouping of Devices for Easier Management

Many Operations Manger (OM) tasks are executed against a set of devices. When thousands of devices are being managed, selecting specific devices for the task could be difficult. For instance, a thousand devices are being managed and a detailed hardware report needs to be run for only the 78xx Media Servers.

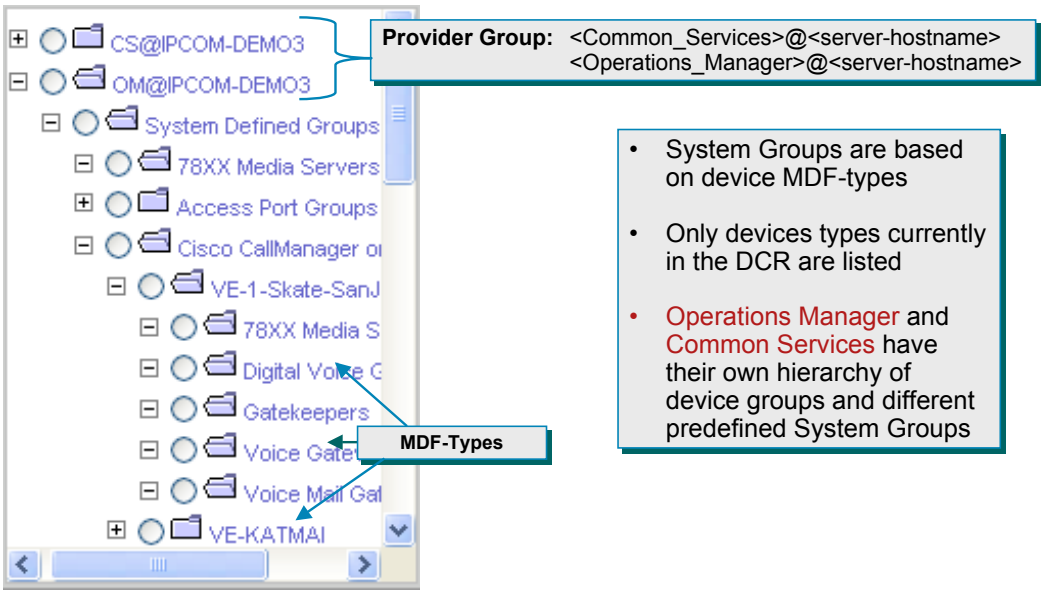
OM uses the concepts of groups to simplify the selection of devices. OM has several default grouping that categorize devices by MDF-types in a hierarchical manner (CCM Cluster > 78xx Media Server, Digital Voice Gateways, Gatekeepers, Voice Gateways, and Voice Mail Gateways). (MDF-type is the normative name for the device type as described in Cisco's Meta Data Framework (MDF) database.

Users can create their own groups, too. These groups are created using a set of rules and can be configured to automatically populate based on adherence to the group rules or only with user intervention basically making for dynamic and static groups. Further, groups can be limited to only the creator of the group (private), or for use by all (public).

This powerful feature further simplifies the use of OM if meaningful groups are created. As previously mentioned, each device has 4 (or more) user fields associated with it (stored in the DCR) that can be used to help define groups. For example, User Field 1 could be assigned to device location. Then, a device group could be dynamically created based on the value of the location user field. Tasks can then be executed for devices belonging to a specific location.

When selecting devices for a task, these system-defined or user-defined groups can be used. A device can belong to multiple groups depending upon the definition of the group.

Inventory Management
Grouping of Devices – System Groups



Grouping of Devices - System Groups

Both Common Services and Operations Manager have their own System Groups that are populated as devices are added to the DCR or OM Inventory. In the case of Common Services, the system groups are based on device types: Routers, Switches, Hubs, Gateways, etc. In the case of Operations Manager, the system groups are based on Unified Communications capabilities: 78xx Media Server, Cisco CallManager, MGCP Gateway, IP SLA device, etc.

Illustrated above is an example of the system defined groups created by Operations Manager (OM).

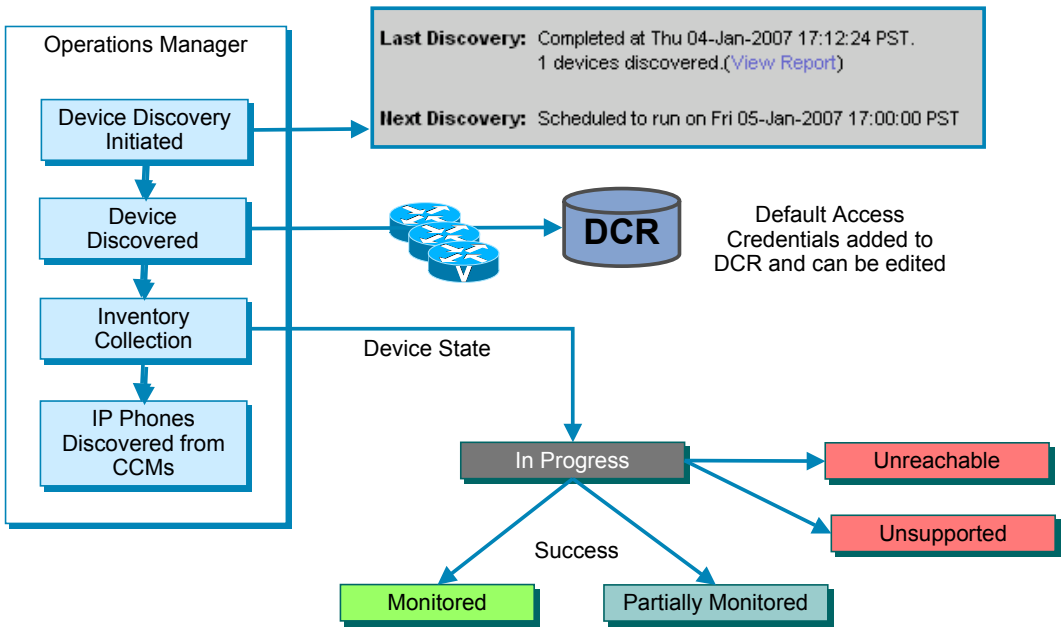
Tip:

When using Operations Manager and selecting devices, use the defined groups under OM@<server_name> to easily select devices by Unified Communications capability. Use the defined groups under CS@<server_name> to select devices when they are simply plain routers and do not have any Unified Communications services.

Note(s):

- *Groups defined by any application are available for use by other applications.*
- *A device based system group will only be listed if a device of that type has been added to the DCR.*
- *These pre-defined groups come under the Provider Group (or the root group), which, by default, is of the format Application@server-hostname.*
- *A Provider Group will exists for each CiscoWorks application installed and is the parent for all the groups defined for a particular application.*

Inventory Management
Device Management Status



Device Management Status

Once the discovery process is started in OM or the scheduled discovery time occurs, the above discovery process is started.

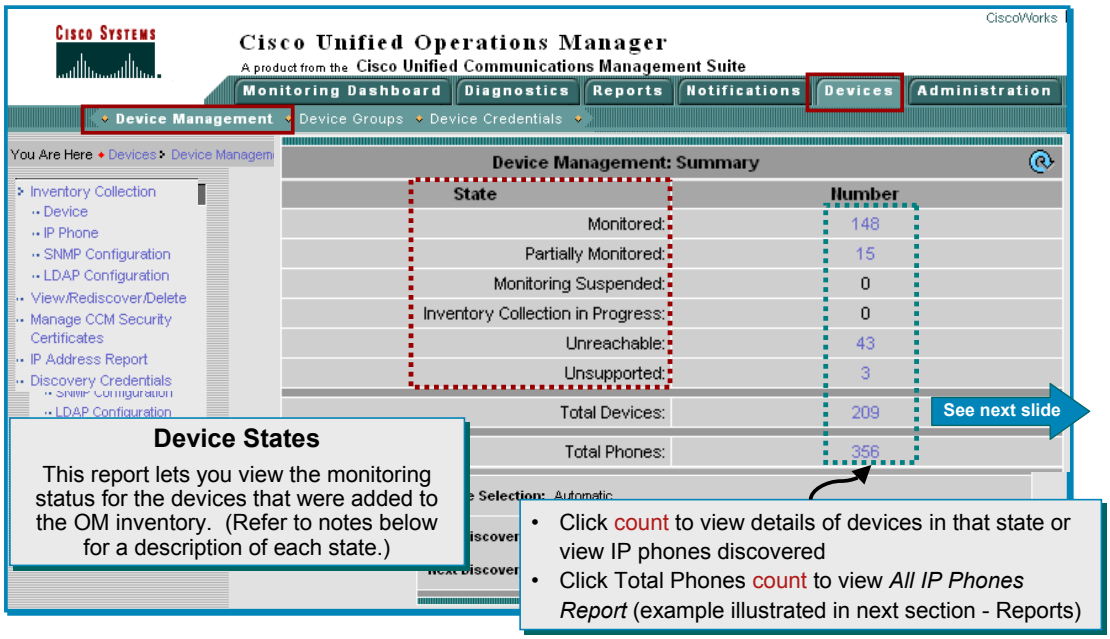
As a device is discovered, either using the CDP information or detected using ping sweep, it is entered into the DCR along with the default discovery credentials.

Following the discovery of devices, information about the devices is collected. This is called Inventory Collection. Here, attributes about the device is collected using SNMP or HTTP. Collecting this information requires access credentials (stored in the DCR), such as SNMP community strings, SNMP v3 user name/password, or HTTP user name/password.

If the device is supported by Operations Manager and reachable using the access credentials, then the Inventory Collection is successful. The device state is reported as Monitored if all information is collected using the known access credentials. The device state may be reported as Partially Monitored if some information could not be retrieved using the known access credentials. For example, information about a Cisco CallManager requires the access credentials (user name / password) for HTTP and it may not have been specified; therefore, only the information that was retrieved using SNMP can be obtained; thus, Partially Monitored.

The Device Management: Summary page, illustrated next, lists the device states for all devices in the OM inventory and the number of devices that are in each device state.

Inventory Management
Status Reports

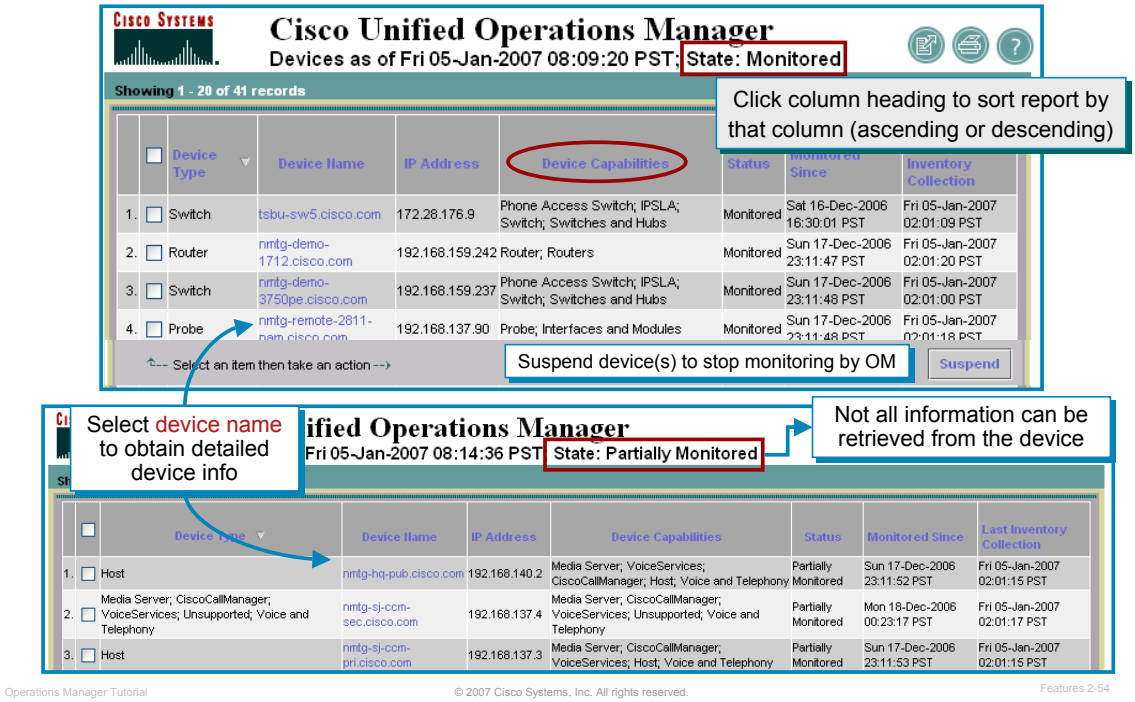


Status Reports

The Device Management: Summary page lists the device states for all devices in the OM inventory and the number of devices that are in each device state. Below are the different possibilities:

Monitored	The device has been successfully imported, and is fully managed by Operations Manager
Partially Monitored	The Cisco CallManager has been successfully imported by some of the data collectors in Operations Manager (i.e. SNMP), but not all; If a device is in this state, you should check HTTP credentials to ensure that the device becomes monitored
Monitoring Suspended	Monitoring of the device is suspended
Inventory Collection in Progress	Operations Manager is probing the device; This is the beginning state, when the device is first added; a device is also in this state during periodic inventory collection; Some of the data collectors may still be gathering device information
Unreachable	Operations Manager cannot manage the device; Could be because the device can't be pinged, SNMP service is not turned on, or the RO community provided by the user is incorrect
Unsupported	The device is not supported by Operations Manager

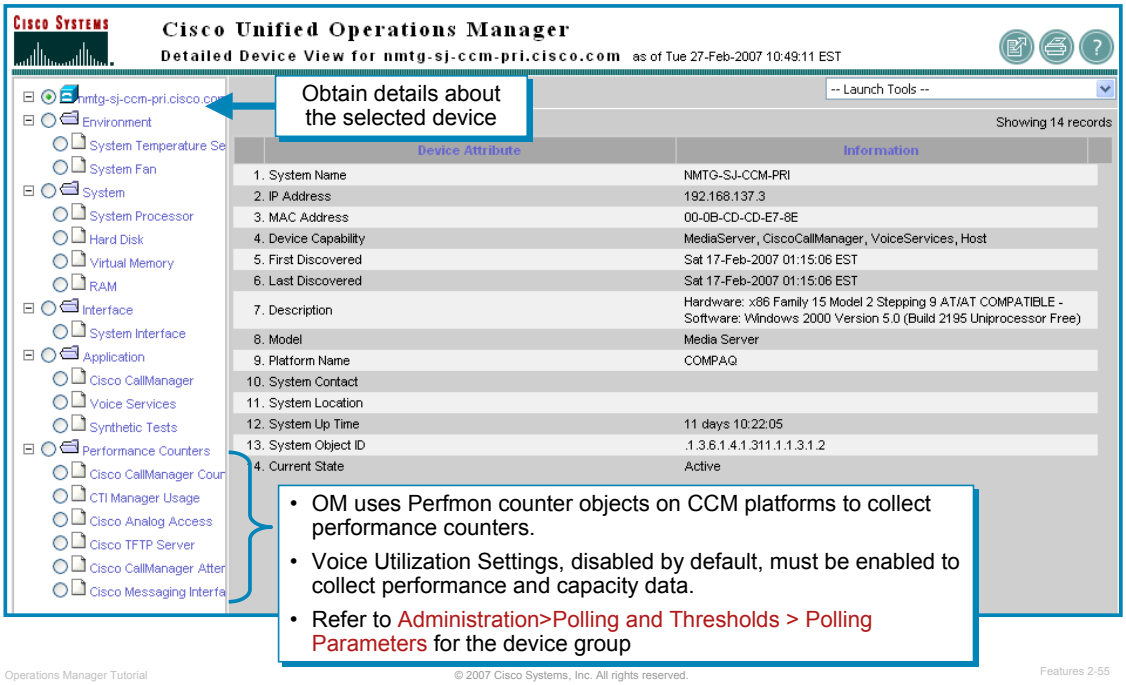
Inventory Management
Device Report (Available Per State)



Device Report

The Device Report lists the device details for the devices in the state that was selected. The report above (State: “All”) is displayed when the count for the **Total Devices** is selected.

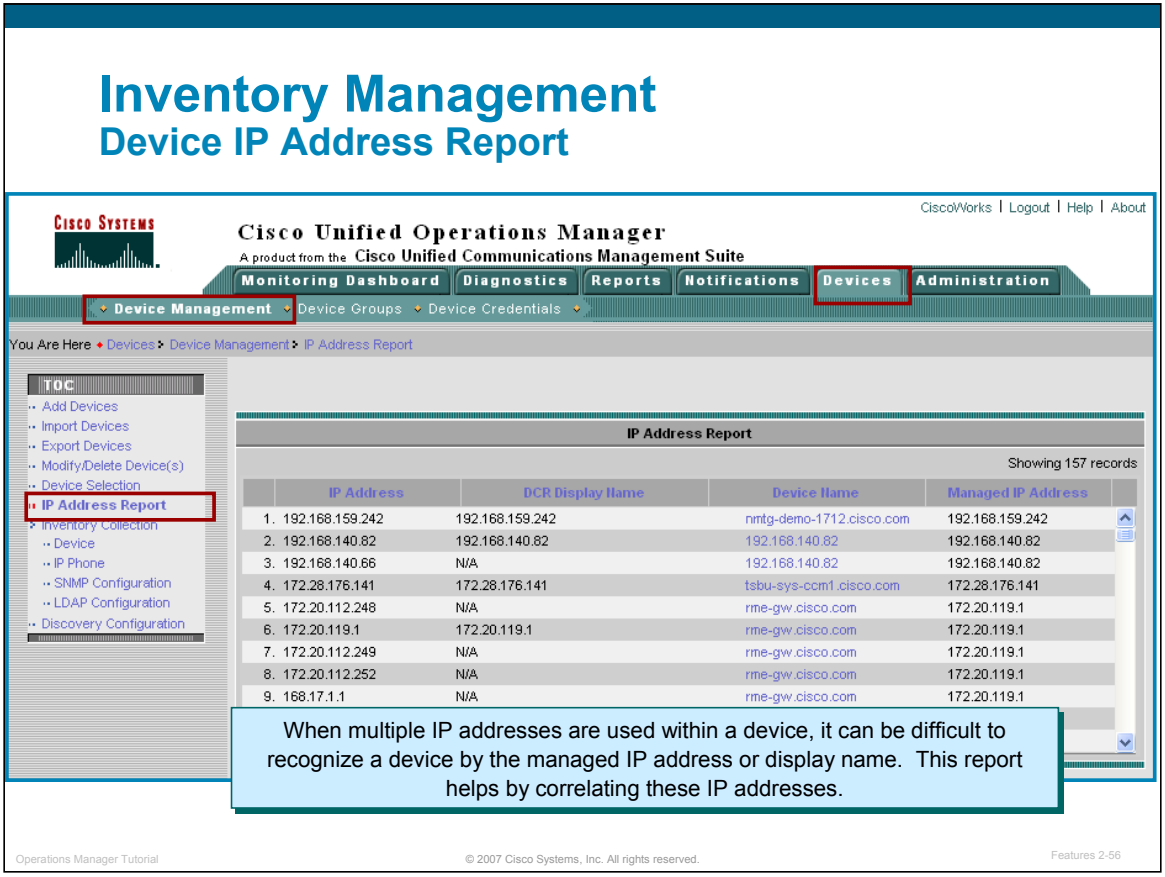
Inventory Management
Device Detail View



Device Detail View

The Device Detail View provides extensive information on the devices and device components for the device selected You can view information on devices that Operations Manager is currently monitoring, as well as devices whose monitoring you have suspended.

- View hardware and software information on system, environment, connectivity, and interface components
- View hardware and software information on subcomponents of aggregate devices
- View application status for Cisco CallManager, Voice Services, Work Flow, and Synthetic Tests, and provide launch points for administrative pages, if appropriate
- Suspend or resume management of a device or a device component so the device is no longer polled, or polling is resumed



Device IP Address Report

The IP Address Report lists all the IP addresses of the devices that are added to the OM inventory. The IP address list includes both the IP addresses of the devices in the DCR (including devices that are not monitored by Operations Manager) and the IP addresses of all the devices in Operations Manager inventory.

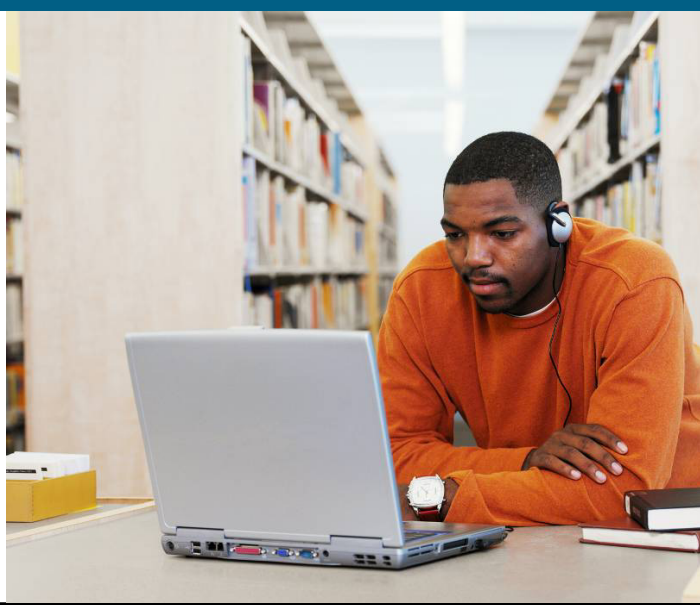
The IP Address Report page displays the following:

- The IP addresses for all the devices in the DCR, but not in OM inventory. The IP Address Report may only display the IP address (if added) and the DCR display name.
- The IP addresses for all the devices in OM inventory.
- All the IP addresses known for each of the devices in OM inventory. If there is more than one IP address for a monitored device, all the IP addresses are displayed. The DCR Display Name column displays N/A and the Device Name and Managed IP Address columns will have the same entries for the corresponding device.
- Duplicate device entries from the DCR. If there is more than one entry for the same device in the DCR (this can occur by varying the DCR display name), the IP Address Report identifies the duplicate entries and appends the display names with the corresponding IP address entry in the DCR Display Name column.

Note: The duplicate entries in the DCR are identified by having more than one display name in the DCR Display Name column of the IP Address Report.

Reports

- Operational Status Views
- Diagnostic Tests
- Inventory Management
- **Reports**
- Event Notification
- Customization / Advanced Features



Standard Reports
Overview

Report Type	Description
Alert and Event History	View stored information on past alerts and events
Service Quality History	View stored information on past service quality issues
IP Phones and Applications	View information about phones, installed applications and inventory changes. View reports on suspect and unregistered phones
Video Phones	View information about video enabled phones and inventory changes

- Reports can be a launch point for other tools
  - Diagnostic Tests
  - Drill down into device name for more details on the device (Configuration, Status, and Polling and Threshold Parameter Settings
- Sort by column headings, export, or print
- User role of “Network Administrator” can view all reports. Check the Permissions Report for other user roles to view reports.

Standard Reports Overview

Operations Manager provides an extensive set of reports that help network managers maintain information about their Unified Communications deployment. The figure above illustrates the various types of reports from Operations Manager.

The historical alert, event, and service-quality reports maintain information about all the alerts and events reported by Operations Manager for up to 30 days. This enables network managers to document any past outage and have access to it for long-term trending purposes.

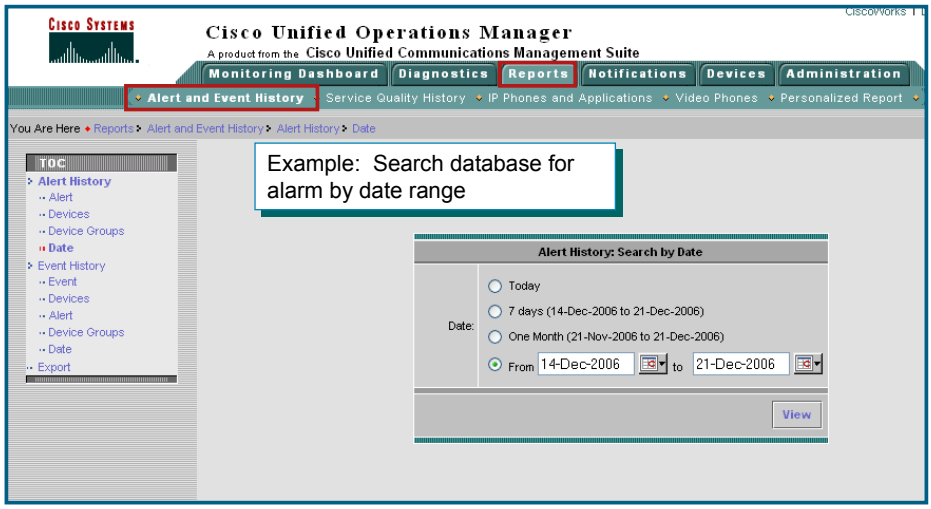
The IP phone inventory reports give network managers instant access to IP phone status information about every IP phone deployed in the network. Extensive information on signaling details and IP connectivity details is maintained and reported. These reports also track changes in phone status and thus serve to document move, add, and change operations on these IP phones.

The customizable reports let network managers pick and choose what type of information they want and create a daily report that is available for them by e-mail or the Operations Manager user interface.

You may not be able to generate some of these reports if you do not have the required privileges. (Refer to the section on Customization and Advanced Features / Security for more information on user accounts and user privileges.)

Standard Reports
Alert and Event History

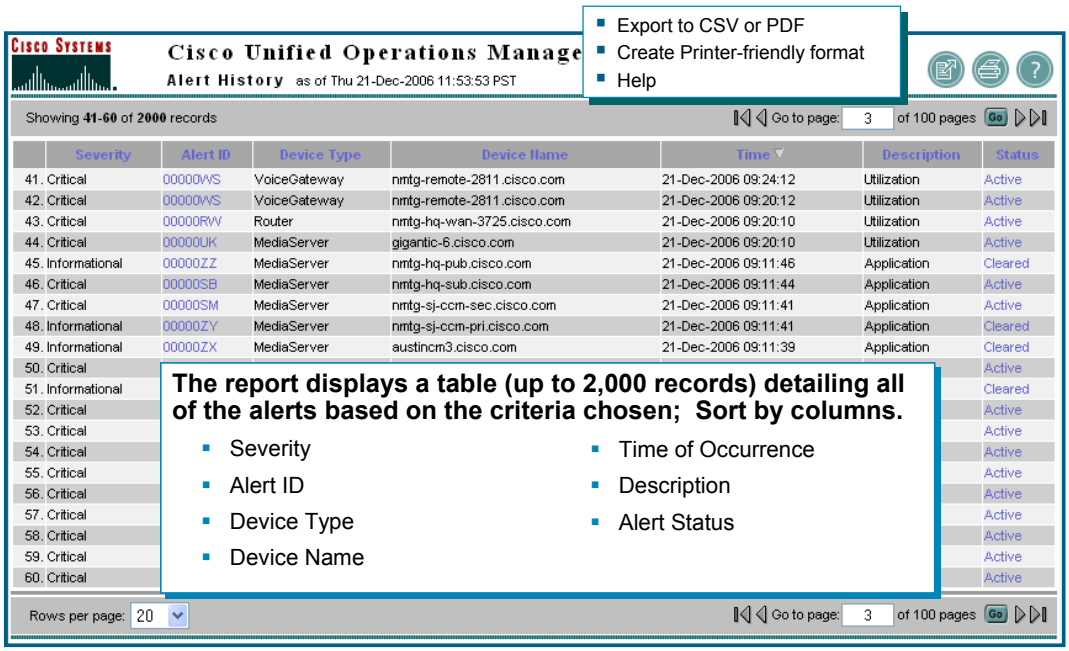
Customize searches according to what you are looking for, such as: alerts and events on certain devices, in a certain time period, or in a certain group



Standard Reports – Alert and Event History

The Alert and Event History reports let you view stored information on past alerts and events. This information is stored in a database, and you can customize searches according to what you are looking for. Use this feature to search through the database to look for alerts or events according to their ID, that occurred on specific devices or device groups or within a specific date range.

Standard Reports
Alert History



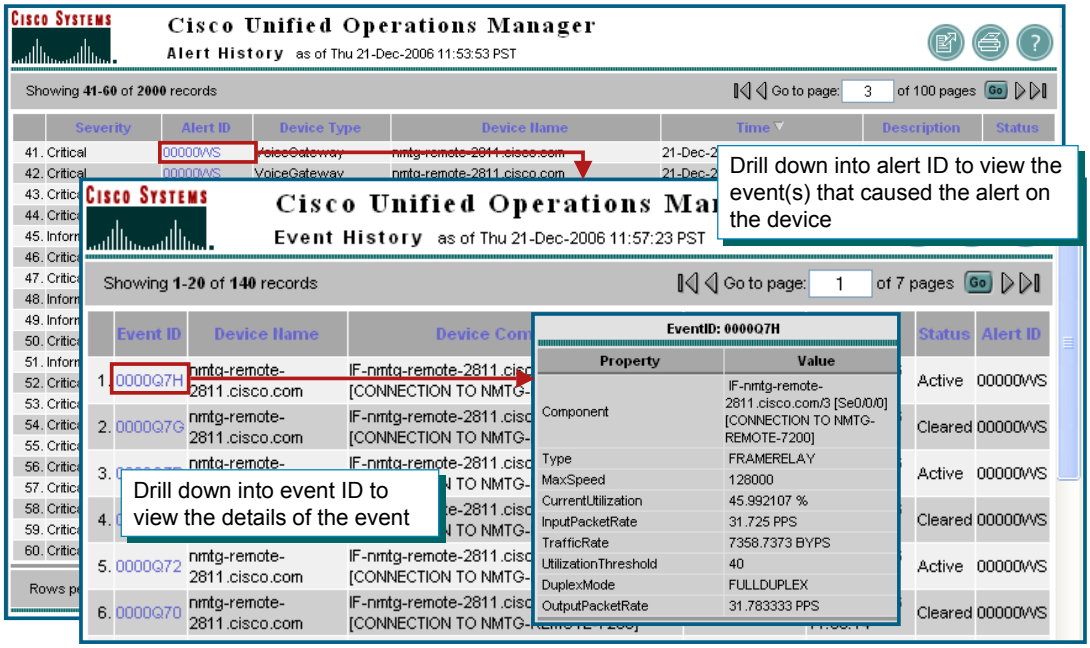
Standard Reports – Alert History

The Alert History report is a scrollable table that lists up to 2,000 records, based on your search criteria. To view database contents beyond the 2,000 records, click the **Export** tool button in the upper-right corner of the window.

The following information is displayed in this report:

- **Severity** – Critical, Warning, or Informational.
- **Alert ID** – Alert identifier number. Clicking this link opens the Event History report, which contains details about the events associated with the alert (see next page).
- **Device Type** – Note: Inventory Collection in Progress indicates that Operations Manager was discovering the device at the time of the alert. The actual device type is reflected when new events occur.
- **Device Name** - Device name or IP address
- **Time of Occurrence** – Date and time when the alert was generated.
- **Description** - Alert category, one of the following: Application, Connectivity, Environment, Interface, Other, Reachability, System Hardware, Utilization. For alerts containing multiple events, the report shows the category of the event with the most recent change.
- **Alert Status** - Based on last polling: Active, Cleared, Acknowledged

Standard Reports
Event History



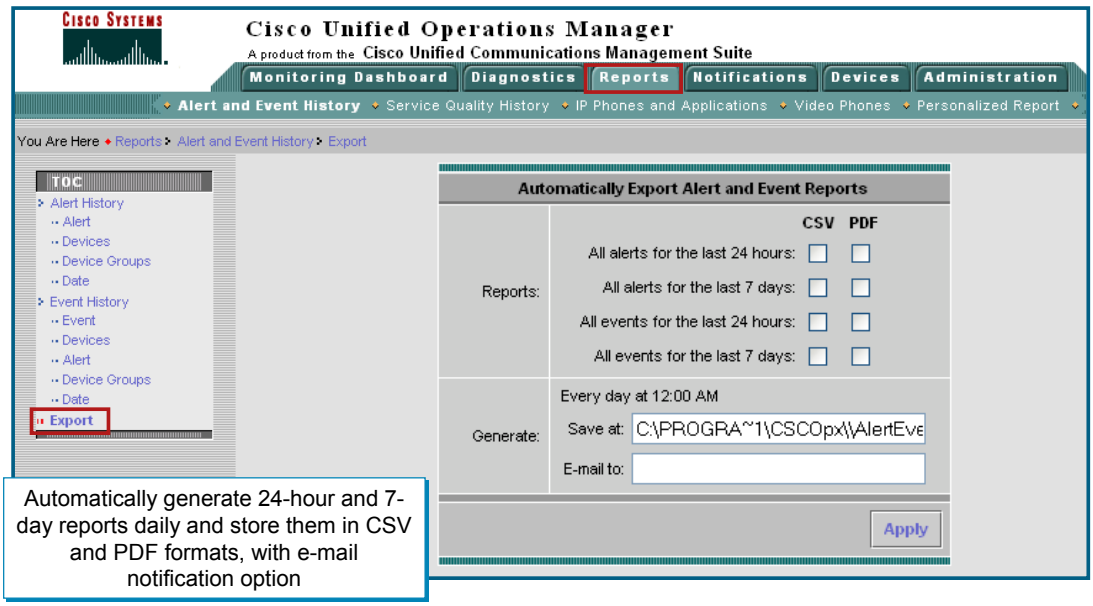
Standard Reports –Event History

Here is an example of the Event History report. This example was obtained by selecting the **Alert ID** in the Alert History report, which allows the user to view the event(s) that caused the alert on the device. This is just one way to generate this report. Using the **Reports> Alert and Events History** task can also generate Event History reports by searching the database using event criteria.

The Event History report lists events. For each event, the Event History report includes:

- Event ID link to open the Event Properties page and view current attribute or threshold values compared with the values at the time the event occurred (illustrated above)
- Device on which the event occurred
- Component on which the event occurred
- Time of the event
- Current status of the event based on last polling:
    - **Active** – Event is live.
    - **Cleared** - Event is no longer live. Also, when a device is suspended, all alerts are cleared. When Operations Manager polling determines that an alarm has been in the Cleared state for 30 minutes or more (from the time of polling), the alarm expires and is removed from the Alerts and Events display.
    - **Suspended** – Operations Manager is no longer monitoring the device.
    - **Resume** - Operations Manager is being configured to monitor the device again.

Standard Reports
Export Alert and Event History



Automatically generate 24-hour and 7-day reports daily and store them in CSV and PDF formats, with e-mail notification option

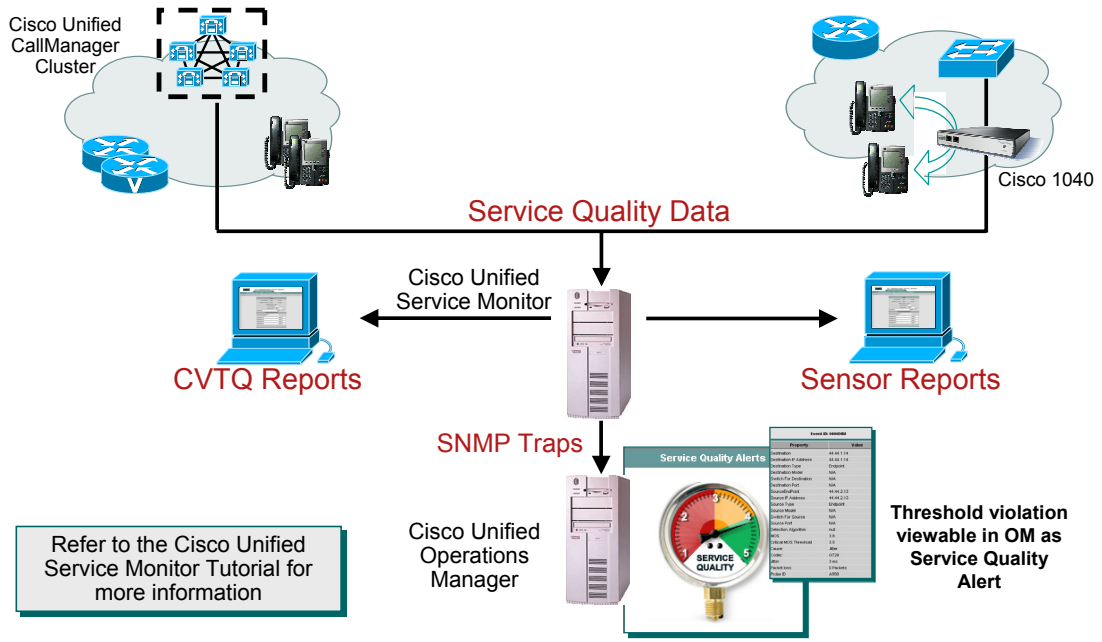
Standard Reports – Export Alert and Event History

Alert and event reports can be generated on a scheduled basis at midnight to provide 24-hour and 7-day reports daily. (7-day weekly reports are generated on Mondays.)

The reports can be stored in CSV and PDF formats. OM can be configured to send an email notification to remind users that the reports have been generated and available for viewing.

- All alerts for the last 7 days--7-day reports are named AlertReports_Weekly_ddmmyyyy.filetype, for example AlertReports_Weekly_17Apr2006.pdf. 7-day reports run weekly on Monday at midnight.
- All events for the last 24 hours--24-hour reports are named EventReports_Daily_ddmmyyyy.filetype, for example EventReports_Daily_20Apr2006.csv.
- All events for the last 7 days--7-day reports are named EventReports_Weekly_ddmmyyyy.filetype, for example EventReports_Weekly_17Apr2006.pdf. 7-day reports run weekly on Monday at midnight.

Standard Reports
Service Quality Reports Overview



Service Quality Reports - Overview

As mentioned earlier in the Service Quality Alerts Dashboard section, Operations Manager can use the information provided by the Service Monitor application to present service-quality (quality-of-voice) alerts on a real-time basis. The service-quality alerts are associated with IP phones or Unified Communications devices that are currently monitored by Operations Manager and present that information in the Service Quality Alerts Dashboard.

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

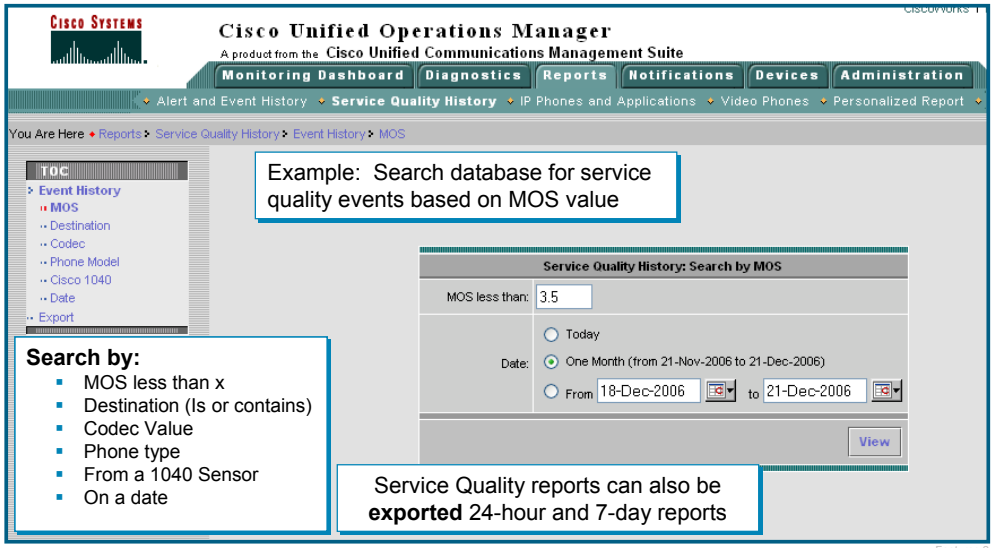
This solution helps enable IP network and IP telephony managers to more effectively manage their IP communications infrastructure by providing near real-time quality of voice metrics and providing alerts when the voice quality falls below a user-defined threshold.

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

For more information on the Cisco 1040 Sensors and Service Monitor, refer to the Service Monitor tutorial or Chapter 5 for online links.

Standard Reports
Service Quality History

- Search history database according to what you are looking for
- Setup Operations Manager to automatically export the information.



Service Quality History Report

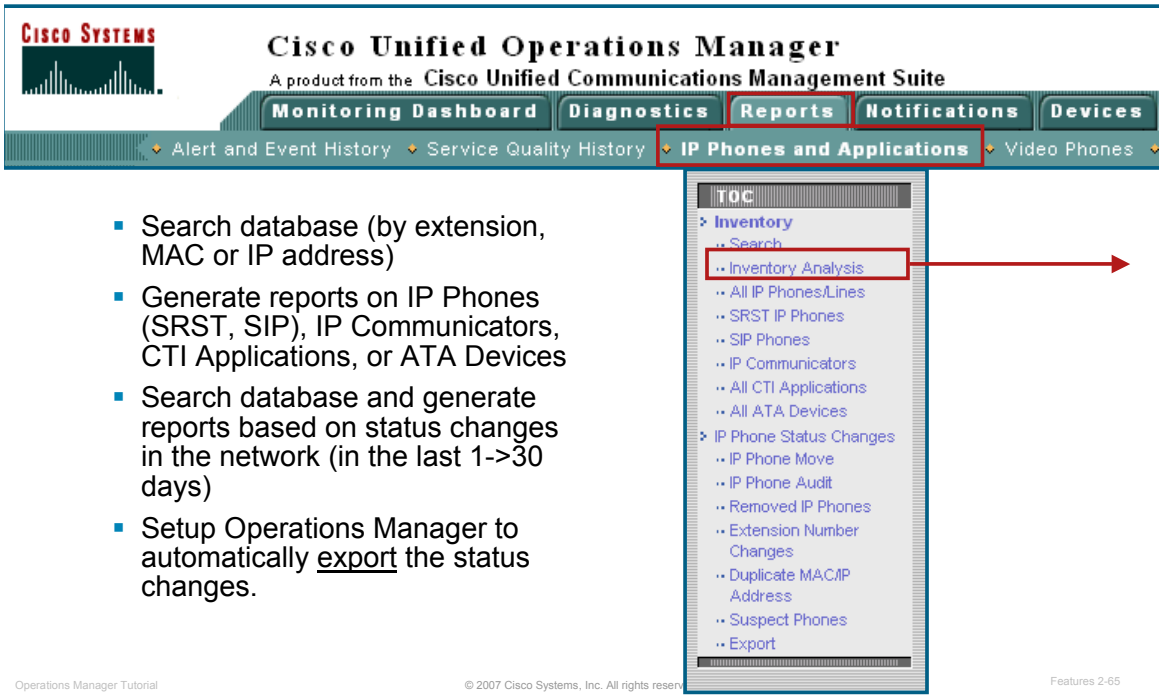
The Service Quality History report is a scrollable table that lists up to 2,000 records, based on your search criteria. To view database contents beyond the 2,000 records, click the **Export** tool button in the upper-right corner of the window.

Use the search criteria in the TOC to search the database for service quality events based on the criteria selected. The report provides information on the following:

- Event Severity
  - Warning--MOS is below the MOS threshold configured on Service Monitor.
  - Critical--MOS is below the MOS threshold configured on Operations Manager.
- Event ID - Click this link to open the event properties window.
- Destination Type: Endpoint or IP Phone
- Destination - IP address or phone extension.
- IP Address - Destination IP address.
- MOS - Mean Opinion Score that triggered the event.
- Cause - One of the following: Jitter or Packet Loss
- Time - Date and time that the event occurred.
- Codec - One of the following: G711, G722, G728, G729
- Source Type - One of the following: Endpoint or IP Phone
- Source - IP address or phone extension.
- IP Address - Source IP address.

You may not be able to generate some of these reports if you do not have the required privileges. (Refer to the section on Customization and Advance Features / Security for more information on user accounts and user privileges.)

Standard Reports
IP Phones and Applications



Standard Reports – IP Phones and Applications

Many reports exist for reporting on IP Phones. The upcoming pages provide examples of these reports.

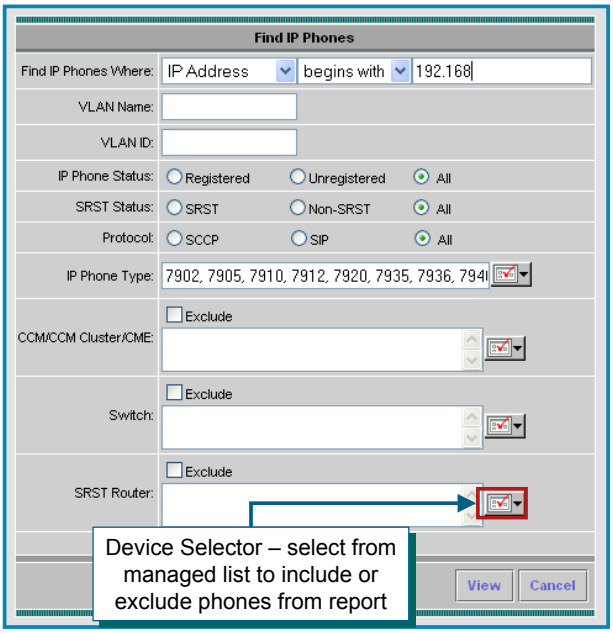
In addition to reports, Operations Manager has the feature to search its database to locate IP phones in the network. You can search for phones using all or only part of an extension number, IP address, or MAC address. The Search Inventory feature provides a quick pop-up window for each phone that matches the criteria. To search for phones using more attributes (i.e. VLAN, phone status, SRST, phone model, CCM address or cluster, connecting switch or SRST router address) or to obtain a full report on phones matching the criteria, use the Inventory Analysis report feature.

Note(s):

- If you are unable to see information about an IP phone, either the switch or the Cisco CallManager with which the phone is associated to, is not monitored by Operations Manager. To correct this, either add the unmonitored switch or CCM to the Operations Manager inventory or if in the inventory, check the status or reachability of the device.
- For the Cisco Wireless IP Phone 7920 to be monitored in Operations Manager, its Aironet access point must also be monitored by Operations Manager. Only the logical information from the Cisco CallManager will be displayed for this phone. All the switch information for the 7920 will appear as Not Available.
- If Cisco IP Soft Phone records do not appear, generate the IPT Applications Details display.

Now let's look at an example of how to generate an inventory report by analyzing the database.

Standard Reports
IP Phones and Applications – Inventory Analysis



Find IP Phones in the managed inventory and generate a report based on:

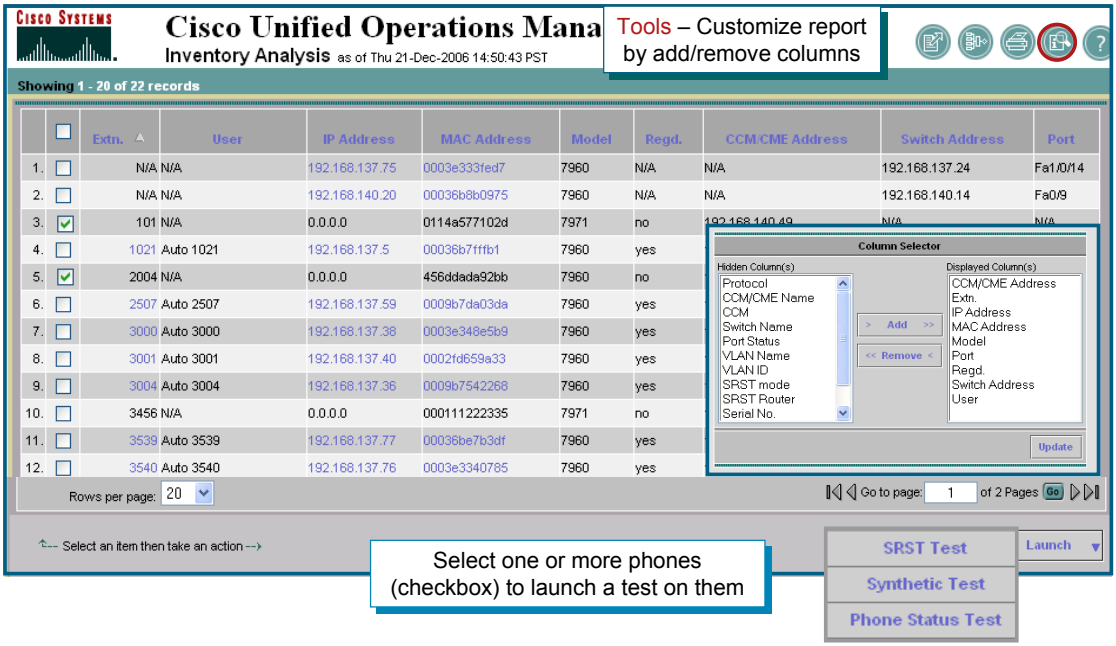
- Extension, MAC or IP address
- VLAN name or ID
- Status
- SRST Status
- Protocol (SCCP, SIP)
- Phone model
- Cluster
- Connecting switch
- SRST router

Standard Reports – IP Phones and Applications – Inventory Analysis

Use the **Reports> IP Phones and Applications** task to search the database based on defined criteria: properties or status changes, as illustrated above.

The dialog offers a variety of parameters in which to search the phone inventory. For this example, the **IP Address** attribute is selected from the “Find IP Phones Where” pull down list. Select **begins with** from the next pull down list, and enter 192.168 in the third box.

Standard Reports
IP Phones and Applications – Inventory Analysis

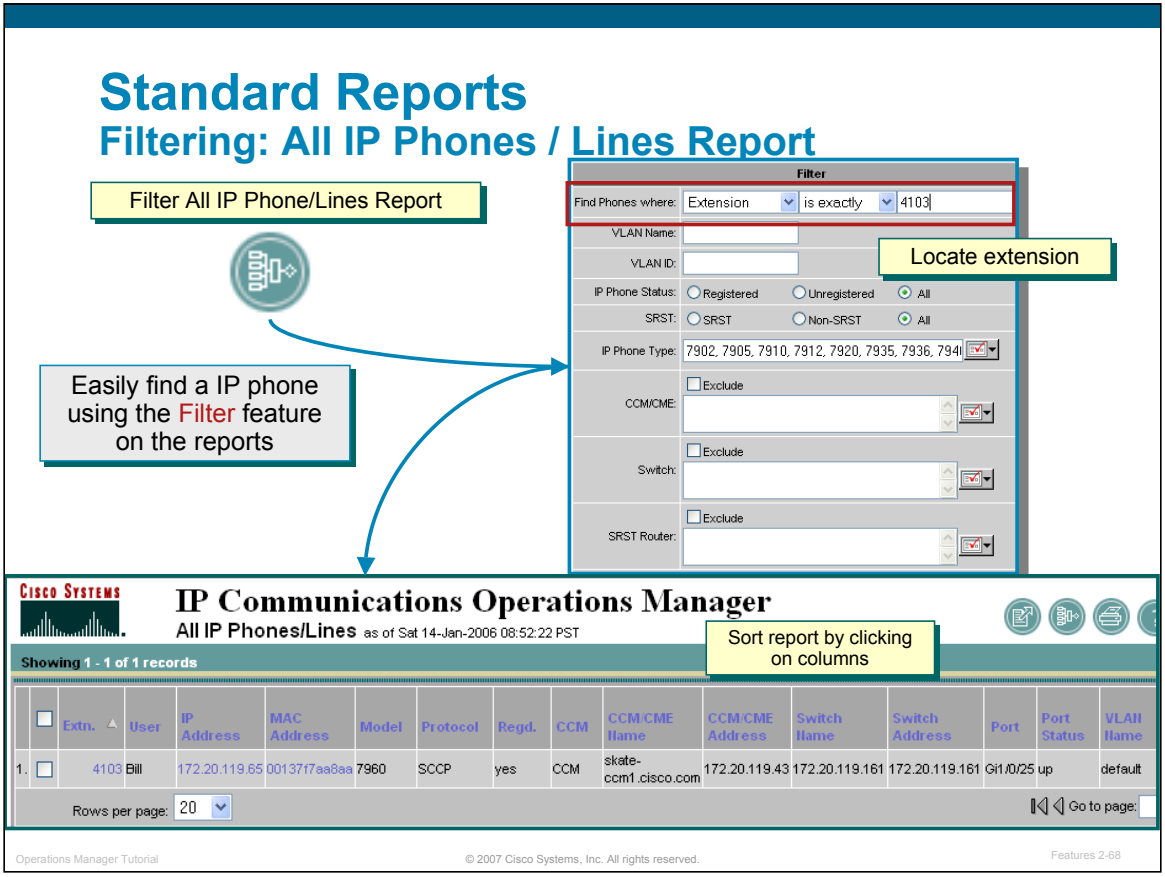


Standard Reports – IP Phones and Applications – Inventory Analysis

As can be seen by the report above, the listed phones all have IP addresses beginning with 192.168.

Like most phone-based reports, you can select certain phones and launch diagnostic tests.

Also, notice the Tools icon. This allow you to customize reports by adding and/or removing columns from the report, as illustrated above.

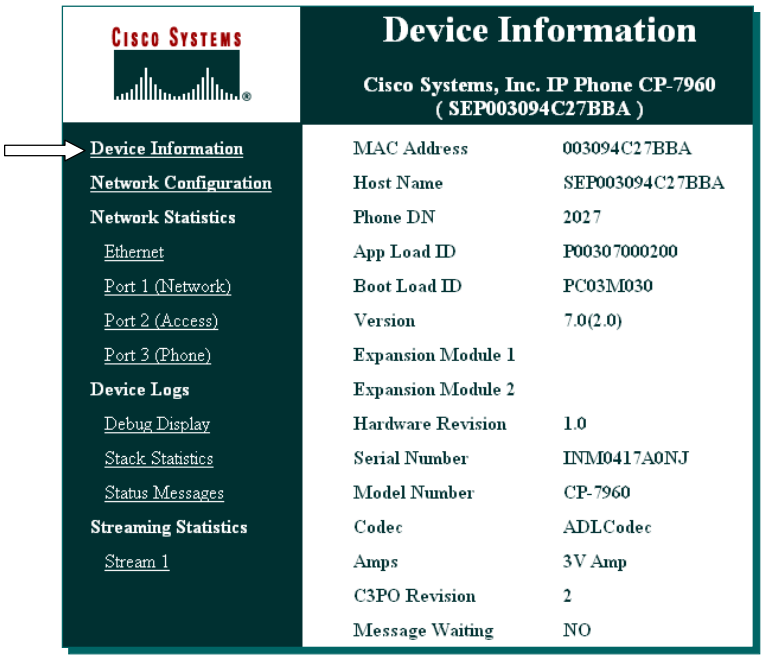


Filtering: All IP Phones/ Lines Reports

The **All IP Phones/Lines Report** lists all IP phones, including IP Communicators and IP phones that are configured for SRST. Use the **Filter** feature to include only the phones that you want to see.

Additionally, the operator could also sort the list (ascending or descending) by clicking on the column headings one or more times.

Standard Reports
Example: IP Phone Web Interface



IP Phone Web Interface

- From any report, click on a phone's extension number, IP or MAC address
- This takes you directly to the IP phone's web interface
- Access the phone's configuration, logs, and statistics

Standard Reports – Example: IP Phone Web Interface

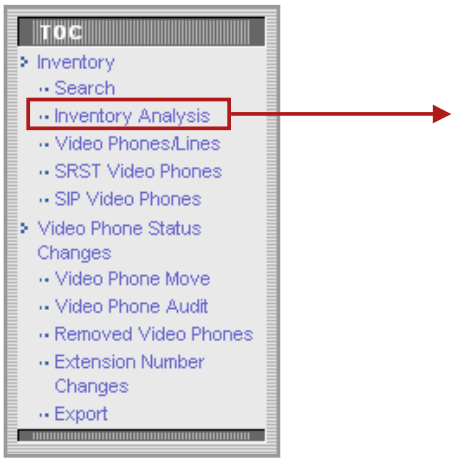
To open an IP phone web interface from any report, click one of the following hyperlinks:

- Extension number
- IP address
- MAC address

Another window opens with information directly from the phone, including network configuration details, device, port, and Ethernet information for the specified IP phone.

Standard Reports
Video Phones

- Search database (by extension, MAC or IP address)
- Generate reports on Video Phones (SRST, SIP)
- Search database and generate reports based on status changes in the network (in the last 1->30 days)
- Setup Operations Manager to automatically export the status changes

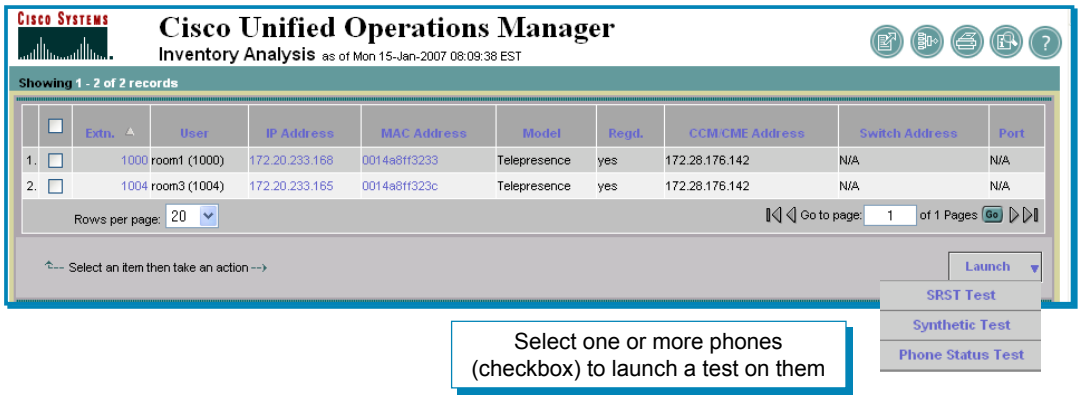


Standard Reports – Video Phones

Video Phones reports provide two types of reports: inventory and video phone status change:

- **Inventory reports** - Provide detailed video phone data, reflecting the current status of Video Phones in your network. Search for a few video phones; list a specific set of video phones--such as phones connected to a switch or phones in SRST mode--or view all video phones and lines:
  - Search--Use Search to view information for a few video phones or a single video phone; search enables you to find phones using all or part of an extension number, IP address, or MAC address.
  - Inventory Analysis--Use the Inventory Analysis report to display Video Phones that meet criteria that you specify; for example, Video Phones that are registered to a particular Cisco Unified CallManager or Video Phones that are not connected to particular switches.
  - Video Phones/Lines--Use the Video Phones/Lines report to view data for all Video Phones that Operations Manager is monitoring.
  - SRST Video Phones--Use the SRST Video Phones report to view data for Video Phones that are configured for Survivable Remote Site Telephony (SRST) only. Video Phones that are configured for SRST are also included in the All Video Phones/Lines report and can be included in the Inventory Analysis report.
  - SIP Video Phones--Use the SIP Video Phones report to view data for all SIP Video Phones that Operations Manager is monitoring.
- **Video Phone Status Changes** reports - Video phones that have undergone a status change during the previous 1 to 7 days:
  - Video Phone Move--View data for phones that have been connected to a different switch or switch port or that have registered to a different Cisco Unified CallManager.
  - Extension Number Change
  - Removed Video Phones
  - Video Phone Audit--Obtain a summary of changes, including data for phones that have moved, been removed, undergone an extension number change, appeared in inventory with a duplicate MAC or IP address, or become suspect.

Standard Reports
Video Phones Example



Select one or more phones (checkbox) to launch a test on them

Standard Reports – Video Phones Example

Above is an example of a Video Phones report using the Inventory Analysis option.

Like most phone-based reports, you can select certain phones and launch diagnostic tests.

Also, notice the Tools icon. This allow you to customize reports by adding and/or removing columns from the report, as illustrated above.

The export feature in the TOC (previous page) is also available for Video Phone reports.

Personalized Reports
Overview

- Operations Manager allows you to create a personalized view of the data associated with key elements such as devices, IP phones, and diagnostic tests
- Also provides system-wide information about added and removed devices and phones
- To create and view a personalized report:
  - Configure/define the contents
  - Export (schedule) the report
  - Select a report and view it

Personalized Reports - Overview

The Personalized Report enables you to configure a report that includes devices, IP phones, and diagnostic tests that interest you. You can create one personalized report per user.

To create a personalized report, use the **Reports> Personalized Reports** menu, and follow these steps:

1. Determine what you would like the report to display. A single report can contain managed devices, IP phones, and OM diagnostic tests that have already been defined.
   a. To add managed devices to the report, select the **Devices** radio button in the Configure pane. The Device Selection dialog will appear. Open the tree hierarchy to select one or more device groups to select or individual devices.

      *When you have the device(s) that you want in the report, click **Save** to save your selections.*

   b. To add managed IP phones to the report, select the **Phones** radio button in the Configure pane. (If phones have already been added to the report, they will be listed here.) Click Add to add phones manually (Known List) or by selecting the phones from the Phone Report. To manual add phones, click Known List and for each phone, enter its MAC, IP and Extension separated by a ",". Multiple phone records must be separated by a ";".

      When you have the IP Phone(s) that you want in the report, click **Save** to save your selections.

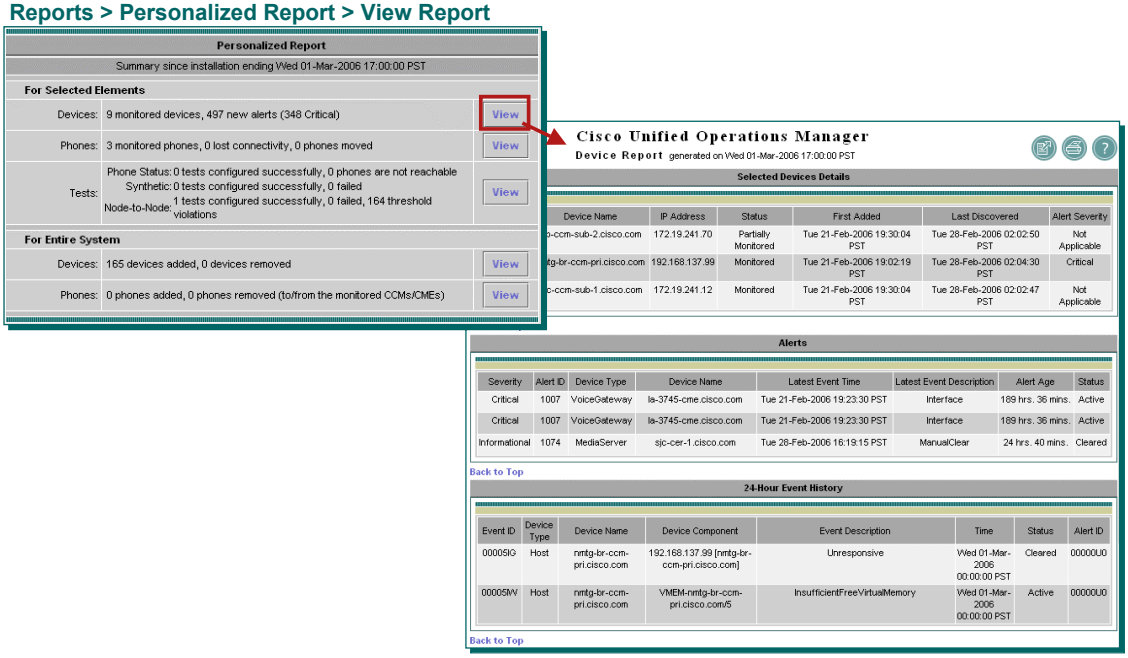
   c. To add Diagnostics Tests to the report, the tests must already be configured and then can be selected by clicking the radio button for the appropriate test type.

      When you have the test(s) that you want in the report, click **Save** to save your selections.

      At any time, you can click **View** to see a summary of your selections (devices, phones, or tests)
2. Next, export or schedule the report so that it may be viewed.

Personalized Reports
Example

Reports > Personalized Report > View Report



Personalized Reports – Example

After you have configured (defined the contents of) your personalized report, scheduled (or exported) it, and after the execution time has passed, you can then view the personalized report

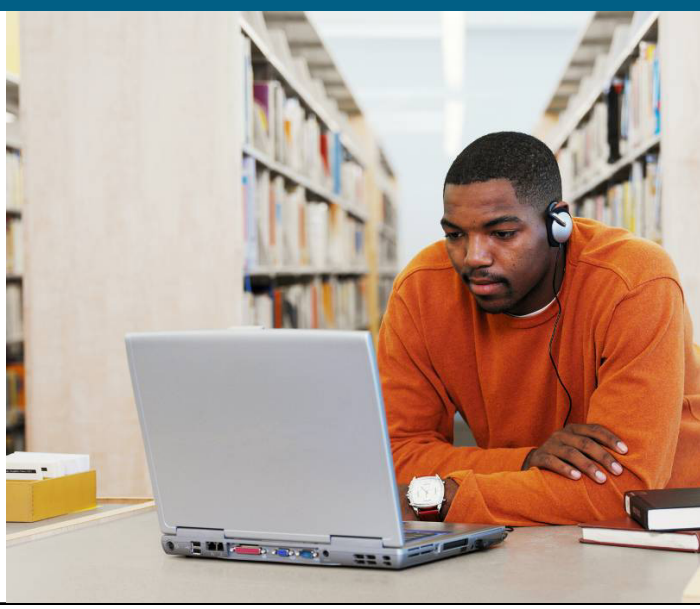
From the Reports tab, select the **Personalized Report** option. Select the **View Report** task from the TOC. A **View** button will be displayed for each type of component. Click the appropriate one to see the data. As can be seen in the report above, the device report provides basic information about each device selected during the configuration of the report and any associated alert information.

The personalized report also includes two system inventory reports detailing the change to the device and phone inventories since the last execution of the report.

<*Intentionally Blank*>

Event Notification

- Operational Status Views
- Diagnostic Tests
- Inventory Management
- Reports
- **Event Notification**
- Customization / Advanced Features



Event Notification Services
Terminology

- **What is a Notification?**
  - An E-mail, Syslog message, or SNMP trap alerting a user to an event
- **How can Notifications be limited to specific devices or events?**
  - Define the Device-Based *Notification Criteria* (reasons to generate a notification)
  - Use Event Sets in the criteria definition to further limit which events are monitored and would trigger a notification
- **How can Notifications be limited to specific Service Quality Alerts?**
  - Define the Service Quality-Based *Notification Criteria*
- **How do I configure Notifications?**
  - Operations Manager has a wizard-based dialog to help define all parameters
  - Define when, during the day, events should be monitored for notification; define what type of notification to send (e.e. E-mail, Syslog, or trap); and define who or which device should receive the notification

Event Notification Services

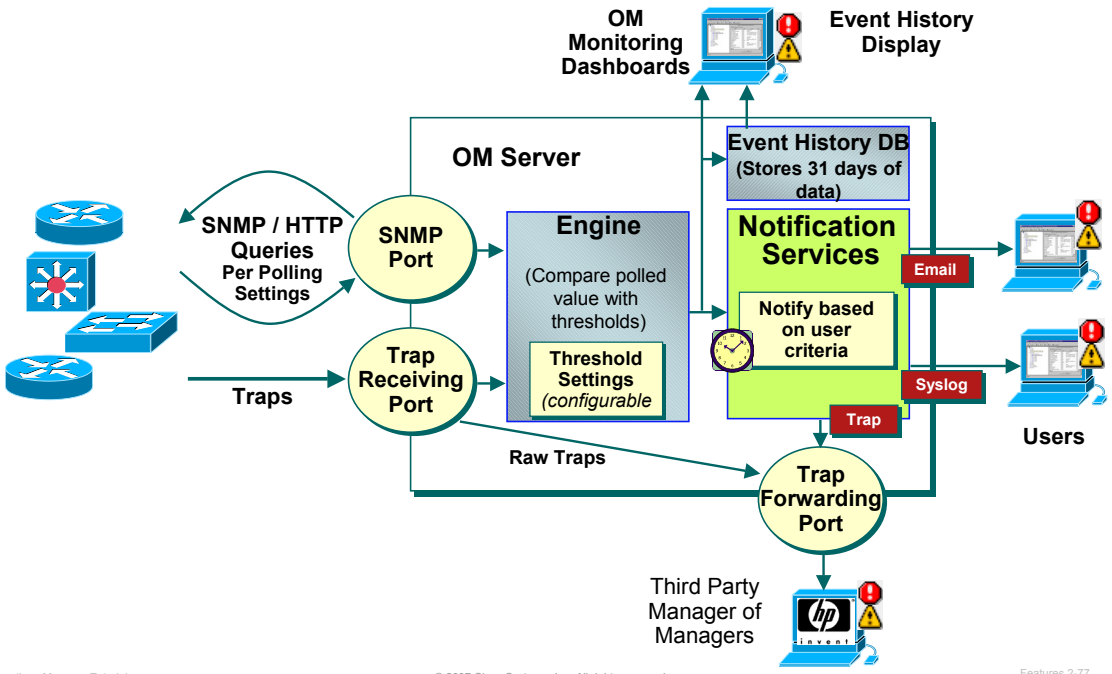
As you have seen earlier in this chapter, Operations Manager displays alerts in response to events that occur in the Unified Communications environment and the IP fabric. These alerts can be viewed in the Monitoring Dashboards, such as the Alerts and Events display. In addition, using the Notification Services in Operations Manager, you can configure Operations Manager to forward information about *specific* alerts and events to SNMP trap daemons on other hosts, Syslog daemons, and users using email.

The receipt of an e-mail, Syslog message, or SNMP trap alerting a user or device of an event is called a *Notification*. The criteria that causes a notification can be defined by selecting the event sets that would cause a notification and then by selecting additional matching criteria for the event set. Operations Manager supports two types of notification criteria: Device-based and Service Quality- based (discussed shortly).

Note(s):

- *Using the **Event Customization** task, you can also customize the names and severity of the device-based events displayed by Notifications. (Refer to the next topic in this chapter, "Customization Features".)*

Event Notification Services
Overall Functional Flow

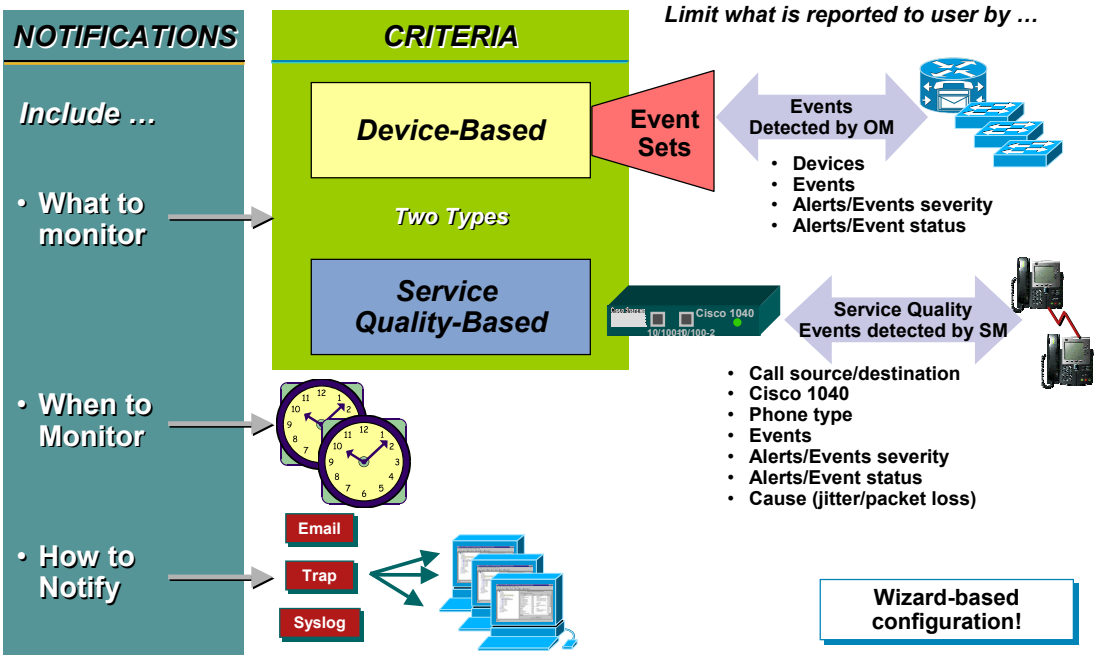


Event Notification Services– Internal Functional Flow

The Alerts and Event display is one of the main ways to use Operations Manager on a day-to-day basis, but would require constant visual contact to be alerted to changes in the state of the network. To free the network administrators from 24/7 visual contact with the Alerts and Events display, Operations Manager allows for alternate means to notify personnel – E-mail, SNMP traps, and Syslog message. Each of these notification mechanisms would provide a summary of the alert/event. The receiver of the notification could then return to Operations Manager for more details.

Notifications are sent based on subscriptions to notification groups. Basically a notification group is a set of events and alerts occurring on a set of devices. This allows for different recipients or notification mechanisms for different devices and alerts for ultimate notification flexibility.

Event Notification Services
Defining Notification Services Within OM



Defining Notification Services Within Operations Manager

To define notification services in OM, you need to define a subscription to notification services. The subscription is monitoring alerts and events between a timeframe, and if the alert or event matches the notification criteria, the subscription will send out an E-mail, trap, or Syslog message to one or more recipients.

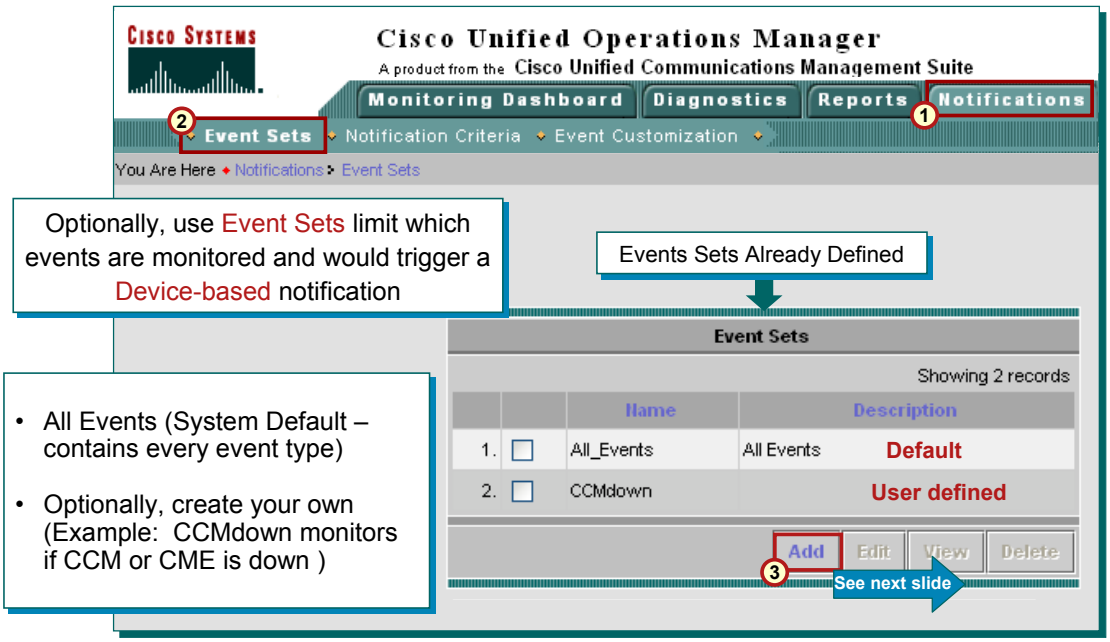
But before you can define the subscription in OM, you need to define the notification criteria which can be either device-based or service quality based. If it is device-based, you also have the option before defining the notification criteria, to define Event Sets.

For example, in some cases, you might want to send notifications for only a subset of the events that Operations Manager monitors. You can set the events that are of interest to you when you define the notification criterion:

- Specify an event set for a device-based notification criterion. You can create as many events sets as you would like.
- Select the events that you want Operations Manager to monitor for Service Quality-based notification criteria. There are few Service Quality-based events and you can select among them when you add or edit Service Quality-based notification criteria.

Let's show you how these components are defined in OM.

Event Notification Services
Event Sets (Optional for Device-Based Criteria)



Event Sets (Optional)

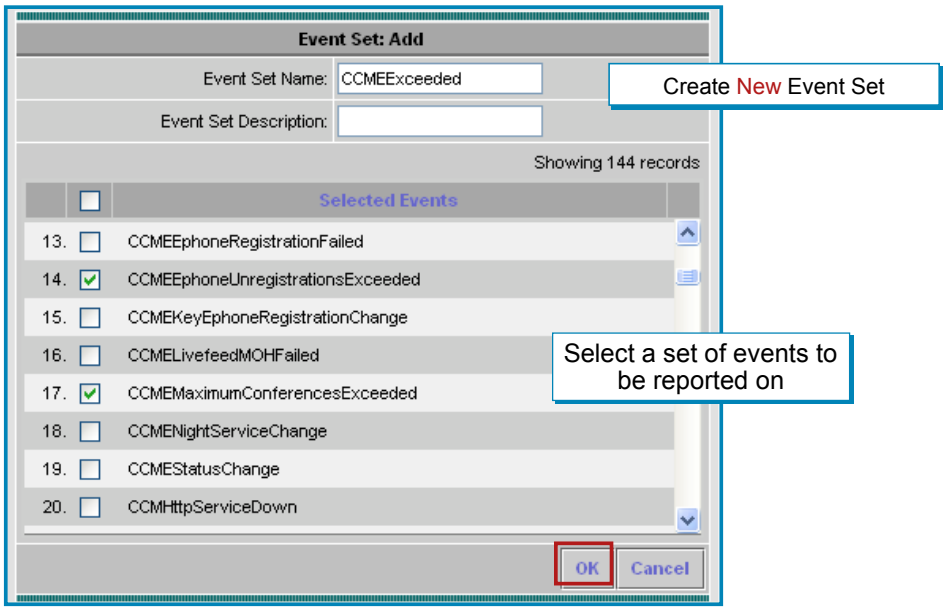
Event sets enable you to group the events the you want Operations Manager to monitor for the purpose of sending notifications. Use event sets to:

- Limit the number of events that Operations Manager notification monitors. When you do not use event sets, Operations Manager notification monitors all events to determine whether to send a notification.
- Aggregate the notifications that you want to send to different destinations. For example, you can create separate event sets for each of the following purposes:
- Limit the amount of e-mail notification sent to specific individuals or departments to only those for certain events.
- Write all occurrences of particular events to Syslog.
- Send SNMP traps when certain events occur.

Note(s):

- *When you create device-based notification criteria (discussed shortly), you must include an event set as one of the criteria.*
- *The default event set, All_Events, includes all events.*

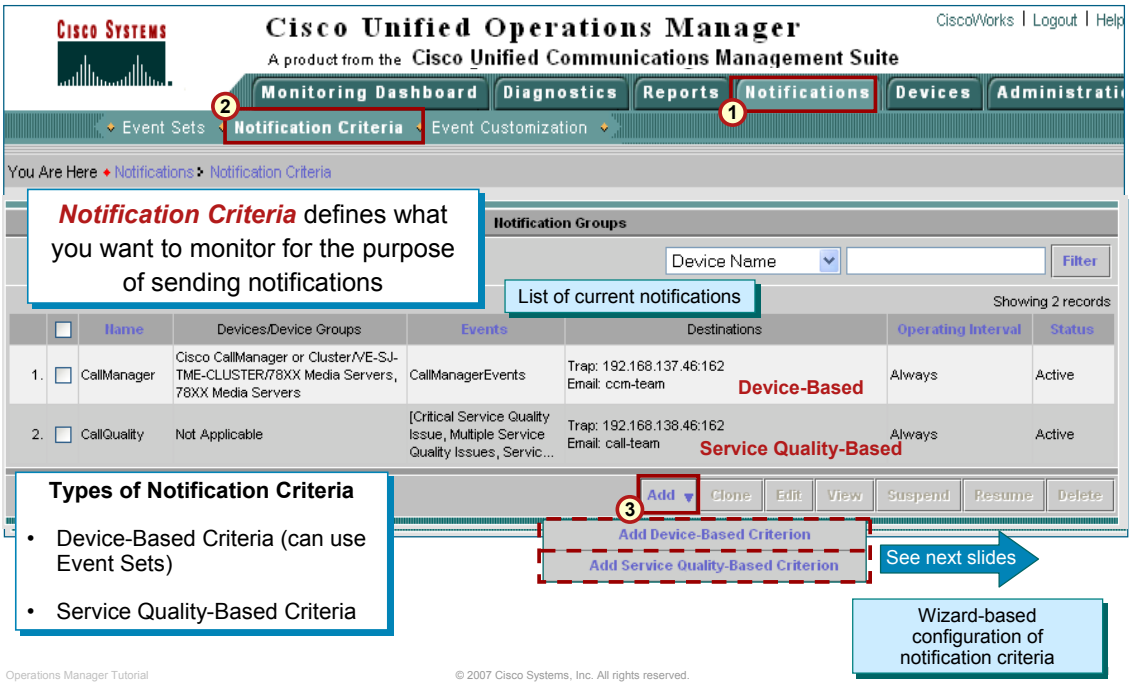
Configuring Notification Services
Event Sets (Optional), (Cont.)



Event Sets (Optional) – Defining a New Event Set

If you want to use event sets to limit the events to be notified on, use the Add button, as shown on the previous page. Enter a meaningful name and description for the event set. Click the events listed is the Selected Events portion of the dialog that you wish to include in this event set. These are the events you will be notified about. You will then be able to select this new event set when defining Device-based Notification Criteria (discussed next).

Event Notification Services
Notification Criteria



Notification Criteria

Notification criteria defines what you want to monitor for the purpose of sending notifications. (A notification criterion is a required part of any subscription.) The criteria that causes a notification can be defined by selecting the event sets that would cause a notification and then by selecting additional matching criteria for the event set.

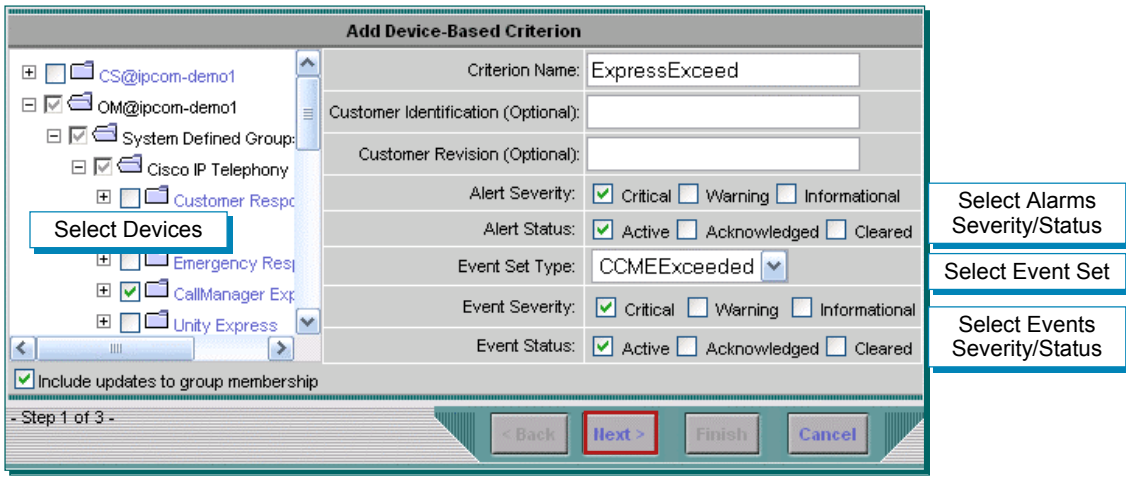
Operations Manager supports two types of notification criteria (both discussed next):

- Device-based
- Service Quality- based.

The Notification Criteria is defined in Operations Manager using a Wizard-based dialog. The first step is to select the type of notification criteria, highlighted here.

Event Notification Services
Define Device-Based Criteria

Limit which alerts / events are reported to user by …



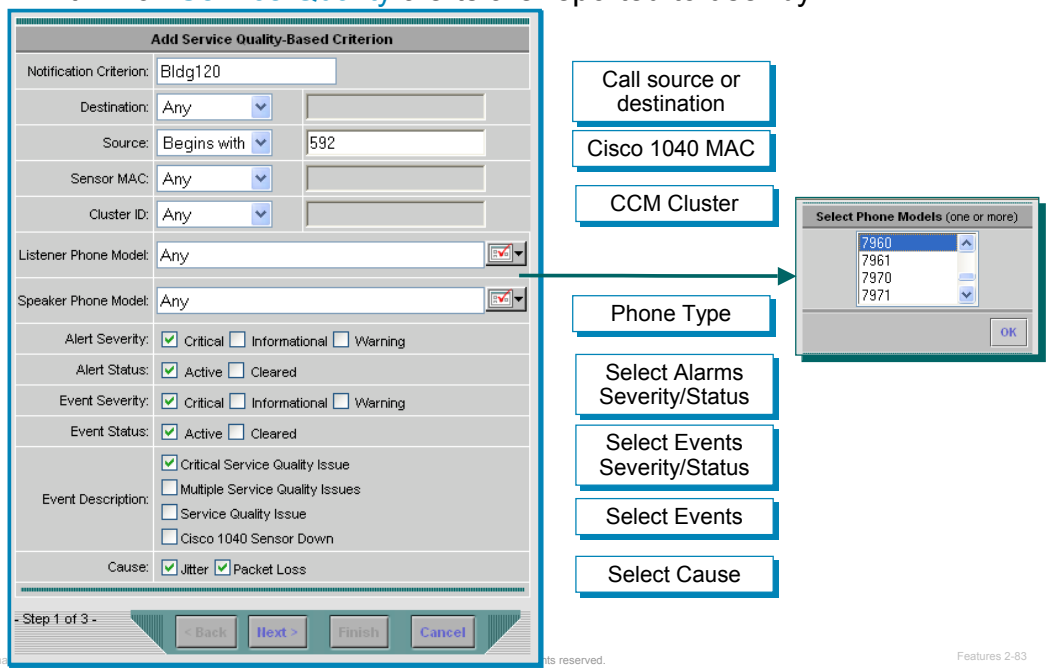
Notification Criteria: Device-Based

If you selected Device-Based Criteria, the Wizard dialog will allow you to select devices to monitor. The dialog includes the following:

- Devices--The devices or device groups that you want to monitor.
- Event sets--(Optional). One or more groups of events that you want to monitor.
- Alert severity and status--One or more alert severity levels and status.
- Event severity and status--One or more event severity levels and status.

Event Notification Services
Define Service Quality-Based Criteria

Limit which Service Quality alerts are reported to user by …



Notification Criteria: Service Quality-Based

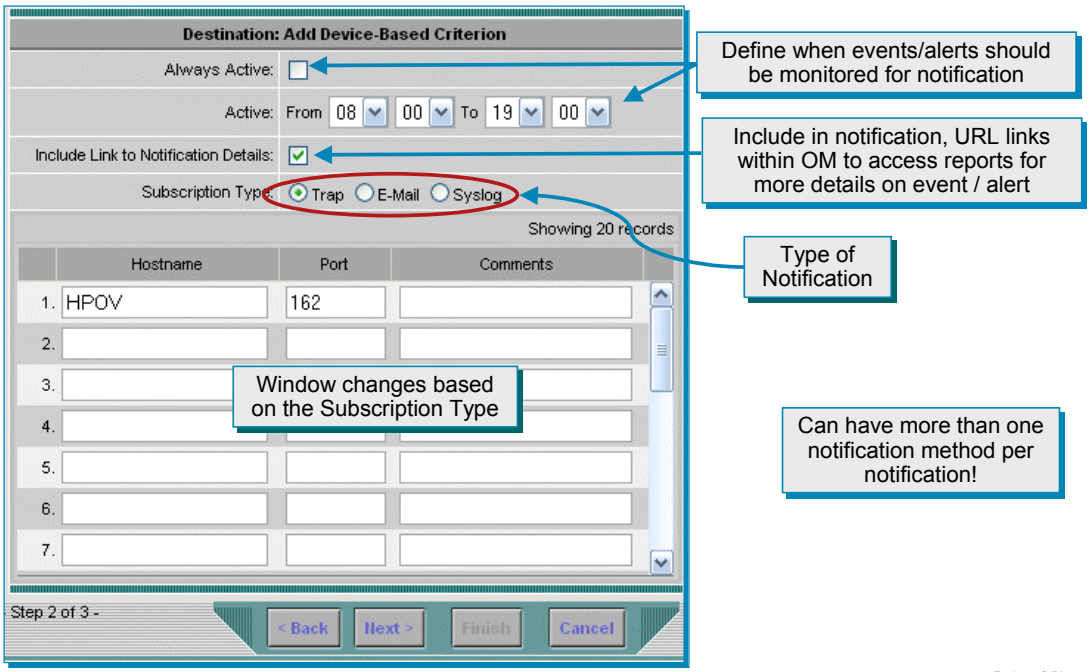
If you selected Service Quality-Based Criteria, the Wizard dialog will allow you to select criteria to notify you based on the following:

- Phones, endpoints, or probes--Phones, call endpoints, or probes that you want to monitor.
- Alert severity and status--One or more alert severity levels and status.
- Event severity and status--One or more event severity levels and status.
- Note: You cannot customize the names and severity of the Service Quality-based events displayed by Notifications.
- Service Quality-based criteria are useful when the Service Monitor application and Cisco 1040 sensors are deployed in the network. Operations Manager must be configured as a trap receiver within the Service Monitor application.

Note(s):

- Service Quality-based criteria do not include events sets.

Event Notification Services
Subscription (Tying It All Together)



Subscription – Tying It All Together

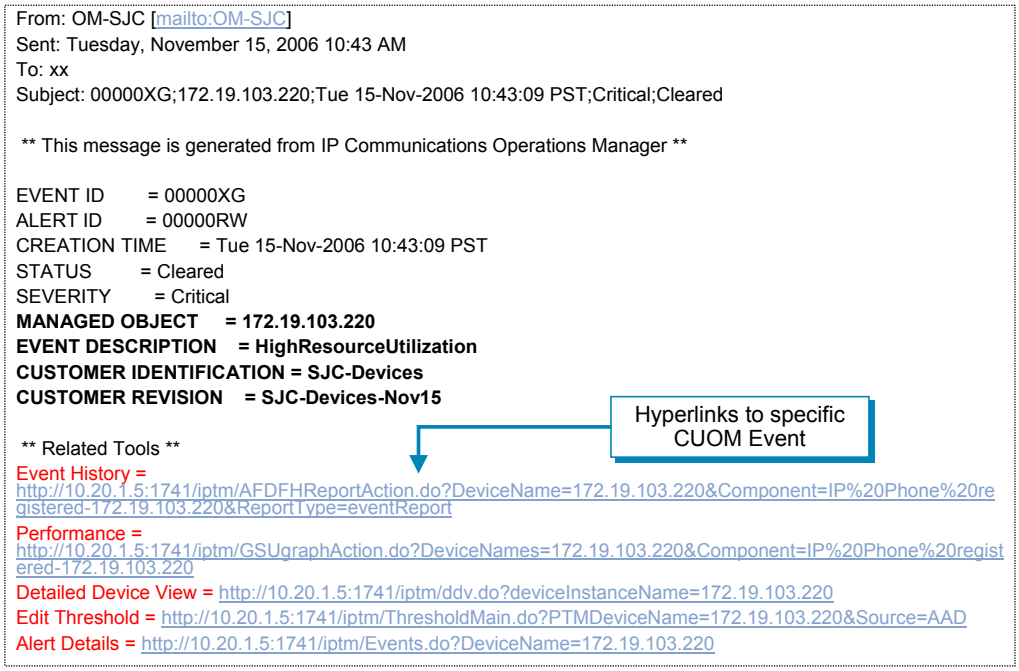
The next step in the Wizard-based dialog is to define the subscription to the notification criteria. A subscription in Operations Manager is the final part of defining Notification Services. The subscription is a user-defined set of rules for generating and sending notifications. The subscription includes:

- Notification criterion--A named set of reasons to generate a notification.
- Notification type--The type of notification to send: SNMP trap, e-mail, and Syslog.
- Notification recipients--Hostnames and ports for system that listen for SNMP traps or Syslog messages; or e-mail addresses.
- Daily subscription activity period--The hours during which Operations Manager should use this subscription while monitoring the alerts and events for which to send notifications.

An extremely helpful feature in OM is to have each subscription configured whether or not to send URLs that enable the recipient to open Operations Manager directly to the relevant page of information. This can be enabled using the checkbox illustrated above.

The last step in the Wizard-based dialog, not shown, is a summary of your notification criteria configuration.

Hyperlinks to Tools in Email Notification
Based on Event and Device Types



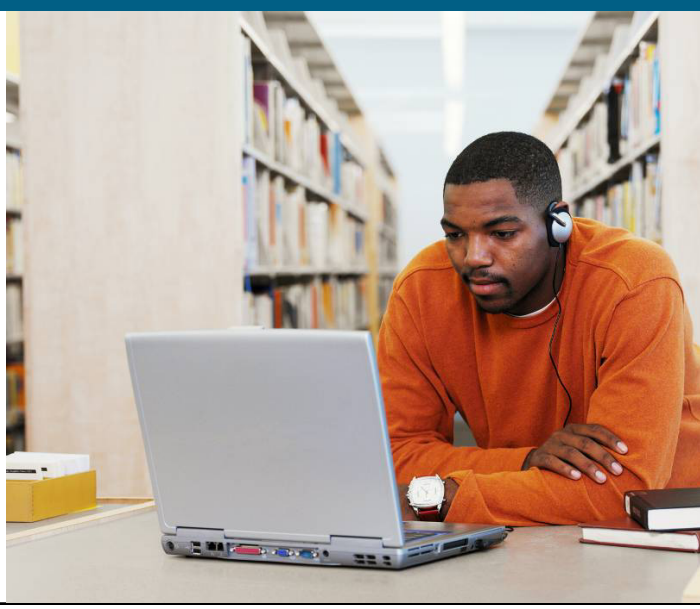
Hyperlinks to Tools in Email Notification

As seen in the Wizard Step 2, there is a checkbox called, **Include Link to Notification Details**. If selected, the notification will include a link back to Operations Manager for more details. This topic illustrates an example of an email notification that contains hyperlinks to more details in Operations Manager.

<*Intentionally Blank*>

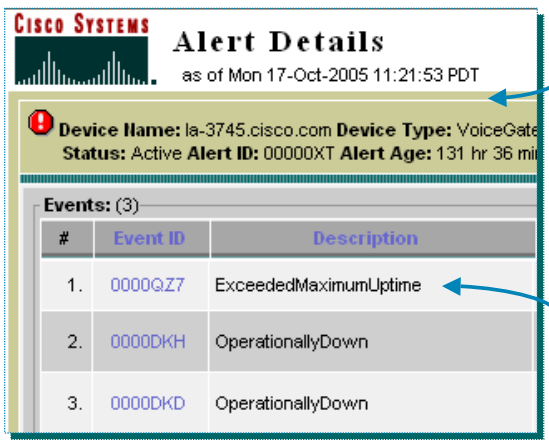
Customization / Advanced Features

- Operational Status Views
- Diagnostic Tests
- Inventory Management
- Reports
- Event Notification
- **Customization / Advanced Features**



Customize Event Names / Severity Levels
Overview

Customizing Events - Optionally, change event descriptions that are more meaningful to you or change the severity level of an event. These customized names will be reflected in both the Alerts and Events display and any Alert History reports you generate.



Event Descriptions appear in Notifications, the Alerts and Events display, and any Alert History reports you generate.

Customize Description

- What does Exceeded MaximumUpTime really mean?
- Maybe change description to: Dial-on-Demand uptime >7200 seconds

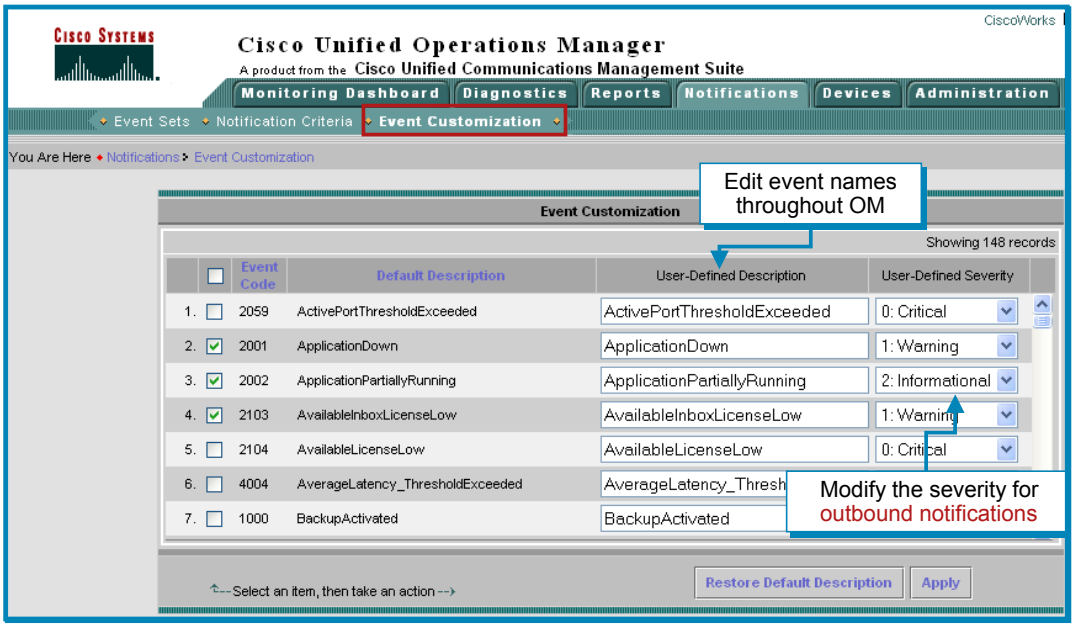
Customizing Event Names and Severity Levels

It might be helpful to make event names more descriptive for viewing in Operations Manager. This task will allow you to do this. When you customize an event description, the new description is reflected in all notifications--e-mail, SNMP traps, and syslog--and on all user interfaces.

When you customize event severity, it is reflected in all notifications--e-mail, SNMP traps, and syslog. Operations Manager uses only the event severity levels in the following table.

Severity Level	Value that Operations Manager Defines	Value That Operations Manager Writes to Notifications	
		E-Mail and SNMP Traps	Syslog Messages
Critical	0	0	2
Warning	1	1	4
Informational	2	2	6

Customize Event Names / Severity Levels
Notifications>Event Customization



Customizing Event Names and Severity Levels

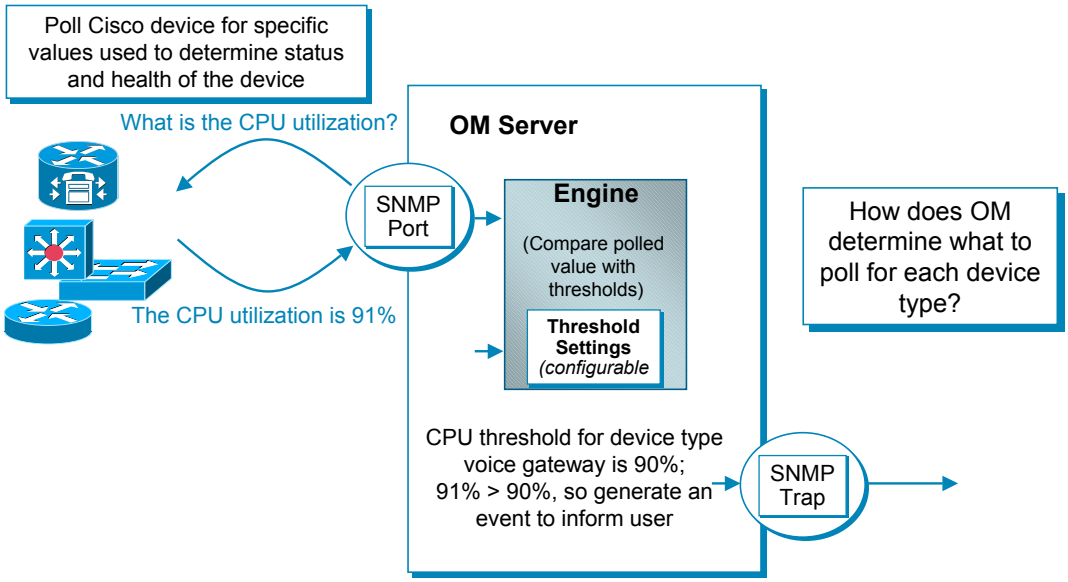
Changing the default event description or severity level of an event is easy! From the Notifications tab, click on Event Customization. Then just select the event checkbox that you wish to customize; change the description or severity level; then click Apply.

You can specify a customized event severity level between 0 and 7. When generating traps, the severity level you specify for the event is stored in the CISCO-EPM-NOTIFICATION-MIB and is sent in all notifications.

Note(s):

- When you customize event severity, Operations Manager continues to process the event based on its default severity. Also, severity levels 3 through 7 are undefined in Operations Manager.
- You can quickly and easily restore the default name and severity for any and all events.

Polling Parameters and Thresholds
Overview

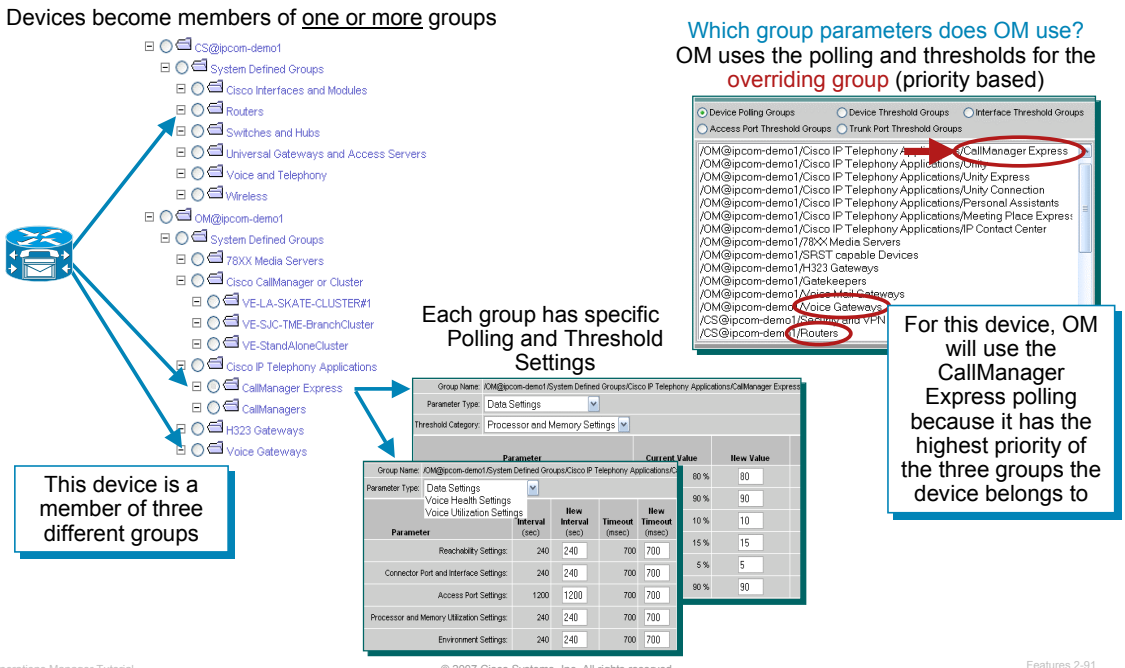


Polling Parameters and Thresholds - Overview

Operations Manager polls all active devices in its inventory. Operations Manager has the knowledge about each device, in particular, its device type. For each device type, specific parameters relative to that device type or group is polled from the MIB (Management Information Base) of the device. When a device is polled, Operations Manager receives the data on many parameters. This data is compared against pre-defined threshold values. If the thresholds have been exceeded, or values have fallen below acceptable levels, Operations Manager generates the appropriate events.

So, how does Operations Manager determine what parameters to poll for each device type? Let's discuss this next.

Polling Parameters and Thresholds
Which Polling/Threshold Parameter to Use?



Which Polling Parameters and Thresholds to Use?

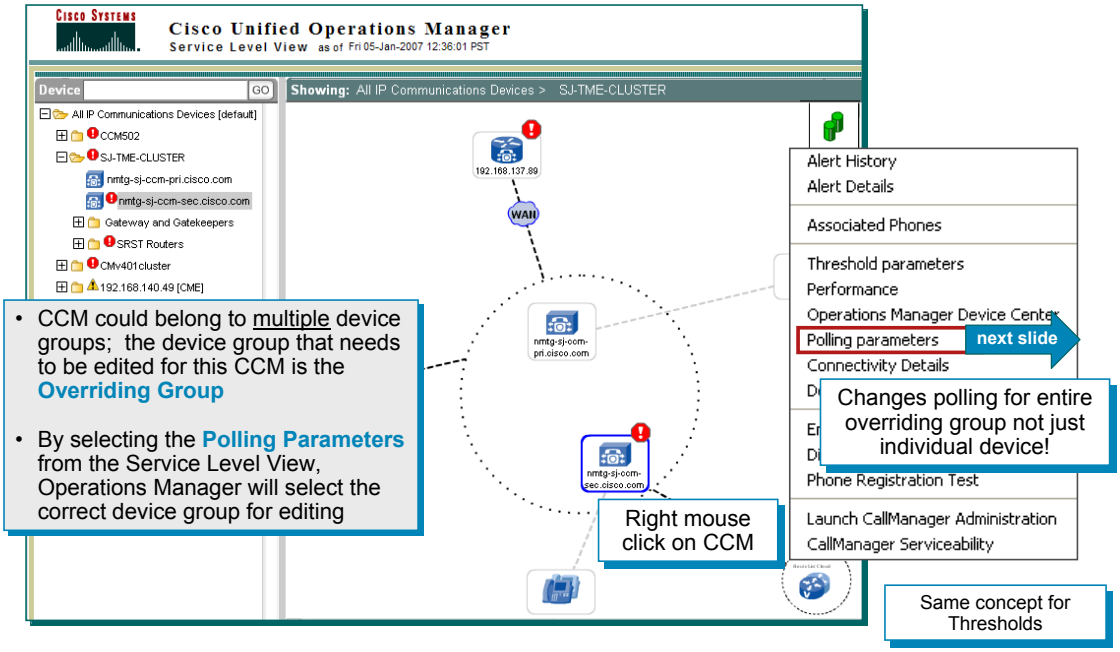
So, how does Operations Manager determine what parameters to poll for each device type? When devices are put into the Operations Manager inventory, they are placed into groups based on information collected from them. These groups may be device, function, or application based. In fact, many devices become members of more than one group.

Each group has been pre-assigned both a polling group indicating what data to retrieve and how often, and a threshold group, which provides the minimum acceptable value for the retrieved data. So a device is polled based on the polling parameters assigned to the group that they belong to. So what happens when a device belongs to multiple groups; which group parameters are used? Operations Manager provides a priority hierarchy for the polling groups. The group with the highest polling group priority becomes the *Overriding Group* for the device.

In the example above, a device belongs to the router group, CallManager Express, and gateway group. Looking at the polling group priority hierarchy, we can see that the CallManager Express polling group has the highest priority; therefore, the device will be polled according to the CallManager Express polling group.

This concept also exists for device, interface, access port, and trunk port threshold groups.

Polling Parameters and Thresholds
Polling Parameters



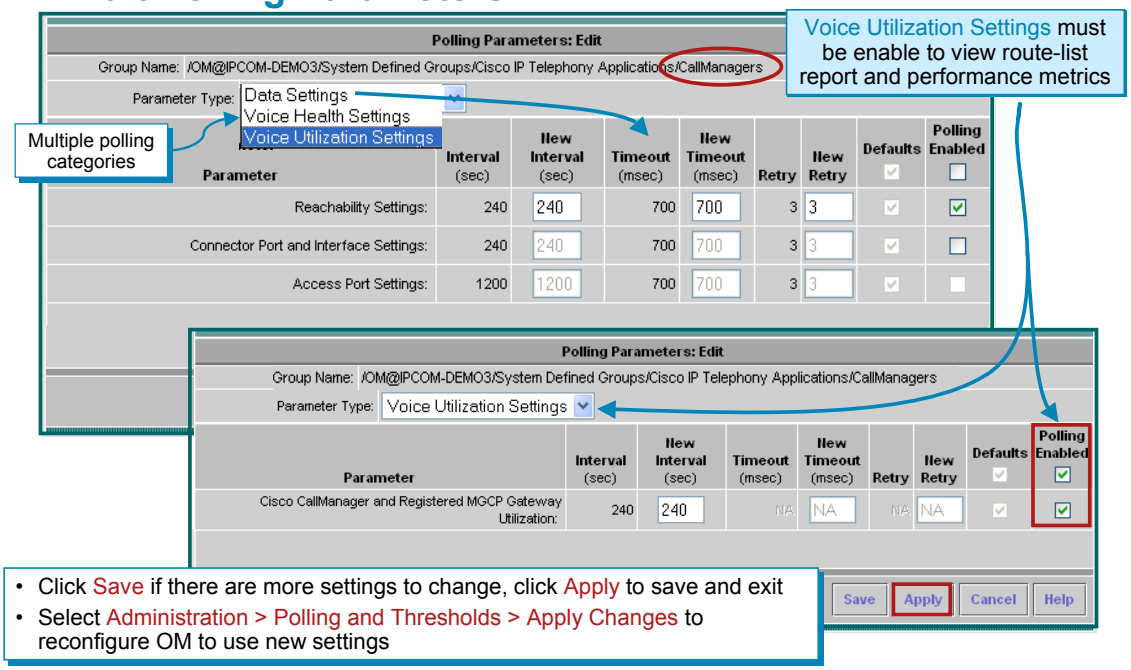
Polling Parameters

A device is polled based on the parameters of the *overriding* polling group. So how do you figure out the overriding group in case you wish to make modifications to the polling or threshold parameters? We can easily modify the polling parameters for the overriding polling group of a device by using the following steps:

1. From the Service Level View, find the device in question (either on the map or the navigation tree) and right click on it to bring up the context-sensitive menu.
2. Select **Polling Parameters**. (See next page.)

Polling Parameters and Thresholds

Edit Polling Parameters



Editing Polling Parameters

The Polling Parameters: Edit dialog for the device's overriding group is displayed. There are multiple categories of parameters selectable using the Parameter Type pull down list. Parameters can be enabled and the retrieval or polling interval can be modified.

This changes the polling parameters for all devices in this group not just the current device!

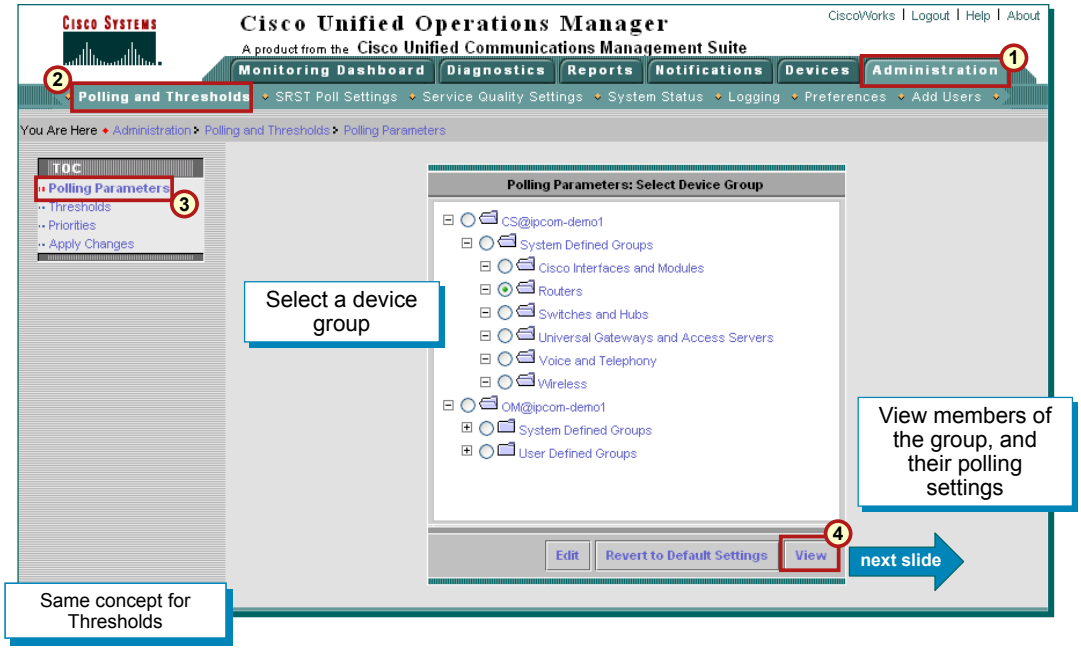
Click **Apply** to save the new settings

For the new settings to take effect, select **Administration > Polling and Threshold > Apply Changes**.

Changes to polling parameters and threshold values do not take effect until you apply changes, thereby reconfiguring Operations Manager to use the new values. Similarly, after you resume devices or device components that were suspended from polling, you must apply changes for the device elements to be polled.

TIP: To graph performance for CallManagers, the Voice Utilization polling parameter needs to be enabled. The Voice Utilization settings control polling for performance and capacity data and is disabled by default. Use these steps on "Editing Polling Parameters" to change the setting.

Polling Parameters and Thresholds
Viewing Group Members

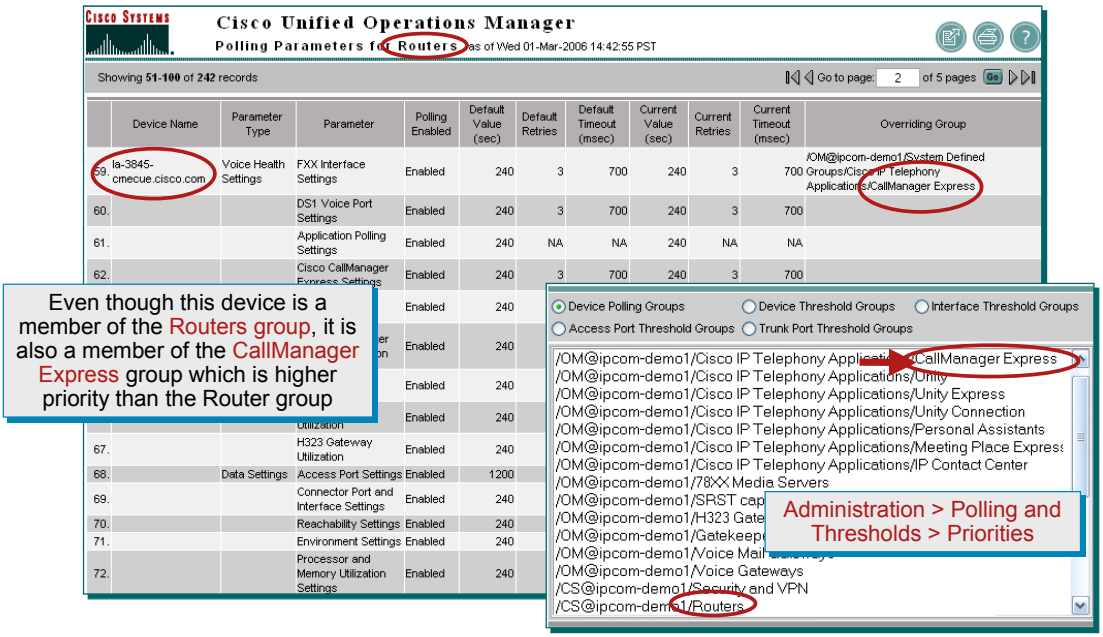


Viewing Group Members

To determine the members of a group, follow this procedure. It also proves useful in determining the overriding group for any of the group members.

1. From the Operations Manager desktop select the **Administration** tab.
2. Select the **Polling and Thresholds** option.
3. From the TOC select **Polling Parameters**. The Polling Parameters Select Device Group dialog is displayed.
4. Select a group from the navigation tree and click **View**. (See next page.)

Polling Parameters and Thresholds
View Group Members, (Cont.)

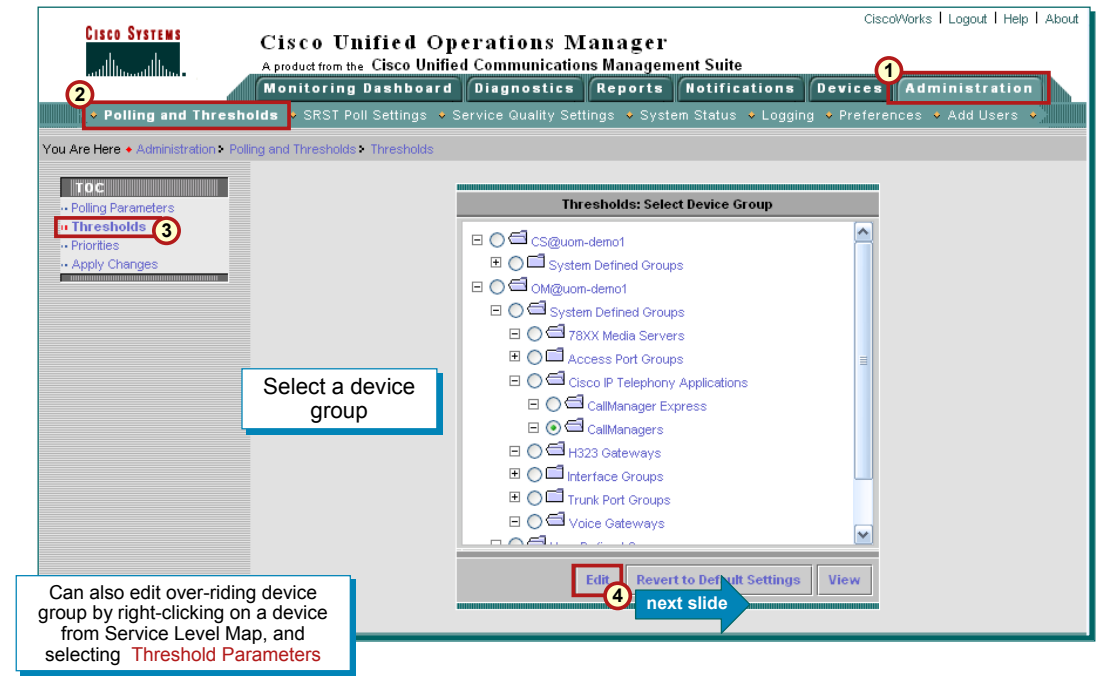


Viewing Group Members, (Cont.)

The polling parameters and group members for the selected polling group are displayed. (The example above, the *Routers* group was selected). It lists all members of the group as well as the polling parameters in use for the devices overriding group, which is listed in the far right-hand column.

The router circled in the figure above may be a member of the Router group, but is being polled using the CallManager Express polling parameters because it is also a member of that group and it has a higher priority than the router group. This can be seen in the last column called, *Overriding Group*.

Polling Parameters and Thresholds
Edit Threshold Settings



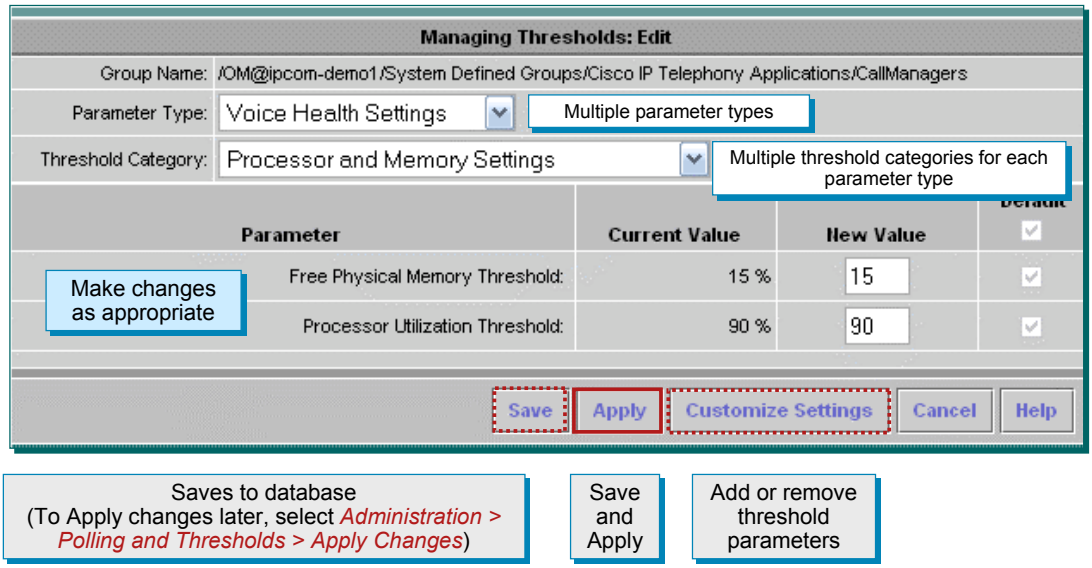
Edit Threshold Settings

These parameters determine when events should be generated based on the value of the attribute polled. The attributes are compared against the pre-defined acceptable threshold values.

Thresholds are also associated with device groups. To change the thresholds for a group use the following steps:

1. From the Operations Manager desktop, select the **Administration** tab.
2. Select the **Polling and Thresholds** option.
3. From the TOC select **Thresholds**. The Thresholds Select Device Group dialog is displayed.
4. Select a group to modify the thresholds for from the navigation tree and click **Edit**. (See next page.)

Polling Parameters and Thresholds
Edit Threshold Settings, (Cont.)



Edit Threshold Settings, (Cont.)

The Managing Thresholds: Edit dialog is displayed. There are multiple Parameter Types that can be selected using the pull down menu. And for each parameter type, there are multiple Threshold Categories. When you edit thresholds, the values that you update are associated with groups, not with individual devices, ports, or interfaces. Simply find the threshold category and then the threshold to change. Review the current value and then make your change. Click **Apply** to save your changes.

You can selectively disable threshold settings by clicking on the **Customize Settings** button. From here, Operations Manager will illustrate the variables that are currently being monitored against threshold settings and other variables that are not being monitored against threshold settings. Operations Manager allows the user with the appropriate user role to allow or discontinue monitoring against the thresholds.

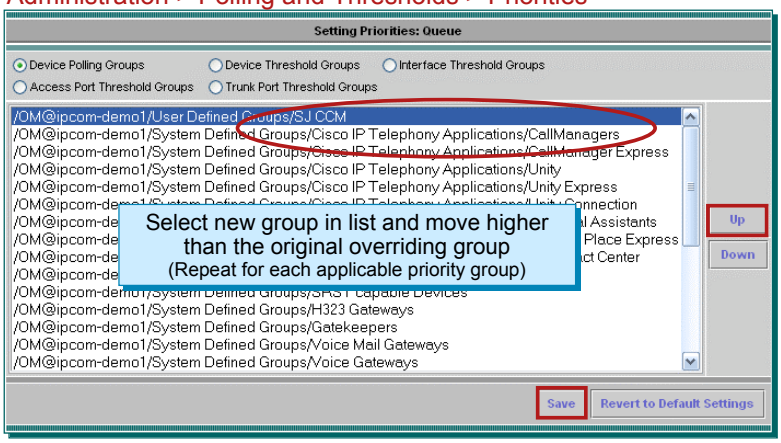
Before the changes take effect, you must select the **Administration > Polling and Thresholds > Apply Changes** task.

Polling Parameters and Thresholds
Creating New Polling/Threshold Groups

1. Create User-defined group for the CallManagers to monitor differently *(i.e. Call Managers in San Jose)*
2. Modify polling parameters for new group
3. Modify Threshold Parameters for new group
4. Make new group's priority higher than the regular CallManagers group and save changes
5. Apply changes (*Administration > Polling and Thresholds > Priorities*)

What if you want to monitor certain CallManagers differently than others?

Administration > Polling and Thresholds > Priorities



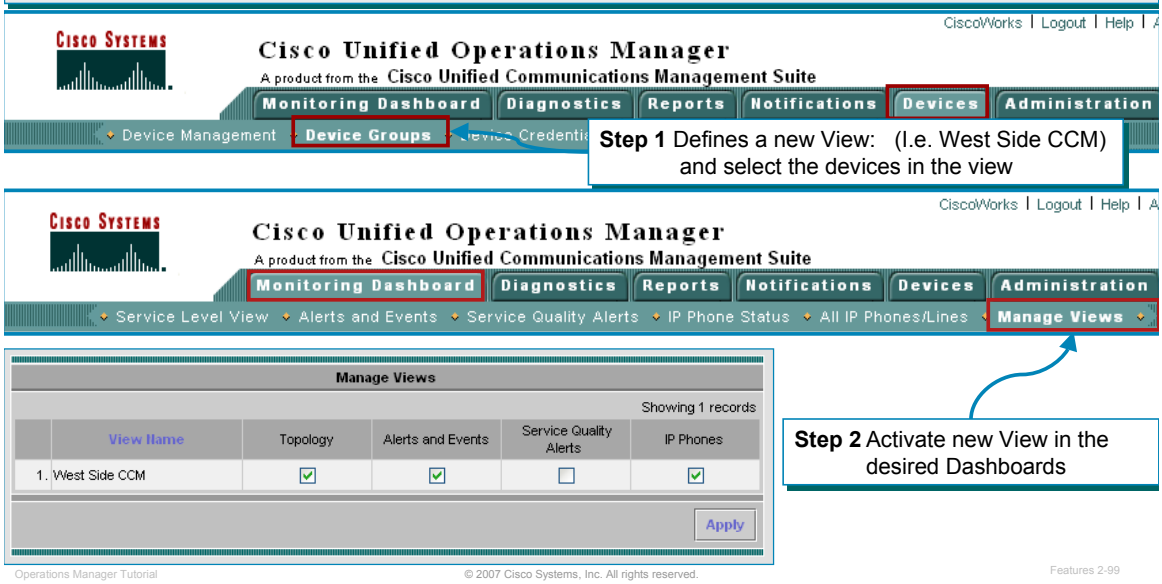
Creating New Polling / Threshold Groups

In many cases, the existing polling and threshold values for a group are adequate. But what happens when you wish to monitor a subset of the devices in a given group differently? For example, you wish to more frequently poll and change the thresholds for only the San Jose CallManagers and still monitor the remaining CallManager with the default CallManager values. This can be achieved by simply creating a user-defined device group that contains just the San Jose CallManagers. (Creating user-defined device groups were discussed in an earlier lesson.)

1. Create a new device group
2. Use the **Administration > Polling and Thresholds > Polling Parameters** task to select the new device group and modify its polling parameters.
3. Use the **Administration > Polling and Thresholds > Thresholds** task to select the new device group and modify its threshold parameters.
4. At this point the devices will still be polled using its old group polling parameters. To use the newly modified parameters, use the **Administration > Polling and Thresholds > Priorities** task to select the user-defined group and move it up the list until it is above the old polling group entry. This will give it higher priority. **Save** changes.
5. Apply the changes to have them take effect using the **Administration > Polling and Thresholds > Apply Changes** task.

Custom Dashboard Views
Overview

Step 1: First, create a new user-defined device group (ex: “West Side CCMs”) from *Devices>Device Groups*
Step 2: Secondly, activate the device group as a view in one or more dashboards



Custom Dashboard Views - Overview

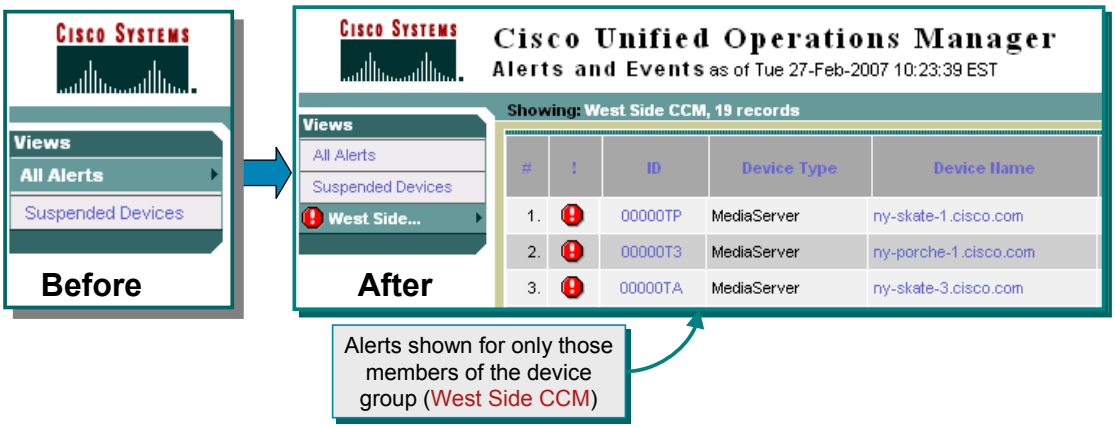
As you as seen throughout this section, views are logical groupings of devices that appear in the Monitoring Dashboard displays (Service Level View, Alerts and Events, Phone Activities, and Service Quality Alerts). There are two default views: **All Alerts** and **Suspended Devices**. These views are static and cannot be edited, deactivated, or deleted. The Service Level View display contains the **All IP Communications Devices** view, which is a default view that cannot be edited, deactivated, or deleted.

Once you decide how you want to cluster your devices into a logical set, create a new User Defined Group in the **Device> Device Groups** menu, and a new corresponding view is created.

Use the **Monitoring Dashboard> Manage Views** menu to create and activate a view of these device groups so they are shown in the Monitoring Dashboard displays. View elements are not shown until the view is activated and is displayed in the view pane (normally every two minutes).

The Monitoring Dashboard displays can have a maximum of 18 active views.

Custom Dashboard Views
Using New Dashboard Views



Custom Dashboard Views - Using New Dashboard Views

The result of creating and activating a new device view illustrated above. This creates an easy to way organize the wealth of information provided by Operations Manager!

<*Intentionally Blank*>

Thank You!

Continue on to Chapter 3 to use the many features of Operations Manager.

Cisco Systems

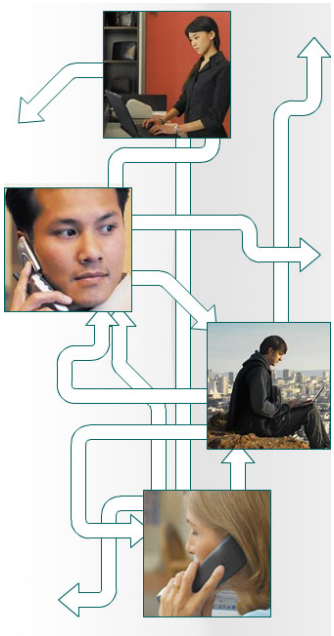
Cisco Unified Operations Manager

Usage Scenarios

Chapter 3

Chapter 3 Outline
Scenarios

1. Getting Started
2. Preparing OM for Initial Use
3. Normal Operational Status
4. Service Availability Testing
5. Node-to-Node (IP SLA) Testing
6. Experiencing Phone Outages
7. Performance Monitoring



Chapter 3 Outline

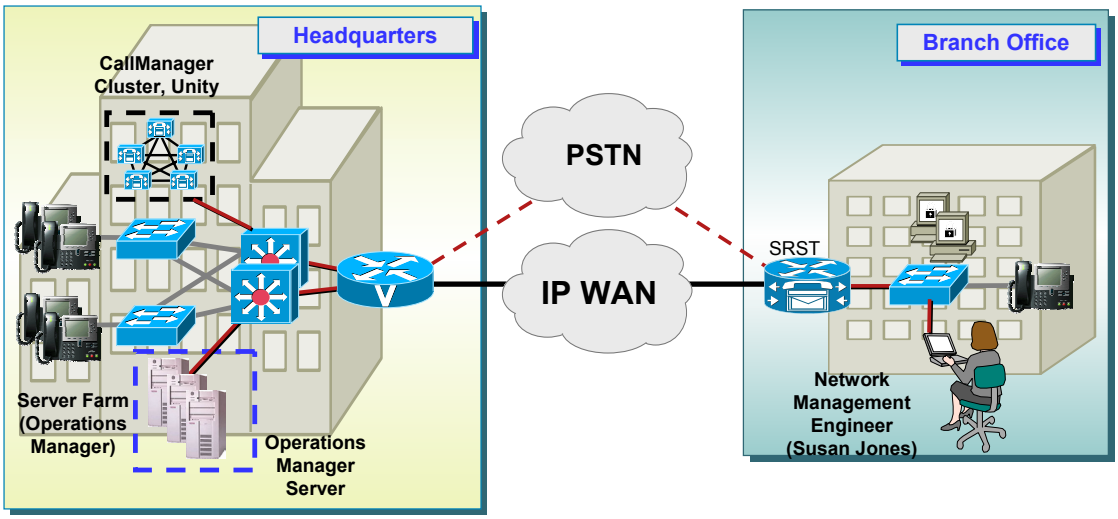
As seen in the previous chapter, Operations Manager provides a unified view of the entire Unified Communications infrastructure and presents the current operational status of each of the elements of the Unified Communications deployment. It continuously monitors the current status of different Unified Communications elements such as Cisco® CallManager, Cisco Unity®, Cisco®, CallManager Express, Cisco Unity Express, Cisco IP Contact Center elements, gateways, routers, and phones and provides different diagnostic tools for faster trouble isolation and resolution. It monitors and evaluates the current status of both the Unified Communications infrastructure and the underlying transport infrastructure in the network.

In this chapter, several scenarios will be presented detailing the steps required to configure and effectively use the different features in Operations Manager.

The first couple of scenarios go through the steps to prepare the network devices and the Operations Manager application for initial use. Thereafter, the scenarios look at common situations for using many of the features described in Chapter 2.

To enhance the effectiveness of the chapter as a learning resource, the reader is encouraged to follow along on an operational system, and to explore the other function options not covered by this tutorial. It would also be wise to view the help screens associated with all functions to better understand the many different options available for most tasks. Launch help by selecting the *Help* link in the upper right-hand corner of the application desktop. The help is content sensitive.

Network Description for Scenarios
Company ABC



Network Description – Company ABC

To help facility the reader's understanding of the setup and use of Operations Manager, the scenarios will follow the deployment of Operations Manager in a fictional company – Company ABC.

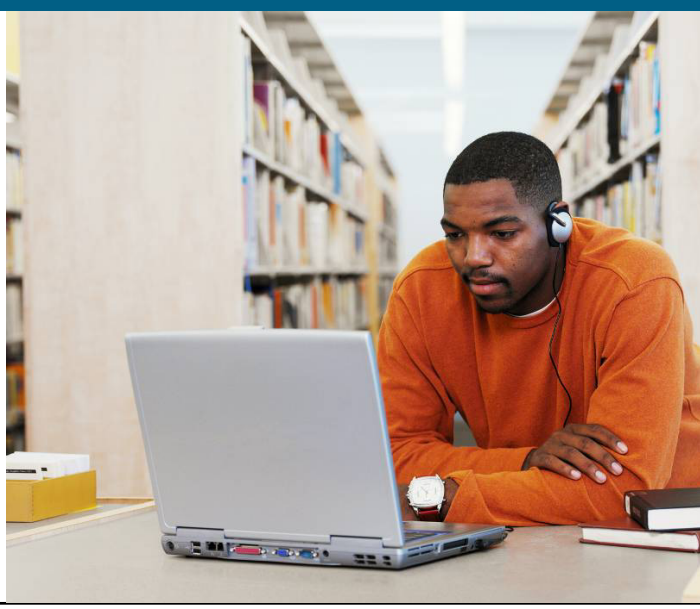
Company ABC has recently adopted Cisco's strategy for converging voice, video, and data onto a single network infrastructure using the Cisco AVVID (Architecture for Voice, Video and Integrated Data). Company ABC is also considering using several other CiscoWorks products such as: LAN Management Solution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

Company ABC wishes to protect their investment by monitoring and evaluating the current status of both the Unified Communications infrastructure and the underlying transport infrastructure in the network. The lead network engineer for Company ABC, Susan Jones, has been tasked with the deployment and use of Operations Manager. So let's peek over Susan's shoulder as she goes about her assignment.

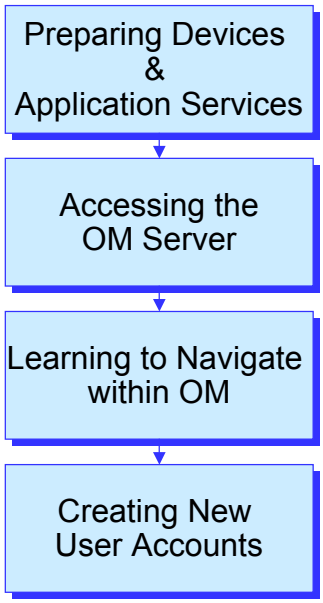
<Intentionally Left Blank>

Getting Started

- **Getting Started**
- Preparing OM for Initial Use
- Normal Operational Status
- Service Availability Testing
- Node-to-Node (IP SLA) Testing
- Experiencing Phone Outages
- Performance Monitoring



Scenario 1: Getting Started
Outline



Getting Started

In this first scenario, Getting Started, we provide the basics required to begin using Operations Manager (OM)– server access, navigation, creating user accounts, as well as important steps for preparing the devices to be managed using Operations Manager.

Prior to trying to manage the devices with the Operations Manager server, the user should first ensure that the devices have been properly configured and that the network allows for network management traffic to pass from the devices to the Operations Manager server.

The user will also learn how to access the server and learn the basic layout and navigation of both the Operations Manager homepage and its desktop.

The final step in this first scenario will show how to create a local user account and assign the user to one or more roles which allow specific privileges within Operations Manager.

Note(s):

For additional details, a link to the Operations Manager Deployment Guide can be found in Chapter 5 of this tutorial.

Getting Started
Preparing Devices for Management

Reachability

- Devices to be managed must be reachable from Operations Manager using ICMP, SNMP, HTTP, and WMI

Accessibility

- Operations Manager uses various access methods (*credentials*) to obtain device attributes and status
- Credential Types:
  - SNMP v1/v2 – Configure SNMP community strings (ro, rw) on the device
  - SNMPv3 (optional) – Configure username / pwd / encryption algorithm on the device
  - HTTP/S (CCM) – HTTPS uses SSL (Secure Socket Layer)
  - WMI (Windows Management Instrumentation) Credentials

Preparing Devices for Management

Before Operations Manager can function correctly, the network devices they interact with must be set up correctly. Operations Manager uses open interfaces such as Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), and Windows Management Instrumentation (WMI) to remotely poll data from different devices in the network. It does not deploy any agent software on the devices being monitored and thus is non-disruptive to system operations. Operations Manager also utilizes ICMP ping and the Cisco Discovery Protocol (CDP) to discovery the network devices.

Note: Ensure that your devices meet these requirements.

1. In order for devices to be managed using Operations Manager, they need to be reachable from the Operations Manager server using ICMP Ping, SNMP, and HTTP. Ensure that firewalls are not blocking these protocols from the Operations Manager server to the devices.
2. Operations Manager uses Simple Network Management Protocol (SNMP) to read and write information from and to the MIBs located on the devices. If the information is not available in the MIB, Operations Manager utilizes HTTP to obtain the information from the html code and XML. SNMP v1/v2 or SNMP v3 (AuthNoPriv mode) are supported. The following defines how to configure SNMP on the devices; these values must also match those defined in Operations Manager. (Refer to Scenario 2 for configuring Operations Manager.)

Preparing Devices for Management, continue …

To enable SNMP v3 on **Cisco IOS devices**, follow these steps

Step 1 Create a view.
snmp view campus 1.3.6.1 included nonvolatile

Step 2 Set the security model.
snmp access cmtest security-model v3 authentication read campus write campus nonvolatile

Step 3 Create a user and specify the authentication protocol to be used.
snmp user cmtester authentication md5 cisco123

Step 4 Create a group and associate the user with it.
snmp group cmtest user cmtester security-model v3 nonvolatile

To enable SNMP v3 on **Catalyst OS devices**, follow these steps:

Step 1 Create a view.

set snmp view campus 1.3.6.1 included nonvolatile

Step 2 Set the security model.

set snmp access cmtest security-model v3 authentication read campus write campus nonvolatile

Step 3 Create a user and specify the authentication protocol to be used.

set snmp user cmtester authentication md5 cisco123

Step 4 Create a group and associate the user with it.

set snmp group cmtest user cmtester security-model v3 nonvolatile

To enable SNMP v1 or v2c on **Cisco IOS devices**, follow these steps:

Step 1 **snmp-server community** <*read-community-string*> **ro**

Step 2 **snmp-server community** <*write-community-string*> **rw**

To enable SNMP v1 or v2c on **Cisco Catalyst OS devices**, follow these steps:

Step 1 **set snmp community read-only** <*read-community-string*>

Step 2 **set snmp community read-write** <*write-community-string*>

Getting Started
Preparing Devices for Management, (Cont.)

Configuration

- SysName must be unique
- Define one interface IP address as the network management interface
- Enable CDP for discovery of neighboring devices (ICMP ping is also used for discovery of network devices; allow ICMP ping across the network)
- If desired, configure devices to send traps to Operations Manager for display in the Alerts and Events view (required for OM management of most UC application servers)

Preparing Devices for Management, (Cont.)

1. The system name must be unique on every Cisco IOS device for network services to discover all Cisco IOS devices on the network.
   - To set the sysName variable on a Cisco IOS device, use the following global configuration command:

     hostname <name>
   - To set the sysName variable on a Cisco Catalyst OS device, use the following global configuration command:

     set system name <name>

2. For Cisco IOS and Cisco Catalyst devices, one of the interface IP addresses must be designated as the management IP address and it must be defined as a loopback IP address.

Preparing Devices for Management, continue …

3. The Cisco Discovery Protocol (CDP) discovers neighboring Cisco devices on the interfaces that have CDP enabled. The CDP table can then be read by Operations Manager to learn information about neighboring devices, and to send SNMP queries to those devices.

   CDP is enabled on Cisco IOS devices by default; otherwise, to enable CDP capability on IOS devices use the following commands.

   - To enable CDP globally: cdp run
   - To enable CDP on specific interfaces only: cdp enable
   - Use the no command to disable CDP capability on Cisco IOS devices.

   CDP is enabled on Cisco Catalyst OS devices by default. To enable CDP capability on Catalyst OS devices use the following commands.

   - To enable CDP globally: set cdp enable
   - To enable CDP on specific ports only: set cdp enable [*all* | *mod/port*]
   - To disable CDP on Catalyst OS devices: set cdp disable

   Use the *all* parameter to enable CDP on all ports on the device, or enter a specific module and port numbers. A range of ports can also be entered. For example: set cdp enable 2/1-10,3/5-1

   Do not run CDP on links that you do not want discovered, such as Internet connections and end-host connection ports on access switches. To protect from CDP DoS attacks, do not enable CDP on links that are connected to non-Cisco devices.

4. Set a domain name on a Cisco IOS or a Catalyst OS device by using the following commands:

   Cisco IOS Devices : ip domain-name <*name*>

   Cisco Catalyst OS Devices: set system name <*name with domain name*>

5. The event notification system in Operations Manager can report on SNMP traps received, or forward to them from another event notification/reporting system. In these examples for enabling traps, the community string “public” helps selective processing of traps on the trap-receiving side.

   To enable traps in Catalyst OS devices to be sent to a particular host, such as the Operations Manager server, enter this command:

   set snmp trap <*ip address of receiving host*> public

   To enable traps in IOS devices to be sent to a particular host , such as the Operations Manager server, using SNMP v2c, enter this command:

   snmp-server host <*ip address of receiving host*> traps version 2c public

6. Some information in the Cisco CallManager or CallManager Express (CCM/CME) is not available in a MIB and cannot be retrieved using SNMP. In this case, the information is obtained using HTTP. The information is extracted from the html code using XML. The Cisco IOS HTTP server provides authentication, but not encryption, for client connections. The Secure HTTP (HTTPS) feature provides the capability to connect to the Cisco IOS HTTPS server securely. It uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

   Use the following command to enable http mode: ip http server

Getting Started
Preparing Devices for Management, (Cont.)

Media Convergence Servers (MCS)

- Verify that the appropriate services are installed for HP Insight Manager and IBM UM Services

Cisco CallManagers (CCM)

- OM uses the AVVID XML Layer (AXL) queries in addition to SNMP to manage CCM. This requires HTTP/S username/password configuration to execute these queries (Same credentials as used for CCM Administration page)
- OM relies on the cluster name of a CCM cluster to uniquely identify and manage a CCM deployment
- Release 4.1 and 4.2 allows for secure communications between OM and CCM using SSL. (enable SSL on the CCM and specifically certain virtual directories)

Cisco CallManagers Express (CME) and SRST

- Download the latest Speedbird IOS MIBs

Cisco Unified Contact Center and Cisco Unity

- The appropriate Remote Serviceability Kit (RSK) must be installed for CUOM to manage them properly
- WMI credentials, which are used as the Windows username and password, must be defined in the Discovery Credentials page

Cisco Unity Express (CUE)

- Add IP address of Unity Express device to CUOM server as if it is a separate device. Cisco Unity Express (CUE) has its own SNMP agent and management IP address.
- To manage the CUE, the latest CUE version (Speedbird) must be used and SNMP RO community strings must be configured.

Preparing Devices for Management, continue …

As shown in the figure above, some of the Unified Communications applications and their hosts have specific requirements as well.

Getting Started
Preparing Network Services

General Services

- Domain Name Resolution
  - Domain name resolution is used for numerous operations in Operations Manager and if the name lookup is slow or does not exist, Operations Manager will appear slow
  - Operations Manager server must be DNS resolvable
- Network Time Protocol
  - To be able to correlate events across multiple devices, the devices need to have the same perception of the time
- Port Availability
  - Many TCP and UDP ports are used to transfer network management traffic. These ports can not be blocked.

Cisco Unified Service Monitor Additional Services (if installed)

- DHCP Server
  - Provides addressing and TFTP server address to Cisco 1040 Sensors
- TFTP Server
  - Provides Cisco 1040 Sensors image and configuration file

Preparing Network Services

Domain name resolution helps make management much easier - humans are much more adapt at using names as opposed to addresses. Numerous functions within Operations Manager also rely on domain name resolution. To avoid potential performance issues, make sure the servers can resolve hostname lookups using either DNS or other method.

Since much of the reporting in Cisco Unified Operations Manager and Service Monitor is used to correlate events, it is important to ensure that the server and devices are time synced using the Network Time Protocol (NTP).

If using Operations Manager through a firewall, ensure that the appropriate ports are opened to transfer management information. A list of the used ports can be found in the installation guide.

Typically, Service Monitor may also be installed in your network and integrated with Operations Manager. Service Monitor also uses two other network services: DHCP and TFTP. DHCP is used to provide addressing to the Cisco 1040 sensors. The DHCP server also provides the sensors with the TFTP server address where the 1040s will retrieve their configuration and image files. The TFTP server stores and provides the Cisco 1040 sensors with their configuration and image file.

(The Service Monitor Tutorial will discuss in detail the setup of Service Monitor and the Cisco 1040 sensors.)

Getting Started
Operations Manager Server Access

- Microsoft Internet Explorer 6.0.28 or 6.0.37
- Adobe Macromedia Flash Player 8.0 or higher
- JavaScript and Cookies enabled required
- Disable Pop-up blockers
- Add server to list of Trusted Sites
- Check Release Notes for changes to requirements

Server Access

Accessing the Operations Manager server is easy! Simply launch Microsoft's Internet Explorer and enter the hostname or IP address of the Operations Manager server followed by the http port being used (port 1741 is used by default during installation) as a URL address:

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

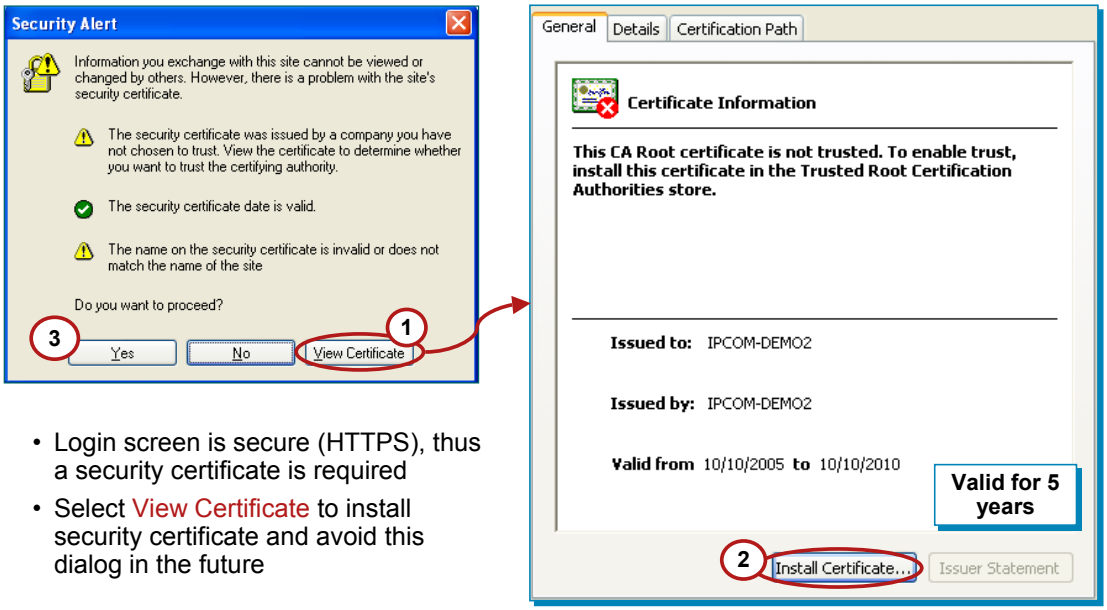
The login to the Operations Manager server is performed as a secure transaction, using HTTPS. Follow these steps to understand the security dialogs and get to the login screen:

1. Prior to being redirected to a secure page displaying the login banner, a pop-up Security Alert is displayed informing you of a Security Alert. To simply continue, select *Yes* or continue to the next step.
2. Optional step: The Security Alert will continue to be presented at each subsequent login until the user installs the certificate by selecting *View Certificate*.

   In doing so, the Certificate dialog will be displayed; select *Install Certificate* and follow the instructions presented. When finish select *OK* in the Certificate dialog, and then *Yes* on the Security Alert window.
3. Optional step: Using the *Tools>Internet Options> Security* dialog of Internet Explorer, add the Operations Manager server as a Trusted Internet site. In doing so, the status bar on the bottom of the browser will be removed resulting in a better screen size for the OM dashboards and dialogs.

(Refer to Chapter 4 of this tutorial for complete client hardware and software requirements.)

Getting Started
Security Certificate



- Login screen is secure (HTTPS), thus a security certificate is required
- Select View Certificate to install security certificate and avoid this dialog in the future

Security Certificate

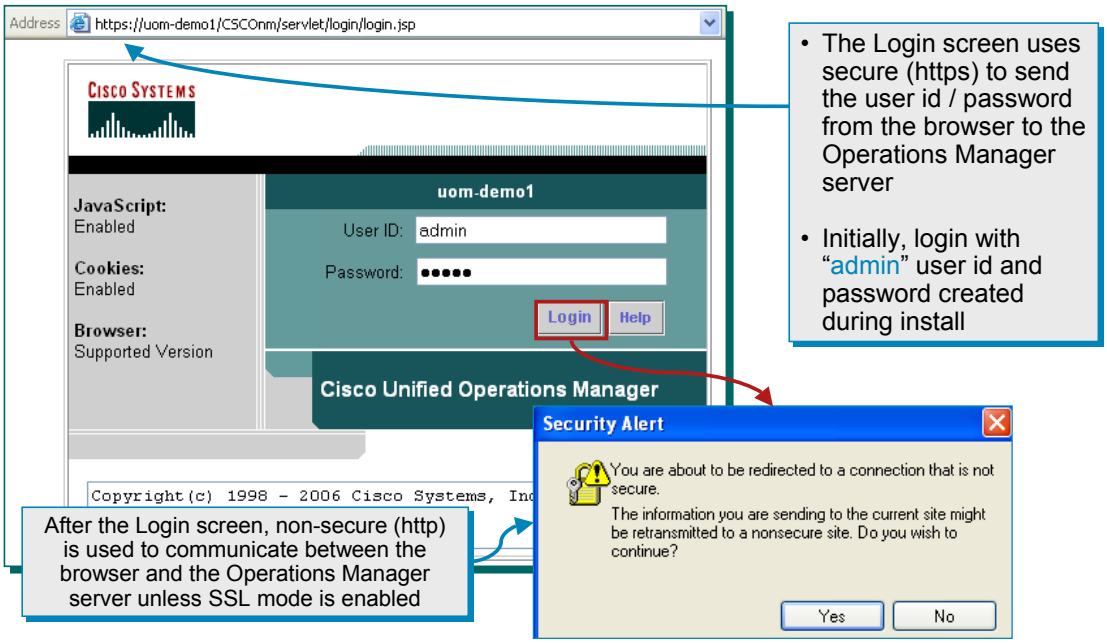
Viewing and Installing the Security Certificate is optional. The Security Alert will continue to be presented at each subsequent login until the user installs the certificate by selecting *View Certificate*.

In doing so, the Certificate dialog will be displayed; select *Install Certificate* and follow the instructions presented. When finished, select *OK* in the Certificate dialog, and then *Yes* on the Security Alert window.

Note(s):

- Additional optional step: Using the *Tools>Internet Options> Security* dialog of Internet Explorer, add the Operations Manager server as a Trusted Internet site. In doing so, the status bar on the bottom of the browser will be removed, resulting in a better screen size for the Operations Manager dashboards and dialogs.

Getting Started
Operations Manager Server Access

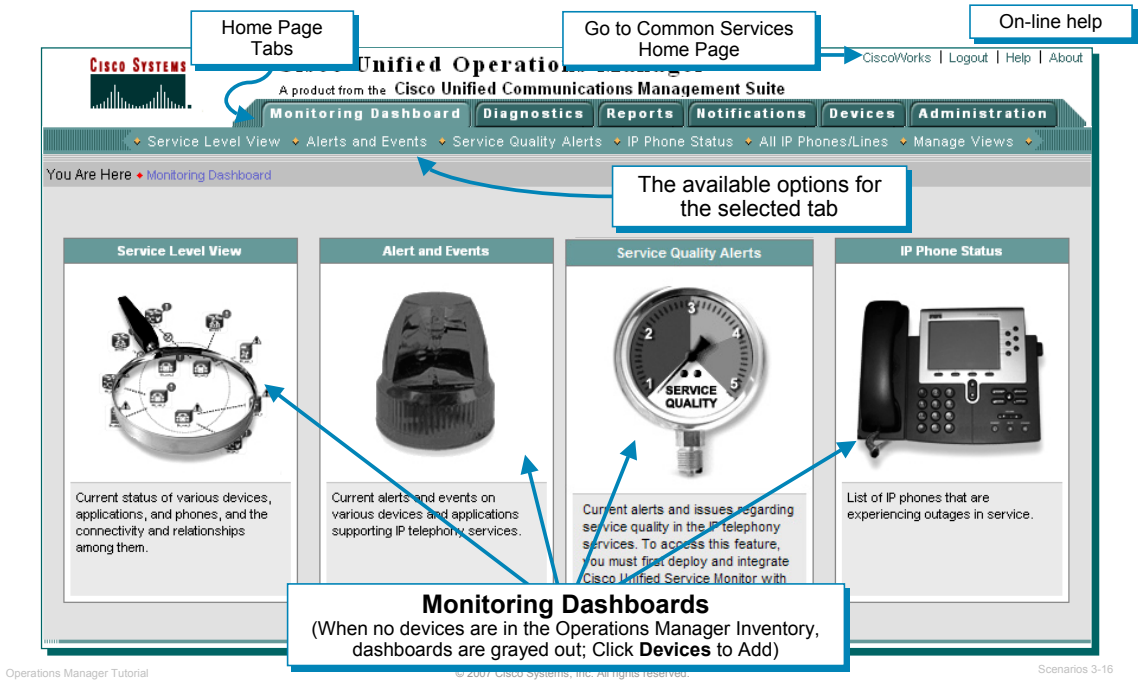


Operations Manager Server Access

If you have installed the Operations Manager server and are logging in for the first time, you can use the reserved "admin" username and password. To log in:

1. Enter ***admin*** in the Name field and the password set for admin in the Password field of the Login Manager. Contact the server administrator if you do not know the password for admin.
2. Click ***Login*** or press ***Enter***. You are now logged in. Login sessions time out after 2 hours of inactivity. If the session is not used for 2 hours, you are prompted to log in again.
3. To change the admin password or configure new users, select ***Administration > Add Users > Local User Setup*** from the Operations Manager menu. (This is described in more detail later in this scenario.)

Getting Started
Operations Manager Homepage



Operations Manager Homepage

After successful login authentication, the homepage for Operations Manager will be displayed. By default, the Monitoring Dashboard tab is selected; thus, the four dashboards can be immediately launched once the Operations Manager inventory is populated with devices. (If no devices exist in the Operations Manager inventory, all dashboards are grayed out.)

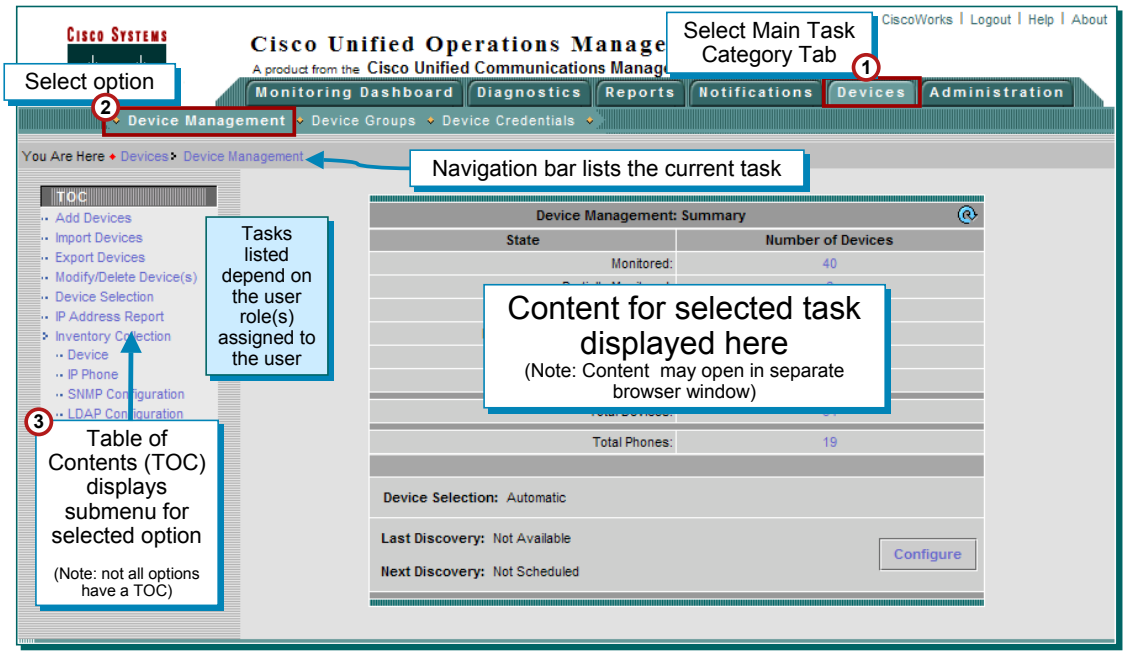
Also notice on the Operations Manager homepage, several important links in the upper right corner: CiscoWorks, Help, and About.

- The *CiscoWorks* link will take you to the Common Services homepage which provides links to services provided by Common Services. (A brief look at these services will be discussed shortly. However, also refer to the Common Services Tutorial for more information.)
- The *Help* link will open a new browser window and take to you an extensive on-line help system for Operations Manager.
- The *About* link will report on this software's running version.

Note(s):

- *The Operations Manager page is displayed as a non-secure operation (http). Optionally, access to the server can be secured using Secure HTTP (https) by enabling SSL in the Common Services. Refer the Common Services tutorial for more information.*

Getting Started
Menu Navigation - Layout



Menu Navigation - Layout

Prior to using Operations Manager, it would be beneficial to become familiar the basic layout to help you understand how to navigate through its menu system.

The main features of Operations Manager are accessible by selecting the appropriate tab. The currently selected tab is identifiable by the different color of the tab and its text. These tabs are the various categories of tasks in Operations Manager:

- Monitoring Dashboards – Allows the user to launch views to monitor Unified Communications services, Unified Communications alerts and events, service quality alerts, and IP phone status
- Diagnostics – Allows the user to setup IP phone status tests, synthetic tests to test CCM services, and Node-to-Node tests to test connectivity and response time
- Reports – Allows the user to view reports on the history of alerts and events, IP phone information and changes, installed Unified Communications applications, and create personalized reports
- Notifications – Allows the user to configure what events should create user notifications and how to notify the user
- Devices – Allows the user to manage the devices that are managed by Operations Manager
- Administration – Allows the user to refine the polling and threshold settings, change application preferences, add/change user accounts, and review log files or system status

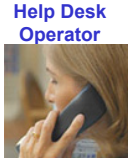
Immediately under the tabs are the tasks or additional sub-categories associated with the selected major task category. Notice that this bar is the same color as the selected tab helping to further identify which tab is selected. To select one of these options, simply click on it. The selected option will be in bold text. 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 Contents (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.

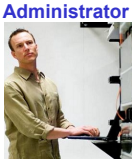
When the selected task has no further sub-tasks, a dialog box with further instructions or simply displaying the requested information will be shown in the content display area. To determine where the user currently is, the display line (appropriately titled “You Are Here”) under the tab options indicates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

Getting Started
Basic Security - Overview

- **Authentication**
  - A procedure to verify that a login (username and password combination) for a server or device is valid
  - Cisco Unified Communication servers provide local user accounts to validate login
  - Other external methods are available
- **Authorization**
  - Access rights (allowed services) are granted to a user based on their login id and their profile
  - Examples: view only, full access, limited services

Different people have different responsibilities and thus, should have different access levels





Basic Security – Overview

By default, Operations Manager uses the Authentication and Authorization mechanism provided by Common Services.

Authentications are performed against a local user database containing a username and associated password. This information is encrypted when sent between the client and the server.

When the user account is created, one or more user roles are associated with it. These user roles, as described next, dictate what tasks in Operations Manager or Service Monitor the user has authority to execute.

When a user is authenticated, the associated user roles assigned to him are then used for authorization purposes.

Getting Started
Authorization – User Roles

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

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

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

Authorization – User Roles

To allow for proper authorization of tasks, Operations Manager and Service Monitor employs the concept of User Roles (also known as user privileges or permissions).

. Many management 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.

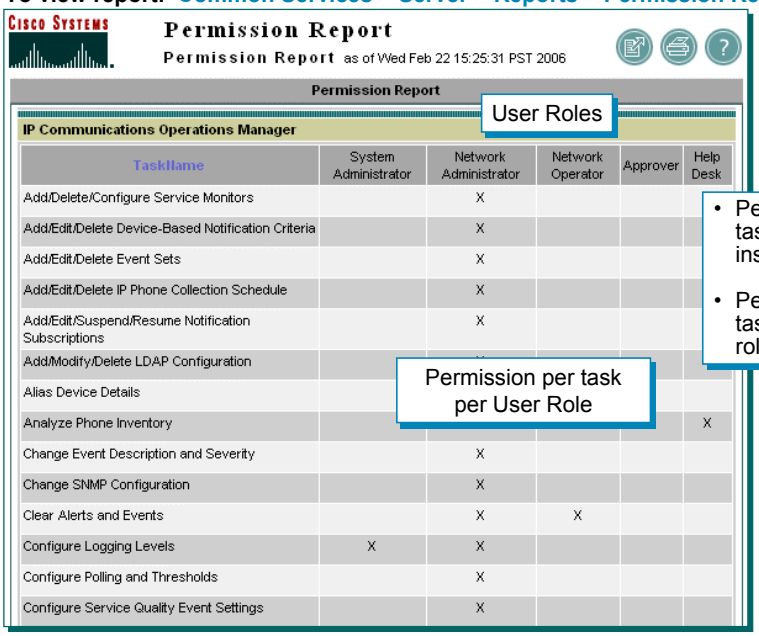
Use of the various functions or tasks within Operations Manager and Service Monitor is based upon the "roles" assigned to user accounts. In fact, if a task cannot be executed by a user role assigned to the logged in user, then that task will not even be displayed in the navigation tree of the application. Common Services 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

Users can be assigned more than one user role, and all are assigned the basic user role – Help Desk. The tasks allowed per user role are static and cannot be modified.

Getting Started
User Accounts - Permission Report

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



TaskName	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Add/Delete/Configure Service Monitors		X			
Add/Edit/Delete Device-Based Notification Criteria		X			
Add/Edit/Delete Event Sets		X			
Add/Edit/Delete IP Phone Collection Schedule		X			
Add/Edit/Suspend/Resume Notification Subscriptions		X			
Add/Modify/Delete LDAP Configuration					
Alias Device Details					
Analyze Phone Inventory					X
Change Event Description and Severity		X			
Change SNMP Configuration		X			
Clear Alerts and Events		X	X		
Configure Logging Levels	X	X			
Configure Polling and Thresholds		X			
Configure Service Quality Event Settings		X			

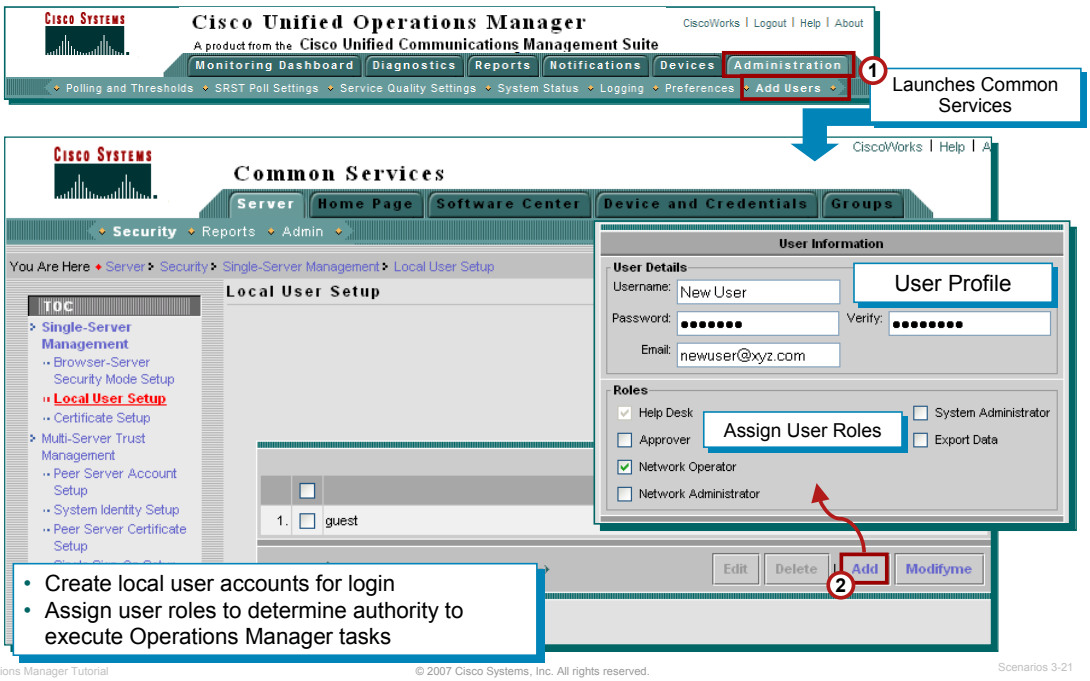
User Accounts - Permissions Report

Common Services includes a report that displays every task for every application on the local server and which user roles have permission to execute it. To view the Permissions Report, go to the Common Services homepage and select ***Common Services > Server > Reports***. From the dialog displayed, select ***Permissions Report*** and click ***Generate***.

Note(s):

- The tasks that are executable by a user role are static and cannot be changed unless the Operations Manager server is integrated with the Cisco Secure Access Control Server (ACS) product. Refer to the Common Services Tutorial or User Guide for more information on integrating with ACS.

Getting Started
User Accounts



User Accounts

Operations Manager allows users, such as the admin user account, with the System Administration user role to create new user accounts and assign user roles to the account.

Creating a new user is simple and straight forward. The underlying Common Services provide the security administration of user accounts. To create a new user account simply follow these steps.

- From the homepage of Operations Manager, select the ***Administration > Add User*** task.
- The previous step / task takes you to the ***Common Services > 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 user is to have. The E-mail address is optional for all user roles except for the role of Approver. (E-mail is how an application informs an Approver user of a job to approve – See the Resource Manager Essentials Tutorial or User Guide for more information about approving jobs.)

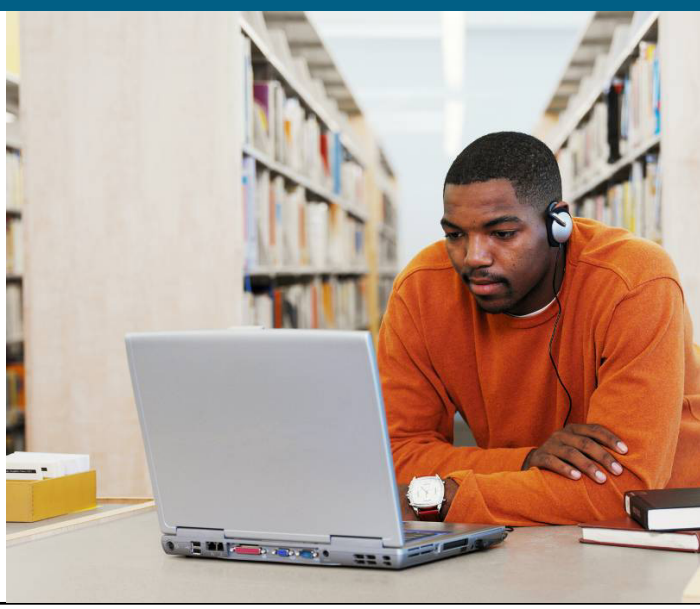
Note(s):

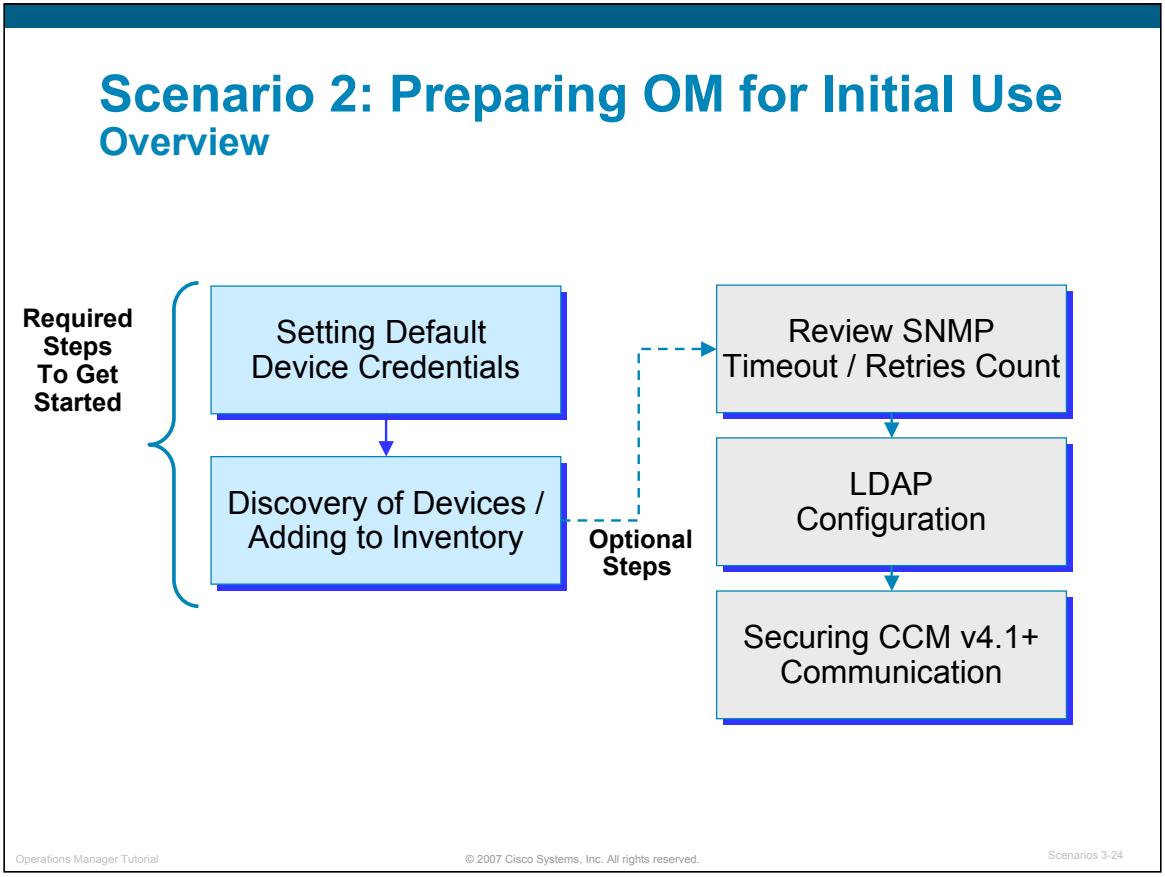
- *All users can view their account using the same task, except selecting **ModifyMe** instead of **Add**. Only the password and e-mail address can be modified by the user, unless they have the System Administrator user role.*

<Intentionally Left Blank>

Preparing OM for Initial Use

- Getting Started
- **Preparing OM for Initial Use**
- Normal Operational Status
- Service Availability Testing
- Node-to-Node (IP SLA) Testing
- Experiencing Phone Outages
- Performance Monitoring





Preparing OM for Initial Use

In the first scenario, the user prepared the devices to be managed, learned how to access and navigate within the Operations Manager server, and possibly created a new user account besides the default user account “admin” that was created during install.

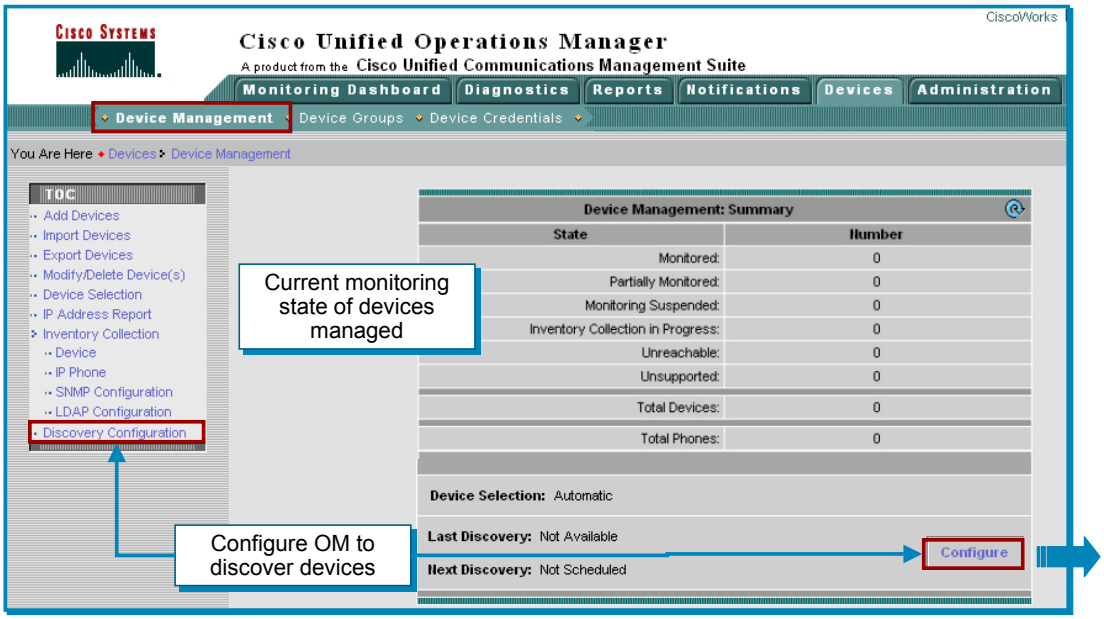
The second scenario, *Preparing OM for Initial Use*, provides the initial configuration steps that are needed in order for Operations Manager to begin monitoring the network.

As you will see in this scenario, before Operations Manager can begin to perform management activities, the following tasks must be performed:

1. The Device and Credentials Repository (DCR) must be populated with the devices to be managed. (*For more detailed information on what the DCR is and its relationship to Operations Manager, refer to Chapter 2 of this tutorial.*)
2. Next, in order for devices to be monitored by Operations Manager, they must be added from the DCR to the Operations Manager inventory.
3. Once the devices are in the Operations Manager inventory, Operations Manager can then be configured to begin monitoring the devices, and to discover and monitor IP phones.
4. Optionally, other settings, such as: the default SNMP settings for time-outs and retries, LDAP configuration, CCM v4.1 or later security certificates, and SNMP trap receiving and forwarding can be defined.

These configuration steps above will be described and illustrated in this scenario. So let’s begin!

Preparing OM for Initial Use
Discover Devices



Discover Devices

Discovering devices means to automatically add devices and their credentials to the DCR and then add them to the OM inventory for management:

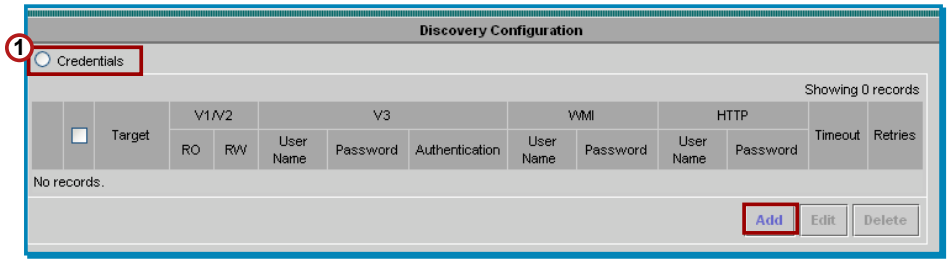
To configure the discovery settings, follow these steps:

1. From the Operations Manager desktop, select the **Devices** tab and then the option, **Device Management**. The Device Management Summary dialog is displayed.
2. To enter the discovery settings, select the **Configure** button or select **Discovery Configuration** from the TOC, as illustrated above. <Continued on next page>

Other methods to add devices to the DCR include the following. These methods will be discussed latter in this scenario.

- Manually – Use the Devices > Device Management > Add Devices task to manually add one or more devices to the DCR.
- Import – Use the Devices > Device Management > Import Devices task to import devices from a file (CSV or XML format) or a local NMS System (HPOV 6.x or NetView 7.x) or remote NMS system (HPOV 6.x, NetView 7.x, or ACS).

Preparing OM for Initial Use
Setting Discovery Credentials



- First, define discovery credentials for a single device or a group of devices
  - Credentials provide the access keys to pull device information
  - When a device is discovered, these credentials are used to pull the data from the device
  - Click Add one or more times to define the credentials for a single device or a group of devices
- Next, (after discovery credentials are defined), set the discovery methods and optional filters.

Setting Discovery Credentials

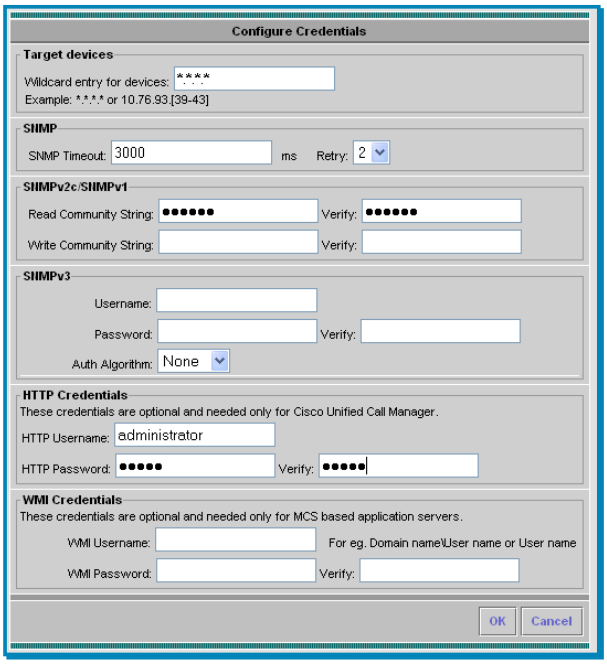
Device credentials provide the access keys to pull information from the device using SNMP, HTTP, or WMI. So when a device (IP address) is discovered, these credentials are used to pull the data from the device. These discovery credentials can be defined for a single device or a group of devices.

To define the discovery credentials for a single device or a group of devices, follow these steps:

1. From the Discovery Configuration dialog, check the radio button **Credentials**.
2. To add a new device credential definition or change one that is already defined for a single device or group of devices, click **Add**. The Configure Credentials dialog appears and is discussed next.

Preparing OM for Initial Use
Setting Discovery Credentials, continue …

- Define discovery credentials by defining the target: single device, multiple devices (separated by commas), subnets, or use wildcards and ranges
- Define SNMP timeout and retry for the target device(s)
- Define credentials for the target device(s)
  - SNMP v1/v2c (RO only needed for IOS devices)
  - SNMP v3
  - HTTP (only required to pull data from CCMs - data that can not be obtained using SNMP)
  - WMI (optional)- Windows credentials - MCS-based application servers only



Setting Discovery Credentials, (Cont.)

Each device in the network can have different access credentials. The Configure Credentials dialog allows the administrator to enter the SNMP v1/v2, SNMP v3, HTTP, and WMI access credentials for a single device or group of devices defined by the Target device field.

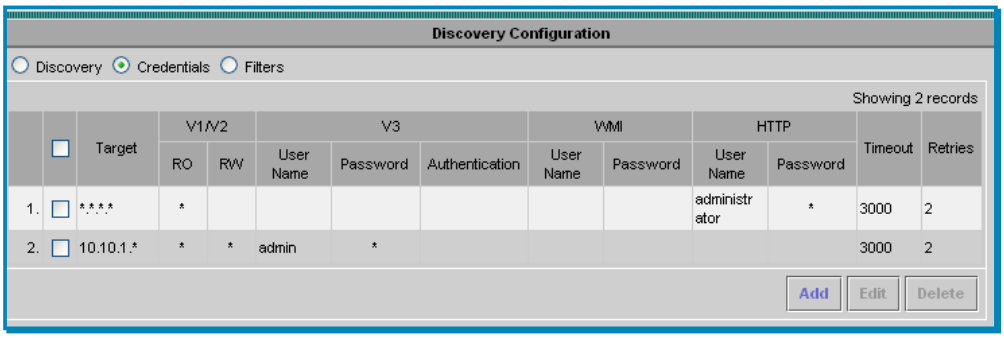
To define access credentials for an individual device, enter the specific IP address in the Target device field. Then fill in the SNMP, HTTP, and WMI credentials, and click OK.

To define access credentials for a group of devices or subnet, enter the IP address range or list of IP addresses in the Target device field. Then fill in the SNMP, HTTP, and WMI credentials, and click OK. Additionally, use *.*.*.* wildcard as a “catch-all for other devices.

Note(s):

- Operations Manager uses SNMP to poll a device’s MIB to retrieve its attributes and configuration. For IOS devices, only the SNMP read-only (RO) string is needed.
- Operations Manager also uses HTTP to pull information that is not available from a MIB. Some data from the Cisco CallManagers must be retrieved using HTTP. If the HTTP credentials are not specified, the monitoring status for the Cisco CallManagers will be “Partially Monitored”.
- To collect performance data for Cisco Unity Connection, Cisco Unity, or Cisco IP Contact Center, the Windows Management Instrumentation (WMI) credential is required. When adding these devices to Operations Manager, verify that the WMI username and password are provided.
- For security reasons, once these default credentials are entered and saved they will no longer be viewable from this page. New credential can always be added.

Preparing OM for Initial Use
Discovery Credentials Summary

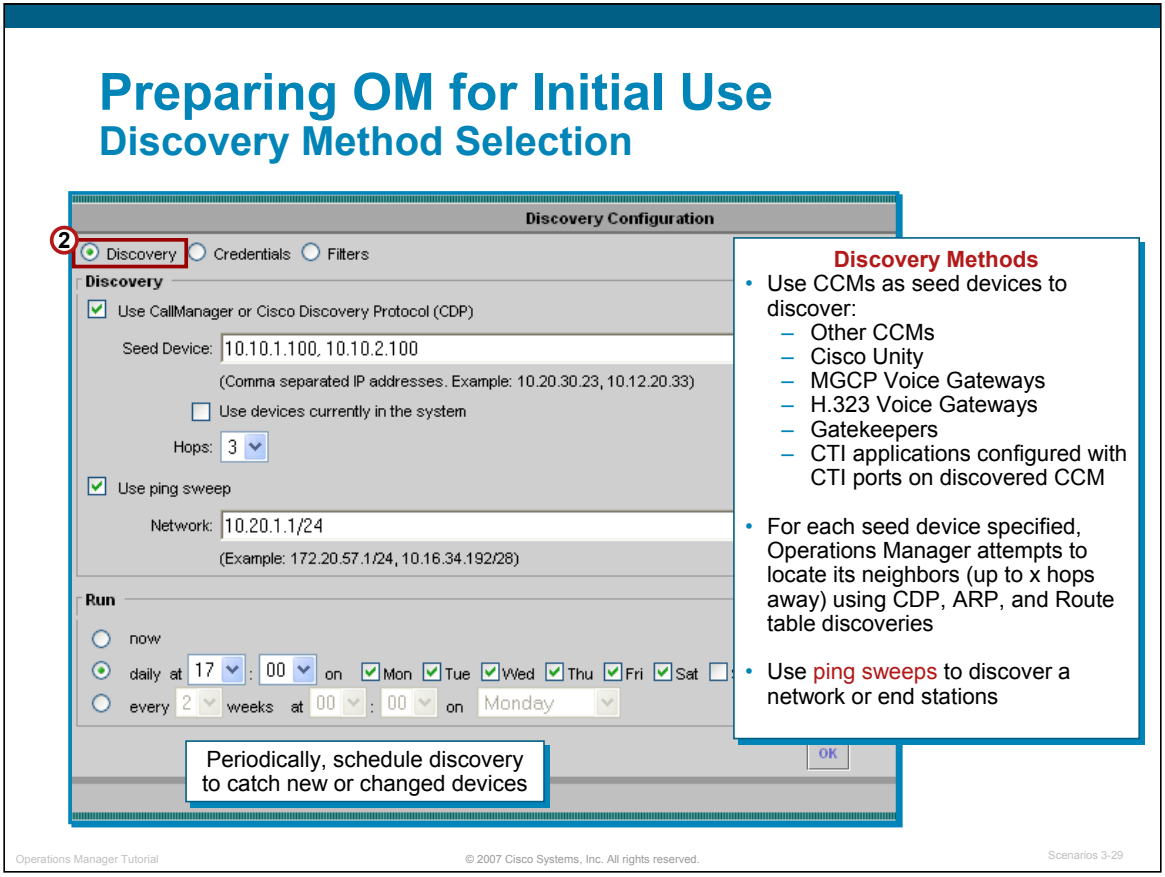


- Table lists discovery credentials defined:
  - *.*.*.* is a catch all target
  - More specific target credentials are used, if available
  - Order of target list doesn't matter
- Next, set the discovery methods and filters.

Discovery Credentials Summary

After adding the access credentials for individual or groups of devices, the target devices are listed in the Discovery Configuration dialog, as illustrated above.

Once the discovery credentials are defined, then set the discovery methods and optional filters. These topics are discussed next.



Discovery Method Selection

After credentials have been defined for one or more target devices, additional radio buttons appear in the Discovery Configuration dialog window. One of the new buttons is **Discovery**, which allows the administrator to configure how OM should discover the devices in the network. This topic describes how to set the discovery method.

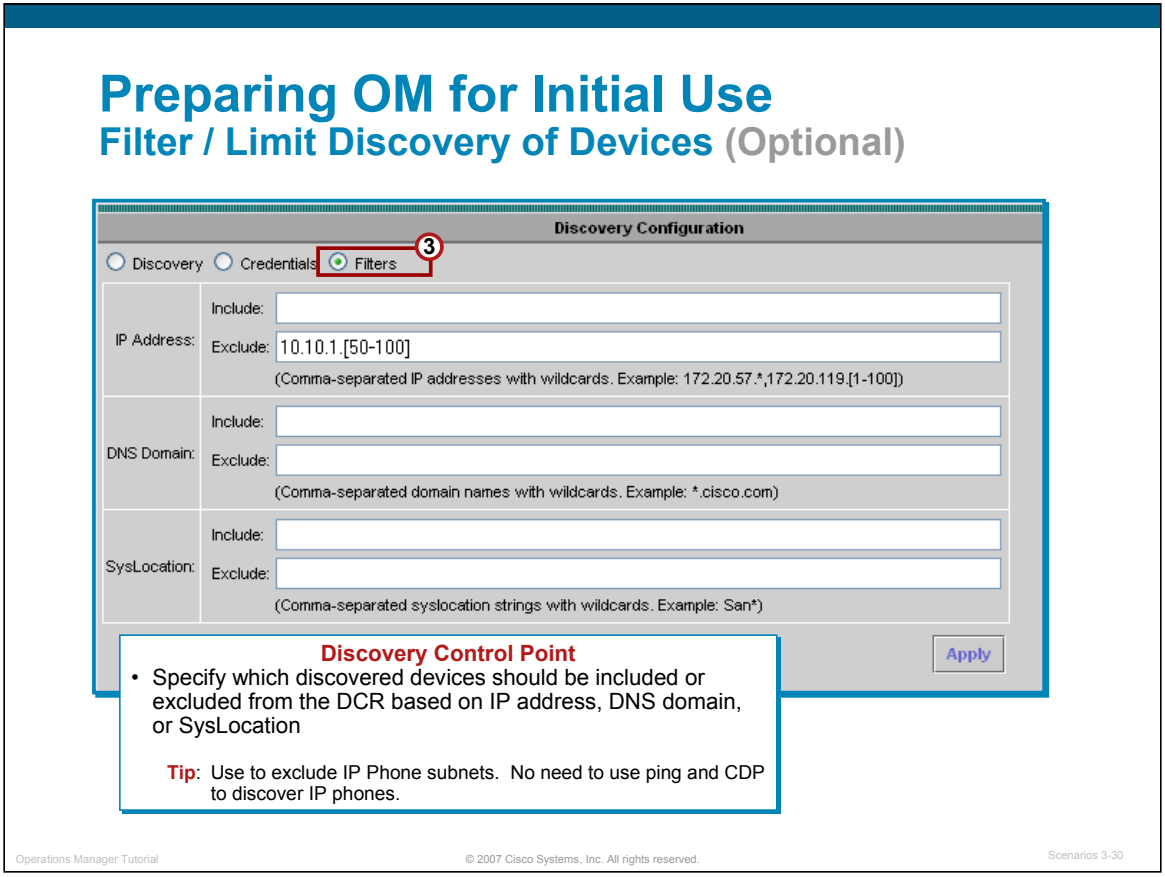
The first method of populating the DCR is to allow the devices to be auto-discovered. Operations Manager can automatically discover devices and add them to the DCR through the use of seed devices or by using a ping sweep across a subnet. The seed device can be a CallManager or a device with CDP (Cisco Discovery Protocol) enabled. You can use one or both methods for discovering the devices. To define the discovery method, follow these steps.

1. The Discovery Settings dialog is displayed. Enter one or more seed devices. Seed devices are starting points for the discovery.

   If the seed device is a CallManager, the process will discover other CallManagers, Unity, voice gateways, gatekeepers, and CTI applications.

   For each seed device specified, OM attempts to locate other devices by querying their CDP neighbor tables. Auto-discovery requires CDP to be enabled on devices in order for one discovered device to be aware of its neighbors.

2. Optionally, select the **Use Ping Sweep** check box and specify a comma-separated list of IP address ranges using the /netmask specification. For example, 172.20.57.1/24 to specify a ping sweep range starting from 172.20.57.1 and ending at 172.20.57.255.
3. **Run** – (Required) Select a radio button and enter the desired schedule to run the discovery process.
4. Click **OK** to start discovery based on schedule specified.



Filter / Limit Discovery of Devices (Optional)

Another radio button in the Discovery Configuration dialog window is called Filters. Filters allow the administrator to specify which discovered devices should be included or exclude from the DCR. This topic describes how to define the filters.

You may not want all devices that are discovered added to the DCR. Use the IP Address, DNS Domain, and SysLocation fields to include or exclude devices from the discovery process as noted below:

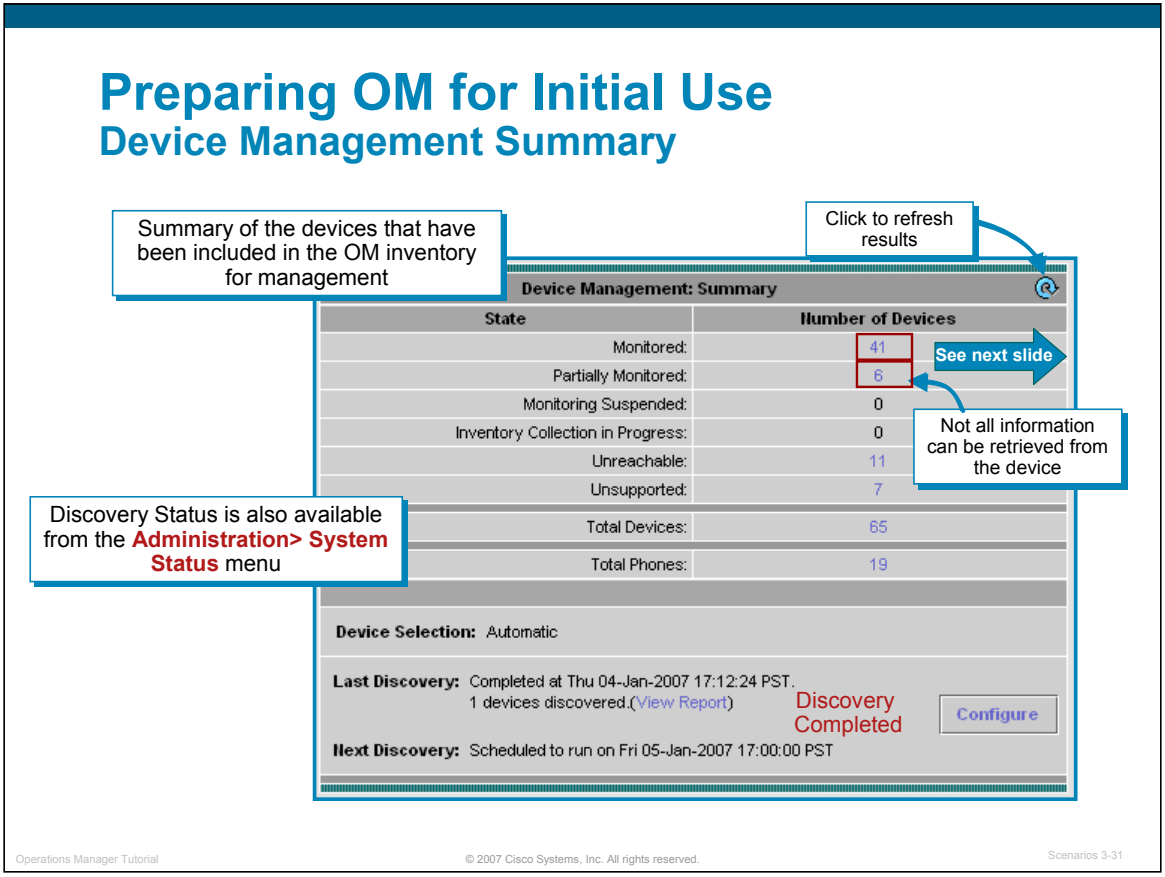
- **IP Address** - (Optional) Enter comma-separated IP addresses or IP address ranges for devices that you want to include or exclude in the auto-discovery process. You can use wildcards when specifying the IP address range. An asterisk (*) denotes the octet range of 1-255. Also, the octet range can be constrained using the [xxx-yyy] notation.

  For example: To include all devices in the 172.20.57/24 subnet in the auto-discovery process, enter an include filter of 172.20.57.*. To exclude devices in the IP address range of 172.20.57.224 - 172.20.57.255 from the auto-discovery process, enter an exclude filter of 172.20.57.[224-255]. Both types of wildcards can be used in the same range specification; for example, 172.20.[55-57].*.

  If both include and exclude filters are specified, the exclude filter is applied first before the include filter. Once a filter is applied to an auto-discovered device, no other filter criterion will be applied to the device. If a device has multiple IP addresses, the device will be processed for auto-discovery as long as it has one IP address that satisfies the include filter.

- **DNS Domain** - (Optional) Enter comma-separated DNS domain names for devices that you want to include or exclude in the auto-discovery process. The DNS names can be specified using wildcards. An asterisk (*) matches any combination of mixed uppercase and lowercase alphanumeric characters, along with the hyphen (-) and underscore (_) characters, of an arbitrary length. A question mark (?) matches a single uppercase or lowercase alphanumeric character or a hyphen or an underscore character. For example: *.cisco.com matches any DNS name ending with .cisco.com. *.?abc.com matches any DNS name ending with .aabc.com, or .babc.com, etc.

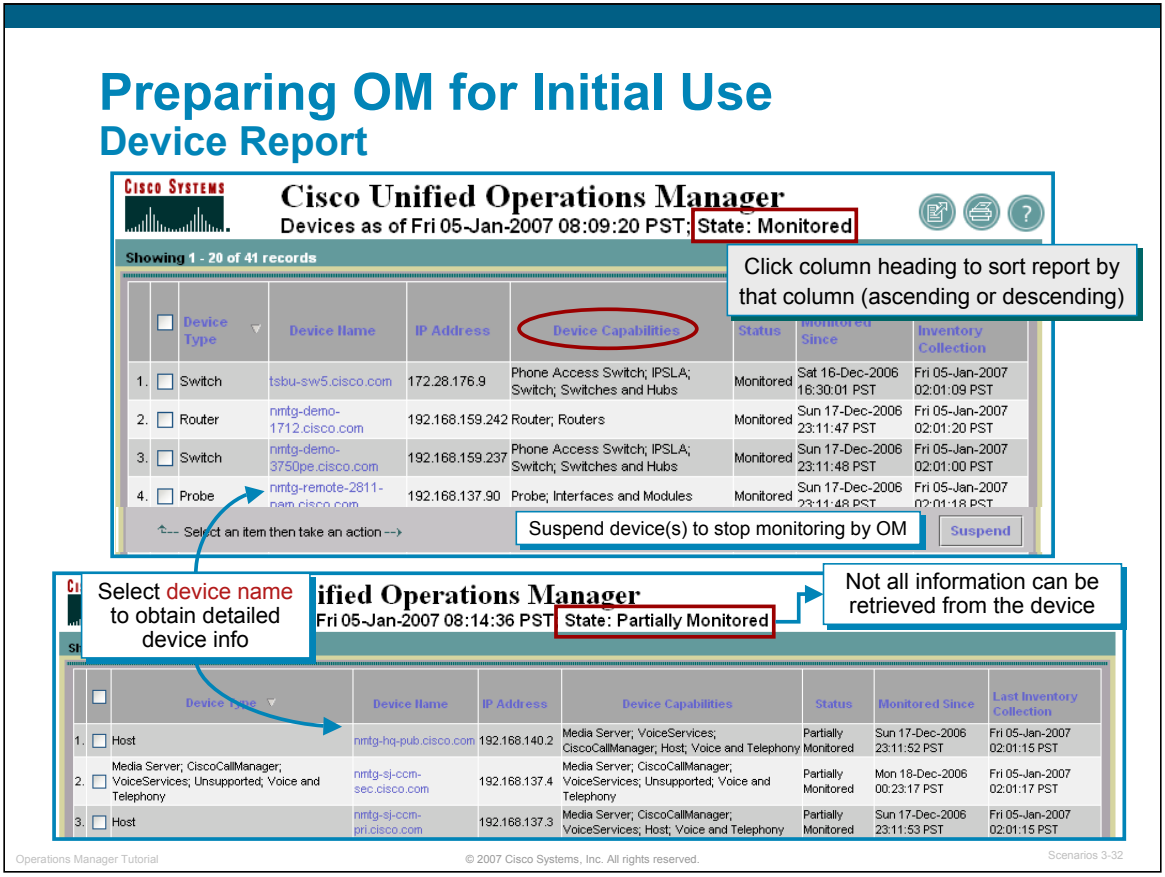
- **SysLocation** – (Optional) Enter comma-separated strings that will match the string value stored in the sysLocation OID in MIB-II, for devices that you want to include or exclude in the auto-discovery process. The location strings can be specified using wildcards. For example, a SysLocation filter of San * will match all SysLocation strings starting with San Francisco, San Jose, etc.



Device Management Summary

The following are the possible device states:

- **Monitored** - The device has been successfully imported, and is fully managed by Operations Manager.
- **Partially Monitored** - The device has been successfully imported by some of the backend processes in Operations Manager, but not all. Some of the information on the device can be not gathered due to its configuration or software version.
- **Monitoring Suspended** - Monitoring of the device is suspended.
- **Inventory Collection in Progress** - This is a transient state; devices will never remain in this state. Operations Manager is probing the device. This is the beginning state, when the device is first added; a device is also in this state during periodic inventory collection. Some of the data collectors may still be gathering device information.
- **Unreachable** - Operations Manager cannot manage the device. See the online help for possible reasons.
- **Unsupported** - The device is not supported by Operations Manager.



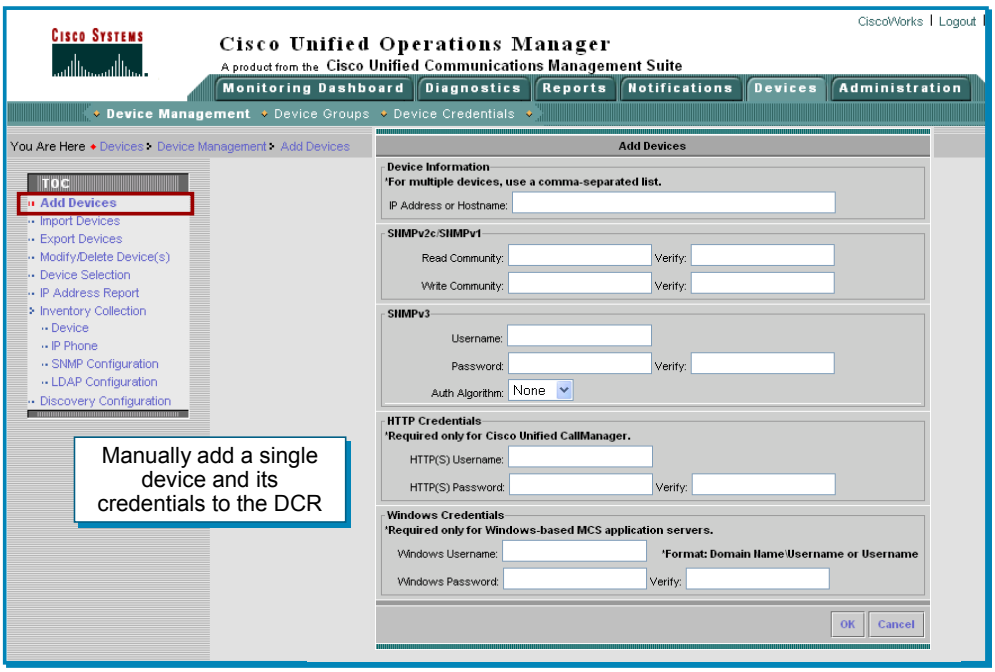
Device Report

Selecting the device count for one of the states in the Device Management Summary page (previous slide) provides a device report for the devices in the inventory that are in that state. These reports can be exported to a file or printed.

The Device Name can be selected to launch a Detailed Device View report that can report on all aspects of the device, including OS version, RAM, applications loaded, interfaces, environmental measurements, and more.

When a device is in the state of "**Partially Monitored**", there are some backend data collection processes in Operations Manager that cannot retrieve all its. This typically happens because the data cannot be collected via SNMP and must be collected using HTTP, and the HTTP user name and password credentials have not been associated with the device (either in the DCR or discovery credentials).

Preparing OM for Initial Use
Manually Add Devices

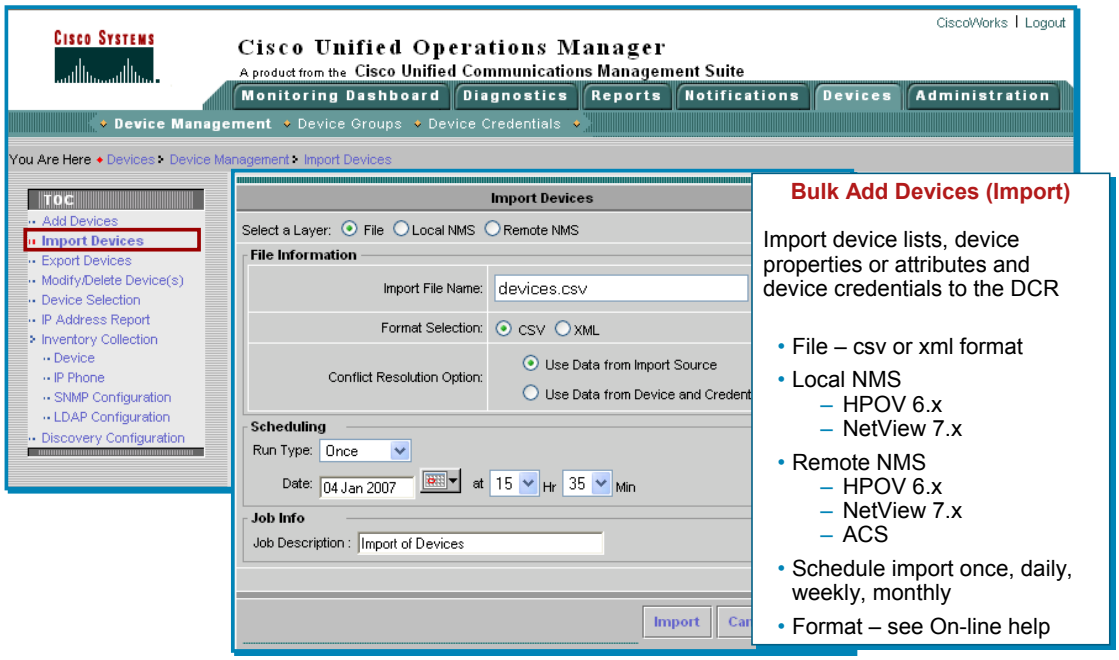


Manually Add Devices

Automatic discovery is one way to add devices to the OM Inventory. Another way is to manually add devices.

To manually add a single device at a time to the DCR, use the **Devices > Device Management > Add Devices** task. This requires entering its IP address or host name and credentials using the wizard, illustrated above.

Preparing OM for Initial Use
Import Devices

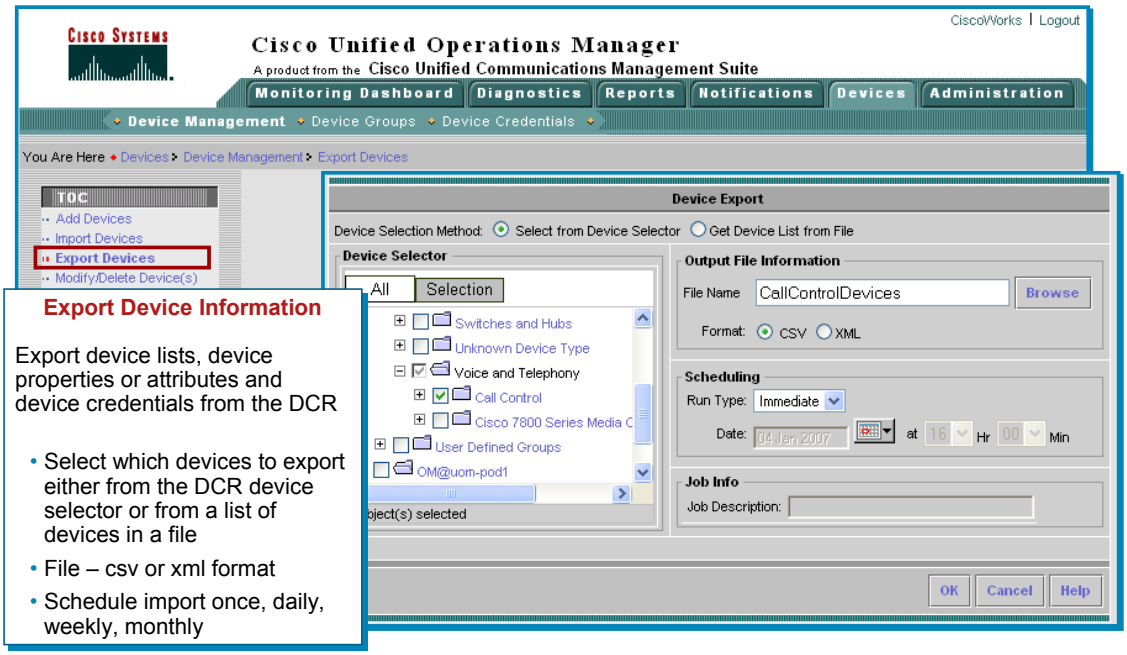


Import Devices

Another way is to add devices is to import devices into the DCR and then into the OM inventory.

To bulk import devices from a file (CSV or XML format) or a local NMS System (HPOV 6.x or NetView 7.x) or remote NMS system (HPOV 6.x, NetView 7.x, or ACS), use the Devices > Device Management > Import Devices task. The import can be scheduled to occur at a specific time.

Preparing OM for Initial Use
Export Devices



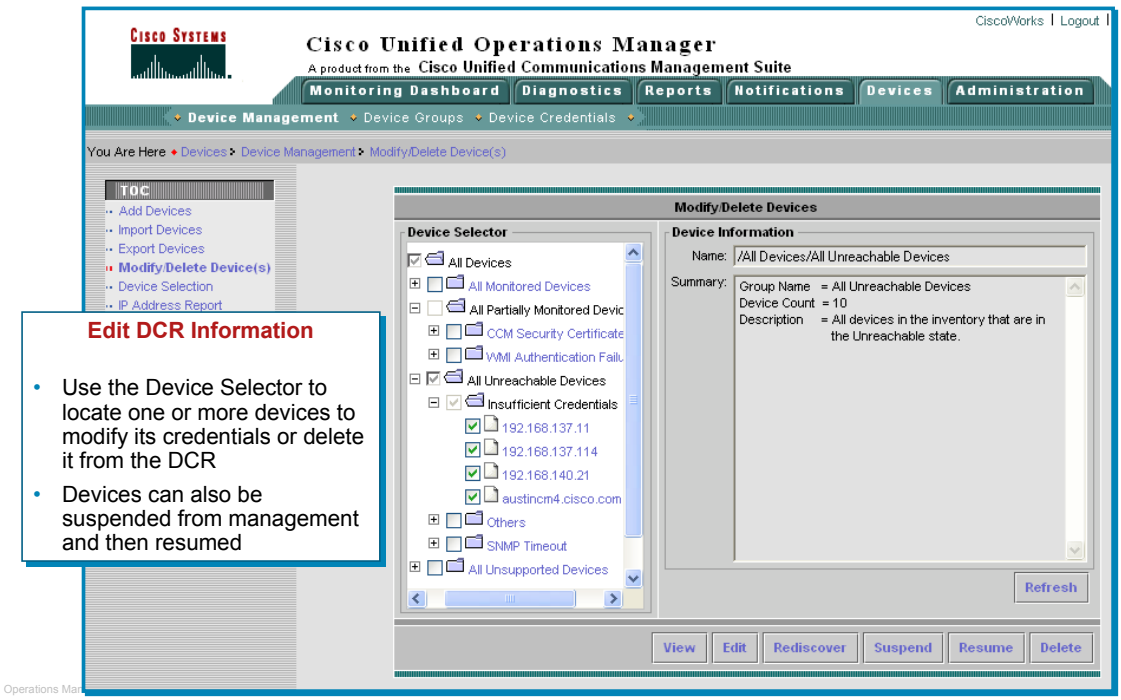
Export Devices

The Export feature is used to export a certain list of devices and their credentials into a file. The device list can be obtained from the device selector, or from a CSV file, as described below.

- Select from Device Selector—Select this option if you want to export devices from the Device and Credential Repository or the OM Inventory. You can output to a file you specify in the Output File Information field.
- Get Device List from File—Select this option if you want to export devices that are listed in a CSV file. The file must already be present on the server. Use this option when the CSV file contains only partial device credentials and you want to get the full list of credentials from the DCR. The input CSV file checks for data with DCR, and exports the data to the output file.

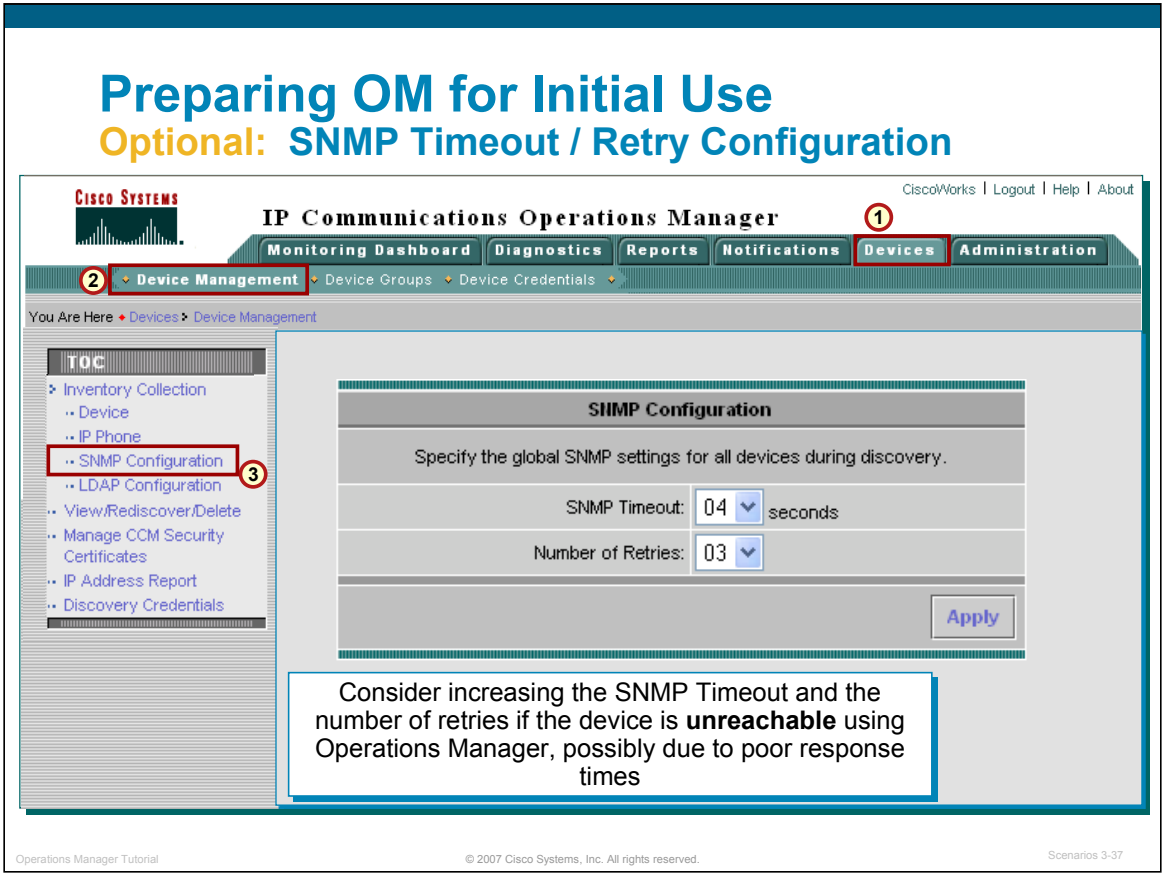
To see the list of attributes that can be exported use the **dcrcli** command line tool. (Refer to the online help for more information.)

Preparing OM for Initial Use
Modify / Delete Devices



Modify / Delete Devices

You can modify or delete devices from the DCR or from the OM inventory. Use the Modify / Delete task to perform inventory collection, view device credentials details, suspend and resume device monitoring, edit credentials, and delete devices. To use this feature, simply select the devices that you wish to modify or delete from the Device Selector and then click the action from one of the buttons.



SNMP Timeout / Retry Configuration

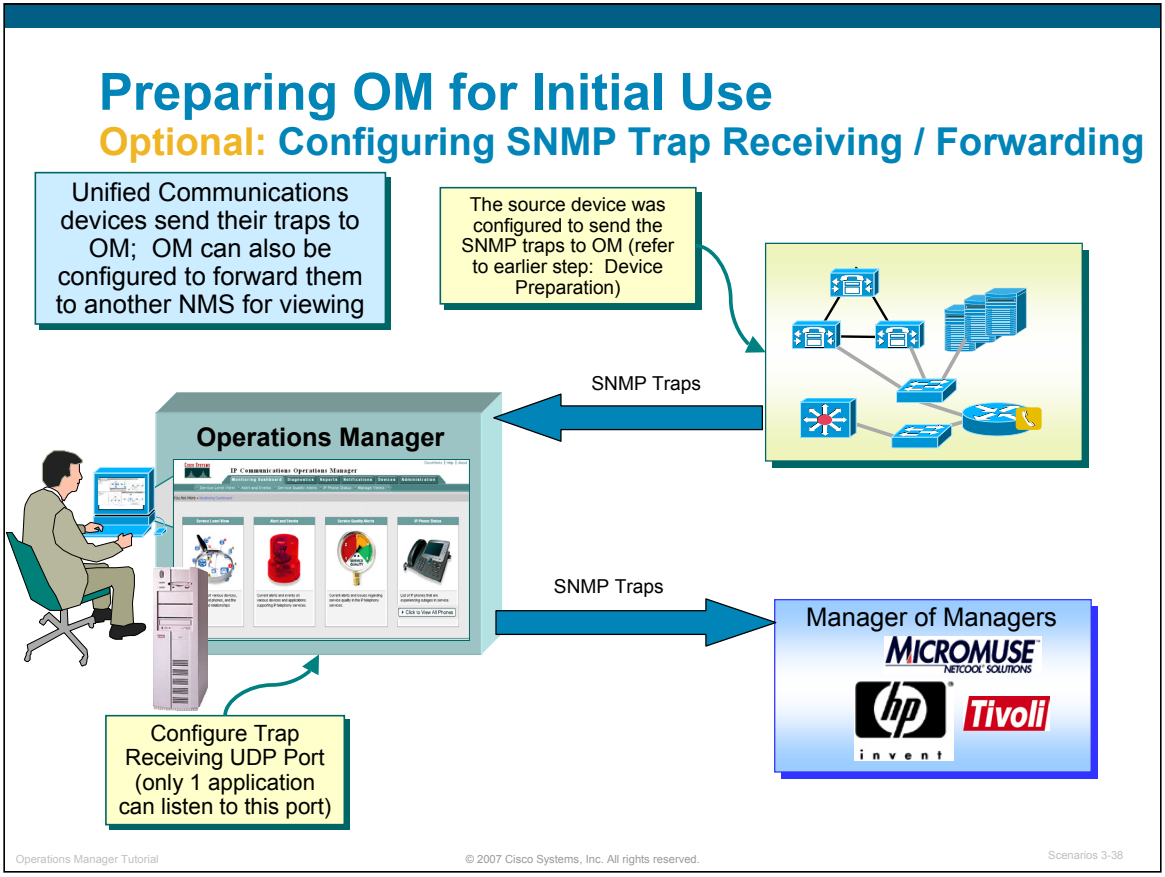
If an SNMP query does not respond in time, Operations Manager will time out. It will then retry contacting the device for as many times as listed under the snmpretries attribute in the configuration file. The timeout period is doubled for every subsequent retry. For example, if the timeout value is 4 seconds and the retries value is 3, Operations Manager waits for 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry.The SNMP timeout and retries are global settings and their default values are:

Timeout—4 seconds

Retries—3

To change these default setting, follow these steps:

1. Select ***Devices > Device Management > SNMP Configuration***. The SNMP Configuration page appears.
2. Select a new SNMP timeout setting.
3. Select a new Number of Retries setting.
4. Click ***Apply*** to make changes effective.



Configuring SNMP Trap Receiving and Forwarding

Network devices can be configured to send SNMP traps to alert operators of specific conditions. For example, in an upcoming scenario, the network administrator will configure the IP SLA feature in IOS devices which can be used for performance and availability testing. When these tests exceed specified thresholds, the IP SLA device can send an SNMP trap to a trap receiver, such as Operations Manager. (SNMP traps are configured in Scenario "Getting Started".)

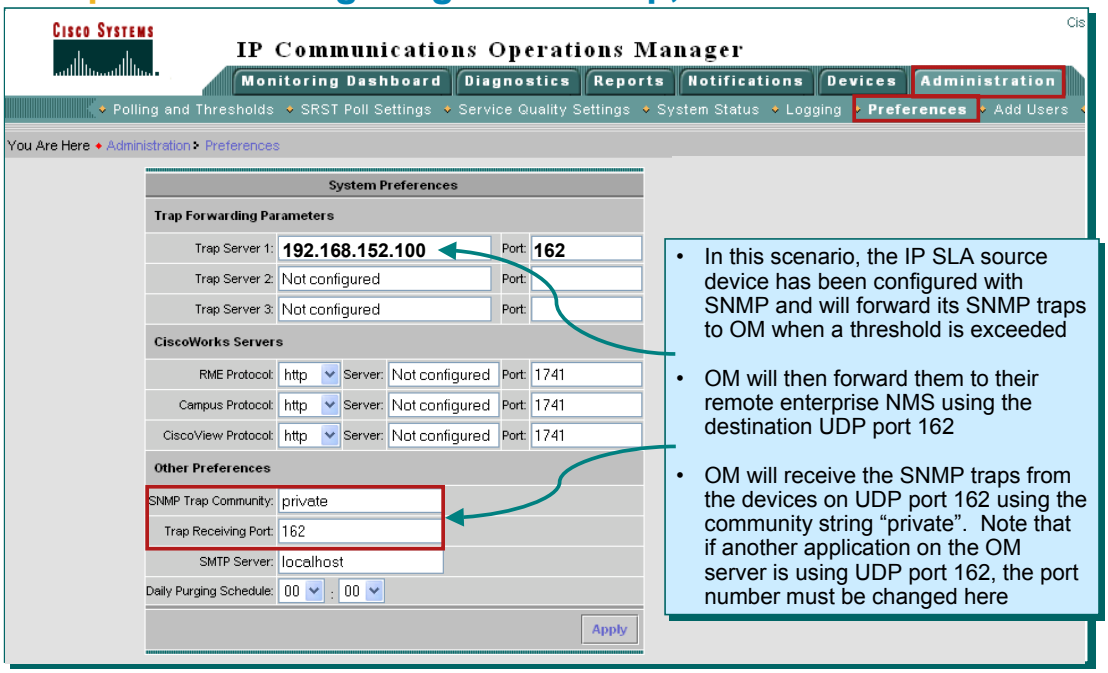
In order for Operations Manager to *receive* SNMP traps from various sources, such as IP SLA devices, you must perform the following:

1. Enable SNMP on your devices and configure SNMP to send its traps directly to Operations Manager. (The source device was configured earlier in this scenario using the command line interface steps for enabling SNMP and sending SNMP traps to a particular host.)
2. Operations Manager can also be used to forward the SNMP traps it receives to a list of servers and ports for event correlation or a network-wide event notification system. This capability enables Operations Manager to easily work with other trap processing applications.
3. And finally, if another application on the Operations Manager server is already listening for traps on the standard UDP trap port (162), you must configure Operations Manager to use another port, such as port 9000. Only one application per server can listen to a used port.

Step 2 and 3 above are configured in Operations Manager under **Administration > Preferences**. Let's look at this dialog next.

Preparing OM for Initial Use

Optional: Configuring SNMP Trap, continue …

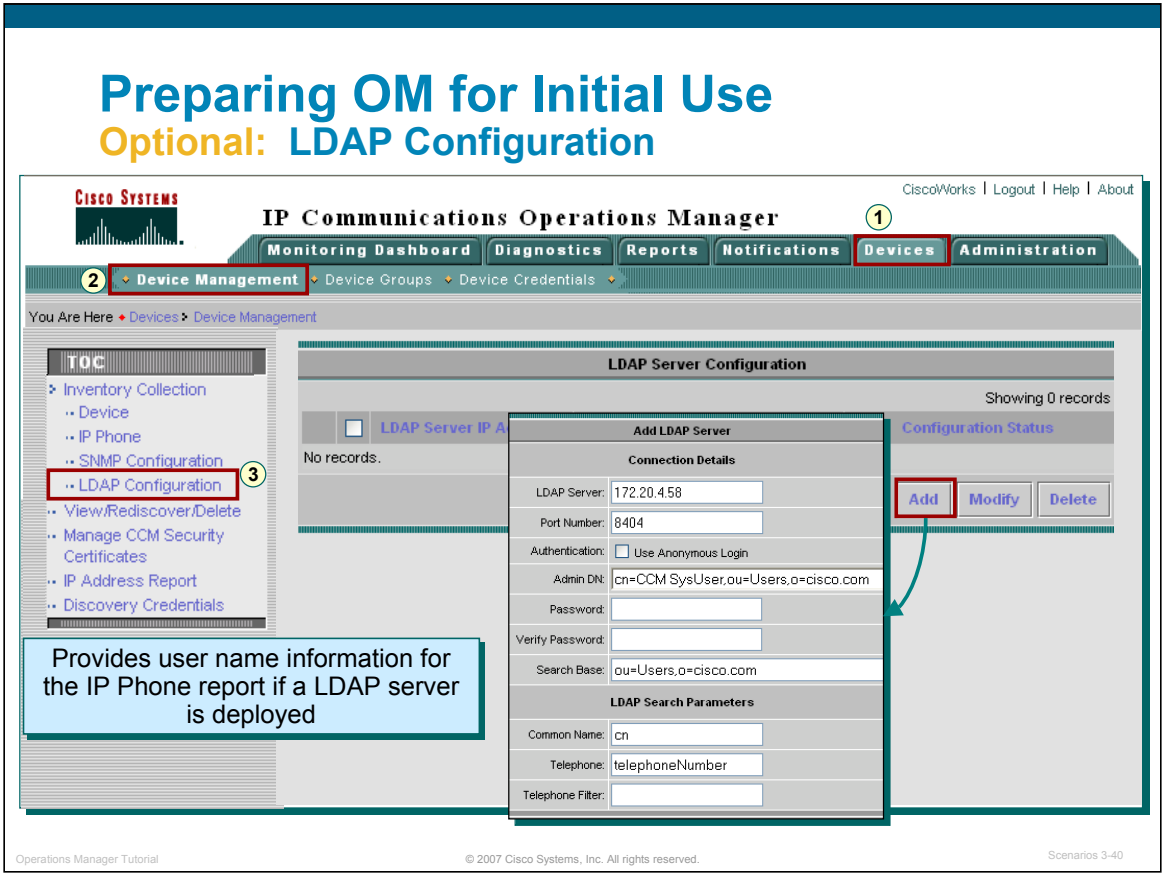


- In this scenario, the IP SLA source device has been configured with SNMP and will forward its SNMP traps to OM when a threshold is exceeded
- OM will then forward them to their remote enterprise NMS using the destination UDP port 162
- OM will receive the SNMP traps from the devices on UDP port 162 using the community string "private". Note that if another application on the OM server is using UDP port 162, the port number must be changed here

Configuring SNMP Trap Receiving and Forwarding, continue …

In order for Operations Manager to *forward* SNMP traps to another remote NMS, follow these steps:

1. From the Operations Manager menu, select to ***Administration> Preferences*.**
2. Under the heading "**Trap Forwarding Parameters**", enter the remote NMS IP address in the Trap Server field. Enter the UDP port number that the NMS is listening to in order to receive the traps. In this scenario, the NMS is listening to UDP port 162 which is typically the default port for SNMP trap listeners.
3. The devices have been configured to sent SNMP traps to Operations Manager using a SNMP community string and UDP port number. Enter these values under the "**Other Preferences**" fields. Note that if another application on the Operations Manager server is using UDP port 162, the port number must be changed here; otherwise there will be a conflict of ports. Only one application can listen to the UDP port at a time.



LDAP Configuration

LDAP, Lightweight Directory Access Protocol, is an Internet protocol that applications use to look up information from a server. For example, every email program has a personal address book, but how do you look up an address for someone who's never sent you email? How can an organization keep one centralized up-to-date phone book that everybody has access to? That question led software companies such as Microsoft, IBM, Lotus, and Netscape to support a standard called LDAP.

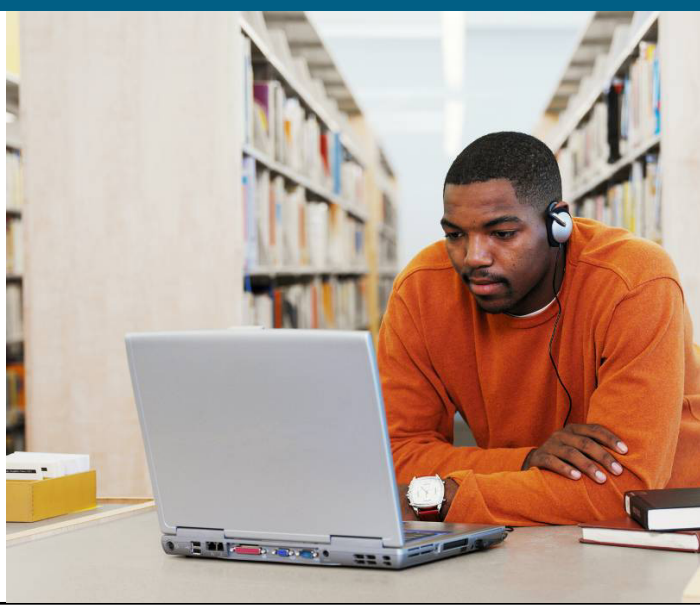
"LDAP-aware" client programs, like Operations Manager, can ask LDAP servers to look up entries in a wide variety of ways. LDAP continues to be a popular standard for communicating record-based, directory-like data between programs.

If LDAP is used in the network, it can be defined here so that information on end-points in the network (i.e. phones) can be correlated. Follow these steps for defining a LDAP server for Operations Manager to use.

1. Select ***Devices > Device Management > LDAP Configuration***. The LDAP Server Configuration page appears.
2. Click ***Add***. The Add LDAP Server page opens.
3. In the Connections Details area, enter the following:
   - The LDAP server name or IP address
   - The port number
   - If you want to use anonymous login for authentication, select the Use Anonymous Login check box
   - An admin DN
   - Enter the password for the LDAP server and reconfirm the password
   - Enter a search base
4. In the LDAP Search Parameters are, enter a name for the search, a telephone number, and a filter.
5. Click ***Add***.

Normal Operational Status

- Getting Started
- Preparing OM for Initial Use
- **Normal Operational Status**
- Service Availability Testing
- Node-to-Node (IP SLA) Testing
- Experiencing Phone Outages
- Performance Monitoring



Scenario 3: Normal Operational Status
Outline

Checking Status of Unified Communication Services

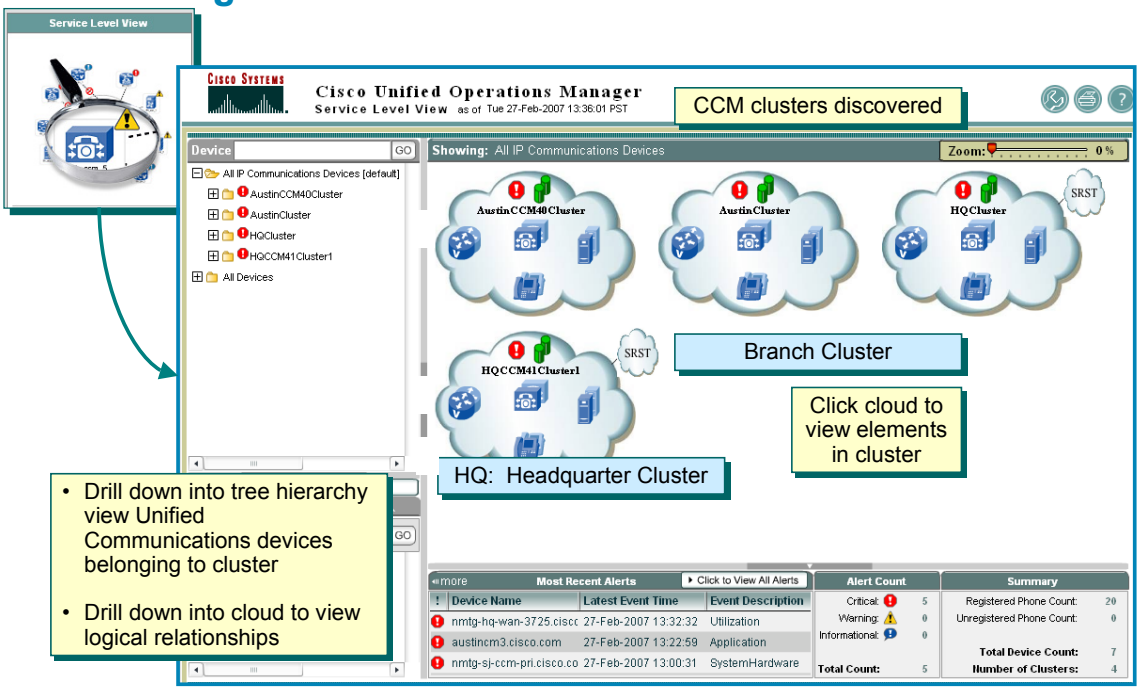
Checking for Unified Communication Device Alerts

Checking for IP Phone Alerts / Outages

Normal Operational Status

In this scenario, we will look over the shoulder of Susan Jones, the lead network engineer at Company ABC, as she looks at the various dashboards, features, and reports within Operations Manager. These dashboards will be reviewed by Susan or someone else on the team on a day-to-day basis. These dashboards are designed so that it can be setup and left running, providing an ongoing monitoring tool that signals the operator when something needs attention.

Normal Operational Status
Viewing Unified Communications Services



Viewing Unified Communications Services

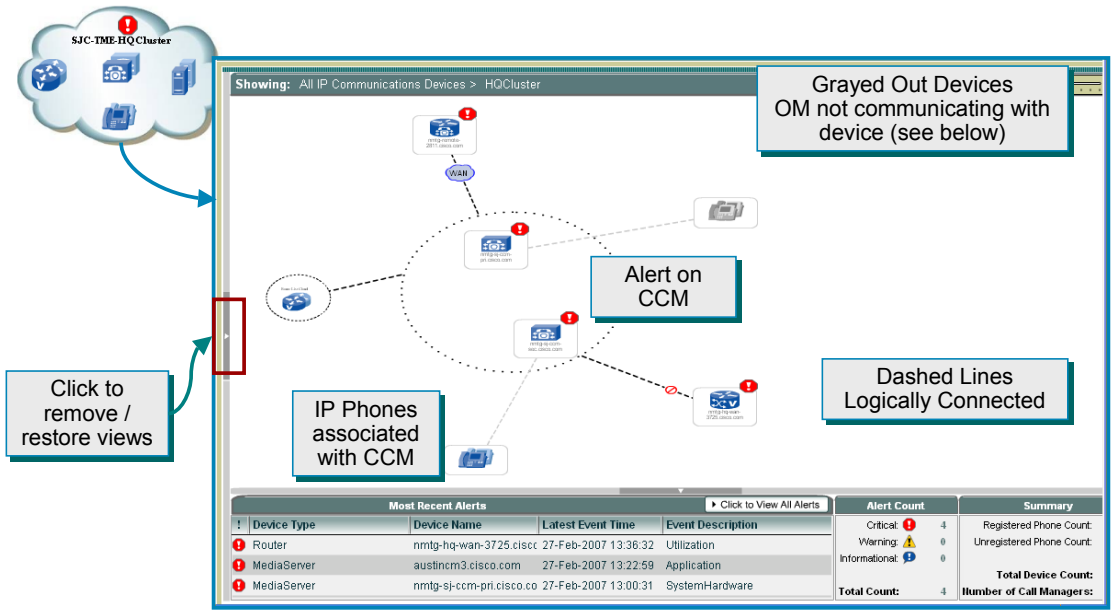
One of the four Monitoring Dashboards in Operations Manager is the Service Level View. This view allows Susan Jones to visualize their Unified Communications deployment by viewing a logical topology of the Unified Communications implementation that focuses on the call control relationships.

The view that is displayed is a real-time auto-refresh display that provides status information about all the Unified Communications clusters and the elements of the clusters in the deployment. The Service Level View is designed so that it can be setup and left running, providing an ongoing monitoring tool that signals you when something needs attention. When a fault occurs in the network, Operations Manager generates an event or events that are rolled up into an alert. If the alert occurs on an element it is shown on the Service Level View.

To launch the Service Level View and view the real-time status information, Susan will follow these steps:

1. The devices managed in the Service Level View have been discovered using the steps from the previous scenario. In order for the devices to be managed by Operations Manager, they must be in the Operations Manager inventory. (Refer to the previous scenario, if you have not completed the discovery.)
2. Launch the Service Level View. The Service Level View is accessible under the Operations Manager Monitoring Dashboard tab. Either select the Service Level View menu item under the Monitoring Dashboard tab or click on the Service Level View picture (*notice that the icon changes when the cursor is placed over the top of it*).
3. By default, the view displays a tree hierarchy and a graphical display of all the discovered Cisco CallManagers clusters. The devices within a cluster can be viewed by opening either the tree hierarchy or the icon representing the cluster (click to open).
4. Click one of the graphical CCM clusters to open to view the logical relationships between the CCM and other devices.
5. As you select one of the clusters either in the tree hierarchy or graphical view, the Alert Count and Phone Summary window panes change to reflect the information for the selected cluster.

Normal Operational Status
Viewing Unified Communications Services, continue …



Viewing Unified Communications Services, continue …

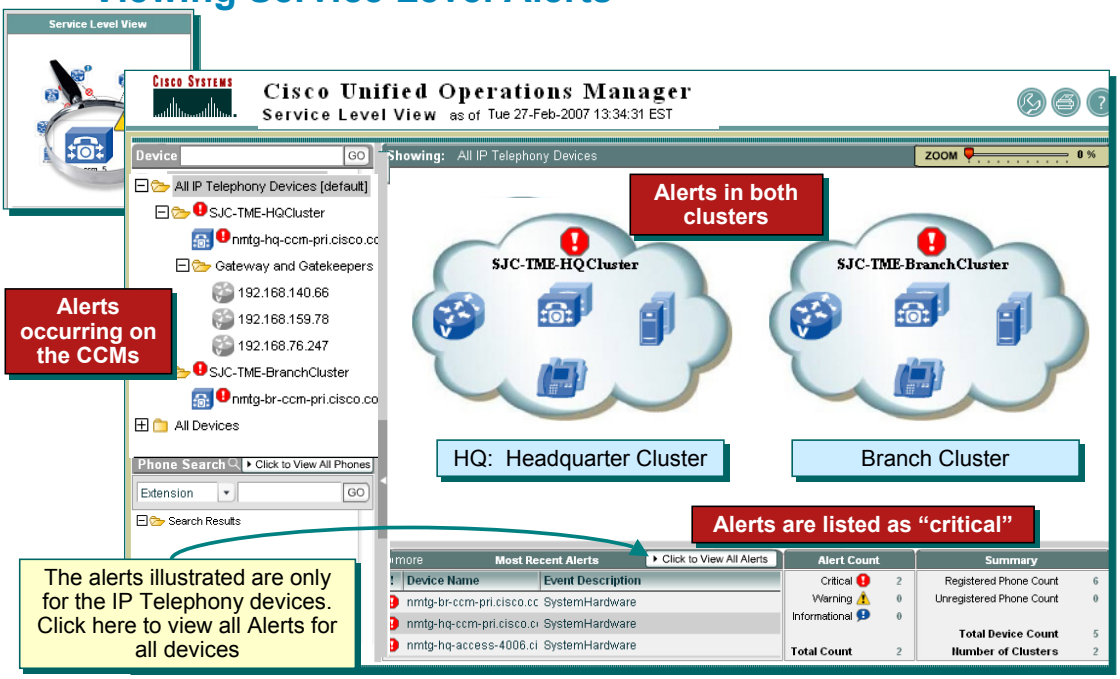
Open one of the CCM clusters to view logical relationships with other devices. Susan opens the cluster view, by using her mouse to either click on it in the tree hierarchy or click on the icon in the graphical display. Continue to learn more about the Service Level View by following these steps:

1. Click the window pane arrows, illustrated above with "remove / restore", to open or close the tree hierarchy or the summary information at the bottom of the screen. This will allow you to expand the graphical, logical topology view.
2. Click the More link in the Most Recent Alerts window pane to expand the pane to reflect the Event Time and the Device Type information. This will also close the tree hierarchy, but can be restored by clicking on the window pane arrow.

Note(s):

- *As illustrated above, some devices may be grayed out. This occurs when the device is not responding to OM using SNMP queries or is outside the discovery boundaries, but was discovered originally from the CCM discovery.*

Normal Operational Status
Viewing Service Level Alerts

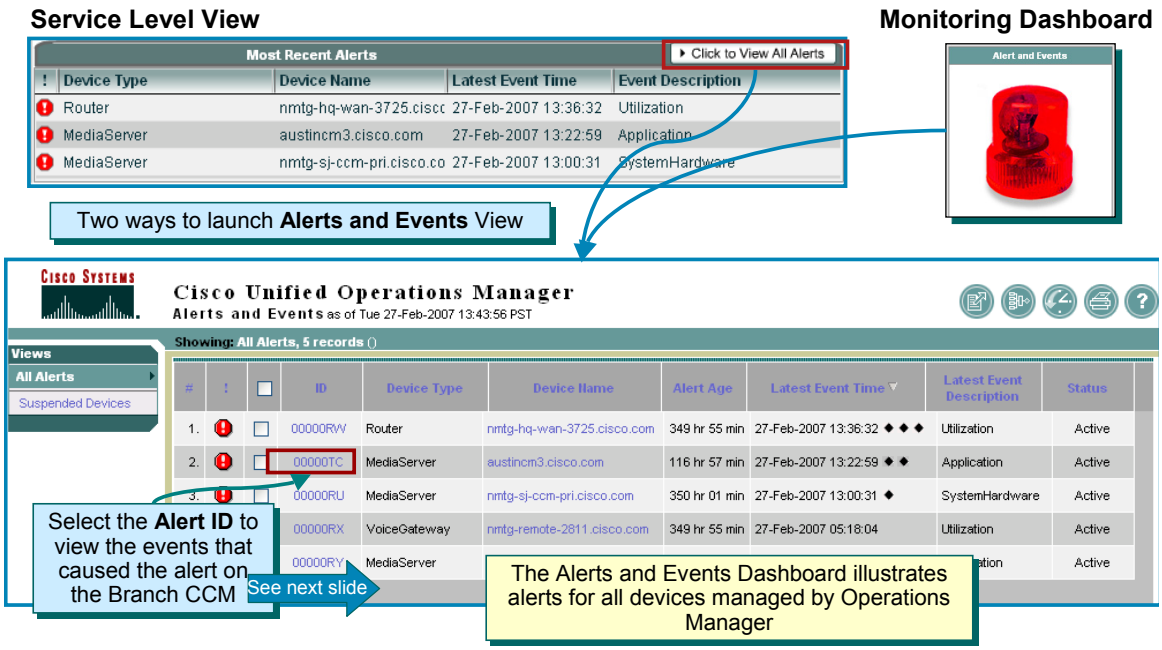


Viewing Service Level Alerts

At first glance, Susan notices *critical* alerts occurring within the Cisco CallManager clusters. She can open the CCM cluster in the tree hierarchy (or open the CCM cluster cloud) to view which device(s) in the cluster has an alert. Susan can also see the "Most Recent Alerts" at the bottom of the Service Level View.

The alerts are coming directly from the Cisco CallManagers at both the headquarters and the branch facilities. Let's find out why!

Normal Operational Status
Checking All Alerts and Their Events



Checking for Alerts

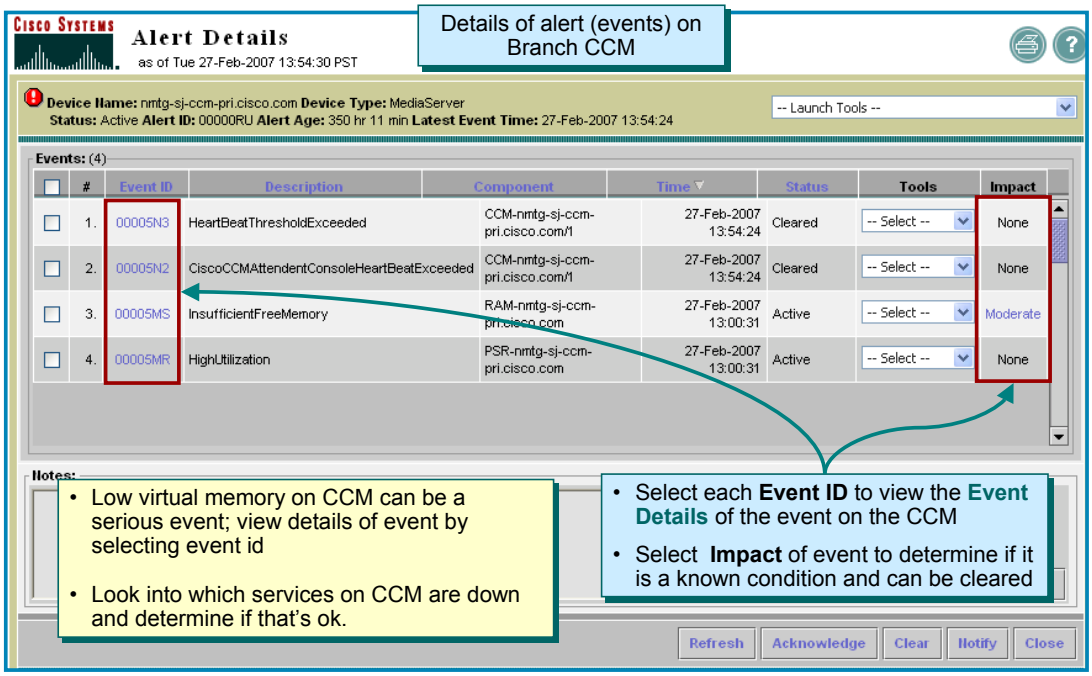
Susan is concerned about the two Cisco CallManagers at the company's headquarters and remote branch locations. The Service Level View provides the administrator with a quick glance at the *recent alerts* on the Unified Communications clusters and the elements of the cluster. In that view, Susan saw alerts related to the system hardware for the CallManagers.

To view *all alerts*, the alert details and events that caused the alert, as well as the alert history, use the **Alerts and Events View**. This view provides real-time information about the operational status of the network.

To launch the Alerts and Events View, Susan will follow these steps:

1. If viewing the Service Level View, simply click the "**Click to View All Alerts**" button, as illustrated above. Otherwise, the Alerts and Events View is accessible under the Operations Manager Monitoring Dashboard tab. Either select the **Alerts and Events View** menu item under the Monitoring Dashboard tab or click on the **Alerts and Events** picture, as illustrated above. (*Notice that the icon changes when the cursor is placed over the top of it.)*
2. The alerts are categorized by device views. By default, there are two views: **All Alerts** and alerts on **Suspended Devices**. Suspended devices are devices in the Operations Manager inventory that are not being monitored by Operations Manager because they have been suspended by an operator. Alerts can still be received from these devices. (*Later in this chapter, you will see how to create a new view to better organize the information based on the devices*.)
3. Select the view **All Alerts** (selected by default).
4. Locate the alerts for the two Cisco CallManagers at the company's headquarters and remote branch locations. Take notice of when the alert was received and how long it has been active.
5. Obtain the events or details of the alert by selecting the alert id.

Normal Operational Status
Viewing Alert Details



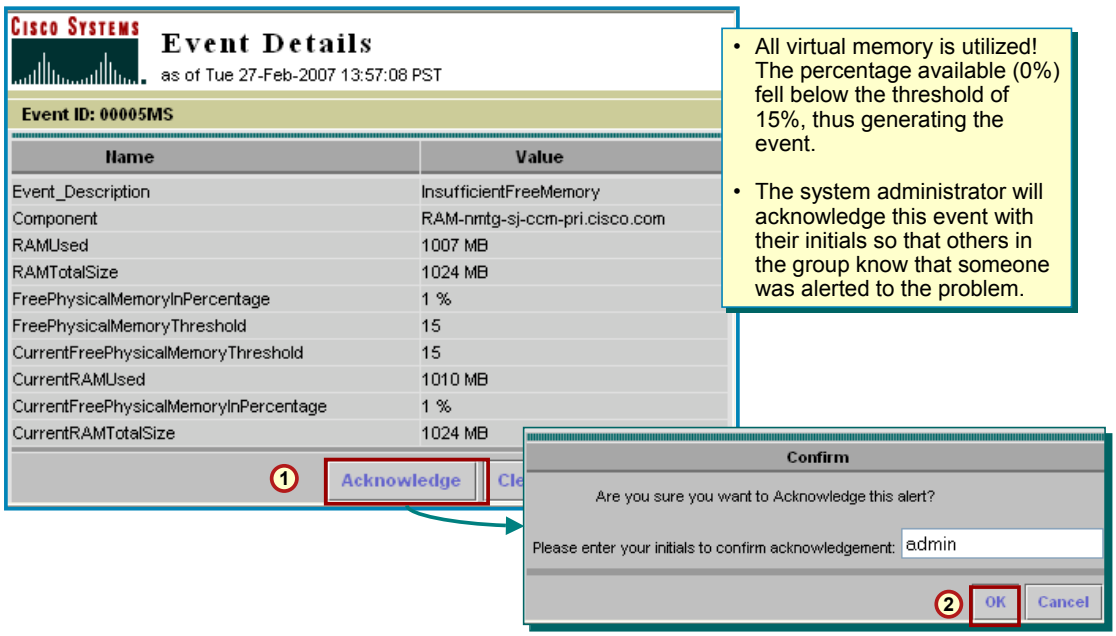
Viewing Alert Details

In the previous step, Susan selected the Alert ID in the Alerts and Events View to obtain more details about the alert on the CallManager located at the branch office, which launched the Alert Details windows, as illustrated above. This view lists the events that occurred on the device and provides a launch point for more information and tools.

Susan quickly notices the following on in the Alert Details view:

1. The Virtual memory on the system has fallen below the recommended level or threshold. Susan verifies the amount of virtual memory used and the recommended level by clicking the Event ID. (Refer to next page for screen illustration.) Susan also clicks the Impact link "High" to view how this event could impact the overall performance of the device. The Impact report confirms that low virtual memory will cause increased page faults and thrashing which will lead to lower performance.
2. Secondly, Susan notices that several services are down on the CallManager. Susan is not sure which services are not running so after evaluating the virtual memory issue, she will click on the Event ID and the Impact link of the Service Down events to investigate those further.

Normal Operational Status
Acknowledging Known Conditions

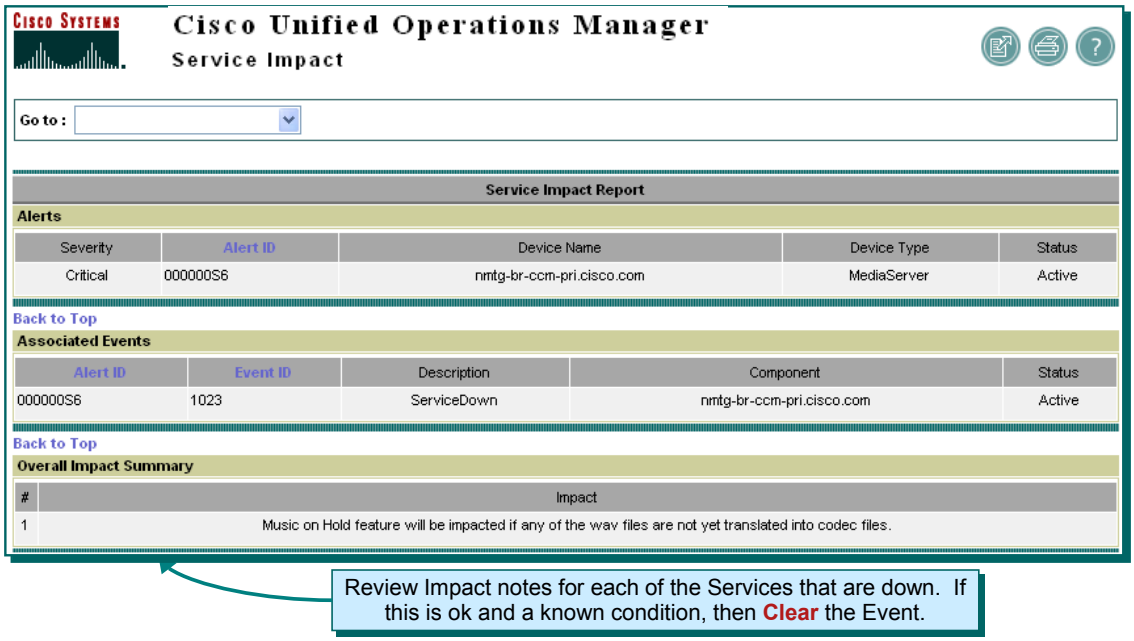


Acknowledging Known Conditions

First, Susan looks into the Insufficient Free Virtual Memory event by using these steps:

1. From the Alert Details window (on the previous page), Susan clicked on the **Event ID** for the Insufficient Free Virtual Memory event. The Event Detail window is displayed.
2. From here, Susan can evaluate the total size of the Virtual Memory (1026 MB) and how much of that is being utilized (1025 MB). Almost all of the virtual memory is being utilized, which will cause increased page faults and thrashing and will lead to lower performance as reported by the Impact report. (The Impact report can be viewed by clicking on the Impact link "*High*" in the Alert Details window.) Susan also notices that the recommended level or threshold for free Virtual Memory is set to 15% (or 85 % utilized).
3. Susan clicks the **Acknowledge** button from the Event Details window so that others in her group know that someone was alerted to the event. She will need to enter here initials or name to confirm the acknowledgement.

Normal Operational Status
Clearing Known Conditions

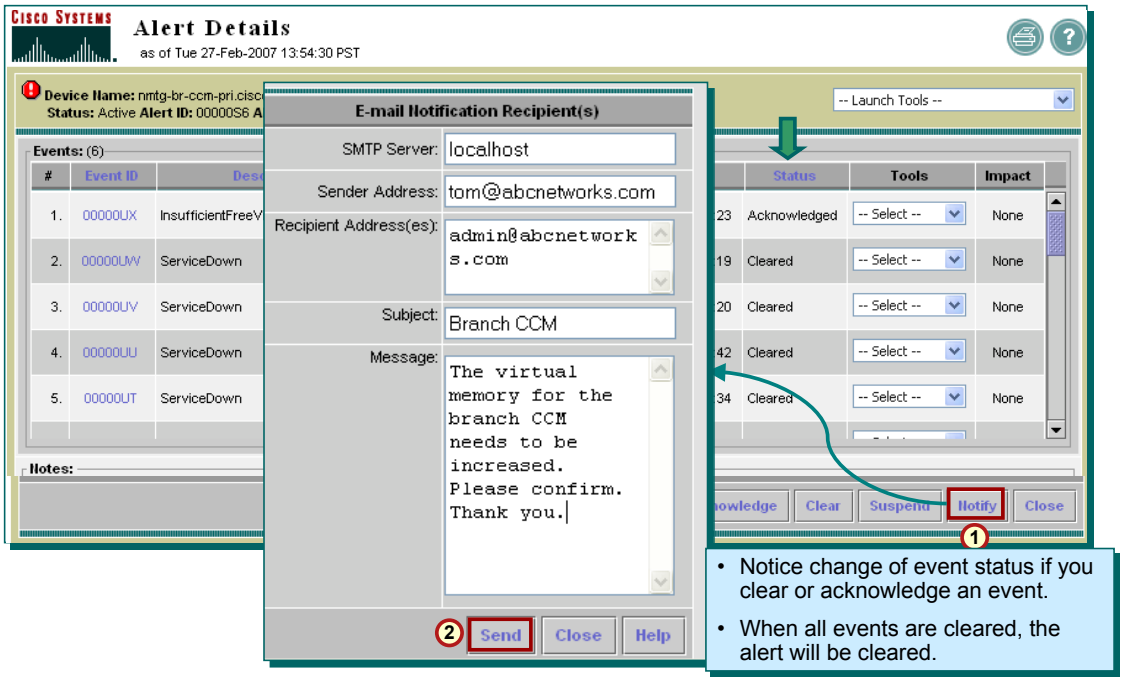


Clearing Known Conditions

Next, Susan looks into the Service Down events on the Cisco CallManager by using these steps:

1. Going back to the Alert Details window, Susan clicks on the **Event ID** for one of the Service Down events. The Event Detail window is displayed. Additionally from the Alert Details window, Susan also clicks on the Impact link “High” to display the Impact Reports.
2. From the Event Details and Impact reports, Susan can evaluate which services or products are not running. Here are the results:
   - Illustrated above: The Cisco MOH Audio Translator is stopped. The Impact: Music on Hold feature will be impacted if any of the wav files are not yet translated into codec files.
   - The Media Streaming Application is stopped. The Impact: Music on hold, Conference Bridge and Announce applications will not work if this service is down.
   - The Cisco Web Attendant Server is stopped. The Impact: Centralized services and call-control functions will be affected for Cisco WebAttendant and Attendant Console clients and pilot points.
   - The Cisco Messaging Interface is stopped. The Impact: SMDI based integration with the Legacy voice mail systems will be affected.
   - The Cisco Extended Functions is stopped. The Impact: Cisco CallBack and Quality Report Tool Features will not work.
3. Susan is O.K. with these services not running since they do not needed these services. Therefore, she will clear the Event in each of the Event Details windows by clicking the Clear button.

Normal Operational Status
Email Notification of Alert



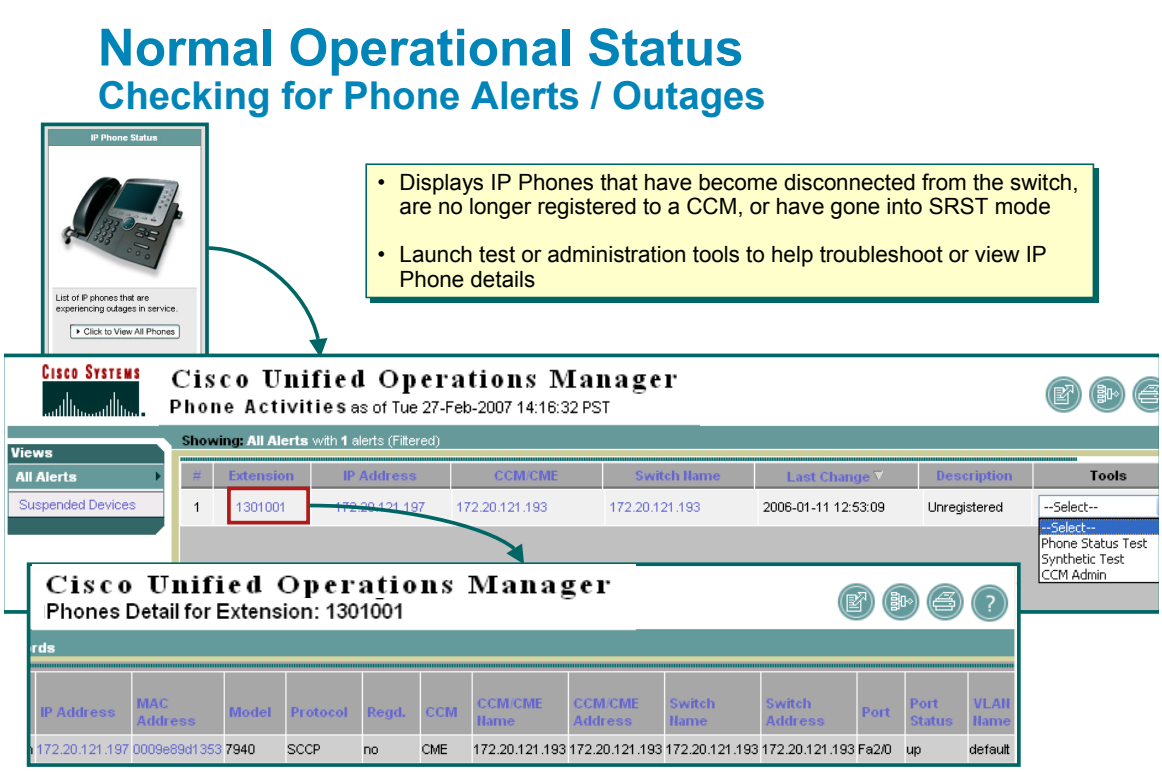
Email Notification of Alert

After reviewing all the events, Susan goes back to the Alert Details window to review the status of the events that she has either Acknowledged or Cleared (notice the Status change in the illustration above).

One additional item that Susan wants to take care of is to notify their local system administrator of the virtual memory issue so that it can be corrected soon. Susan clicks on the **Notify** button and can then directly from Operations Manager issue an email notification to their system administrator.

Note(s):

- *When all events for an alert are cleared, the alert will be cleared in the Alerts and Events dashboard.*



Checking for IP Phone Outages

The last monitoring dashboard that Susan checks on a regular basis is the IP Phone Status dashboard. This display provides real-time information about the operational status of the IP phones in the network. This display is also designed so that it can be set up and left running, providing an ongoing monitoring tool that signals you when something needs attention with an IP phone.

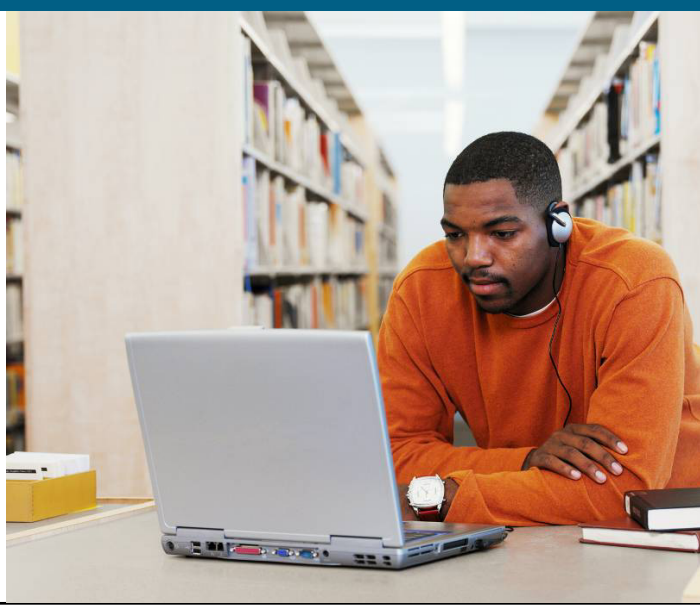
To launch the IP Phone Status dashboard, Susan will follow these steps:

1. The IP Phones managed in the IP Phone Status dashboard need to have their associated CCM and their connecting switch discovered. They should have been discovered using the steps from the previous scenario. (Refer to the previous scenario, if you have not completed the discovery.)
2. Launch the IP Phone Status View. The IP Phone Status View is accessible under the **Operations Manager Monitoring Dashboard** tab. Either select the **IP Phone Status** menu item under the Monitoring Dashboard tab or click on the **IP Phone Status** picture (*notice that the icon changes when the cursor is placed over the top of it*).
3. The Phone Activities window is displayed and shows information about the IP phone(s) in your network that have become disconnected from the switch, are no longer registered to a Cisco CallManager, or have gone into SRST mode. In the ABC network above, one IP Phone has become unregistered with the associated CCM.
4. Susan clicks on the IP Phone **Extension** number in the view. This launches the **Phones Detail** report. Here Susan can easily identify the IP phone and its connecting switch, port, and VLAN and determine if the phone is a known outage. Susan determines that this phone should be out of service.

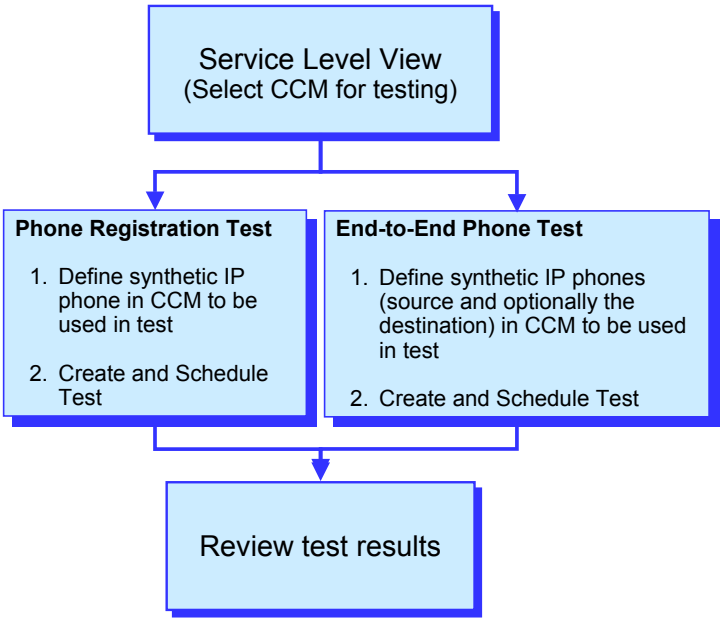
<Intentionally Left Blank>

Service Availability

- Getting Started
- Preparing OM for Initial Use
- Normal Operational Status
- **Service Availability Testing**
- Node-to-Node (IP SLA) Testing
- Experiencing Phone Outages
- Performance Monitoring



Scenario 4: CCM Service Availability Testing



CCM Service Availability Testing

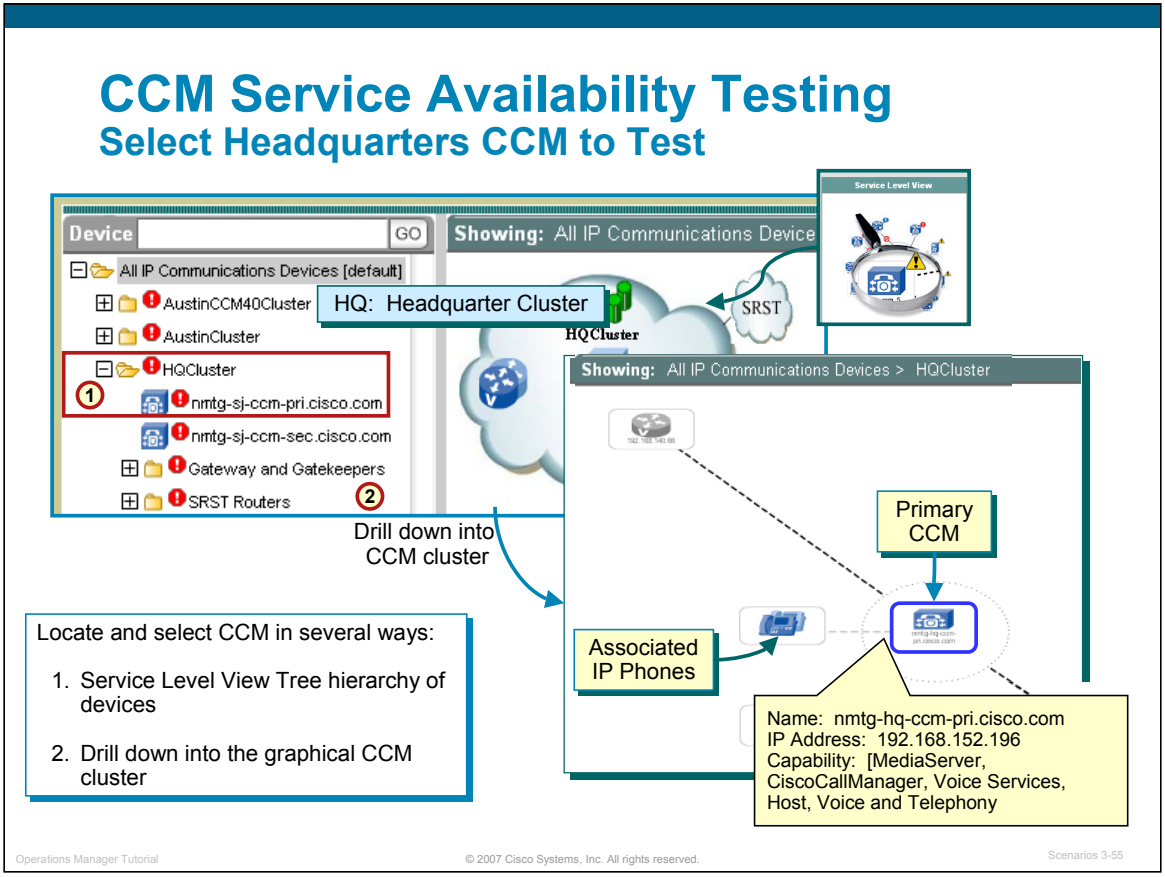
In this scenario, Susan will create and schedule a phone registration test to continuously check the service availability of the Cisco CallManagers at the company ABC headquarters and branch office.

The phone registration test is a diagnostic test using synthetic transactions created by Operations Manager. The transactions are tests that can be used to measure the availability of voice applications in the network. These tests verify whether the voice application can service requests from a user, such as verifying that phones can register with a Cisco CallManager (CCM).

This scenario goes through the exact steps for configuring this test.

Note(s):

You can only configure one Phone Registration test per Cisco CallManager.

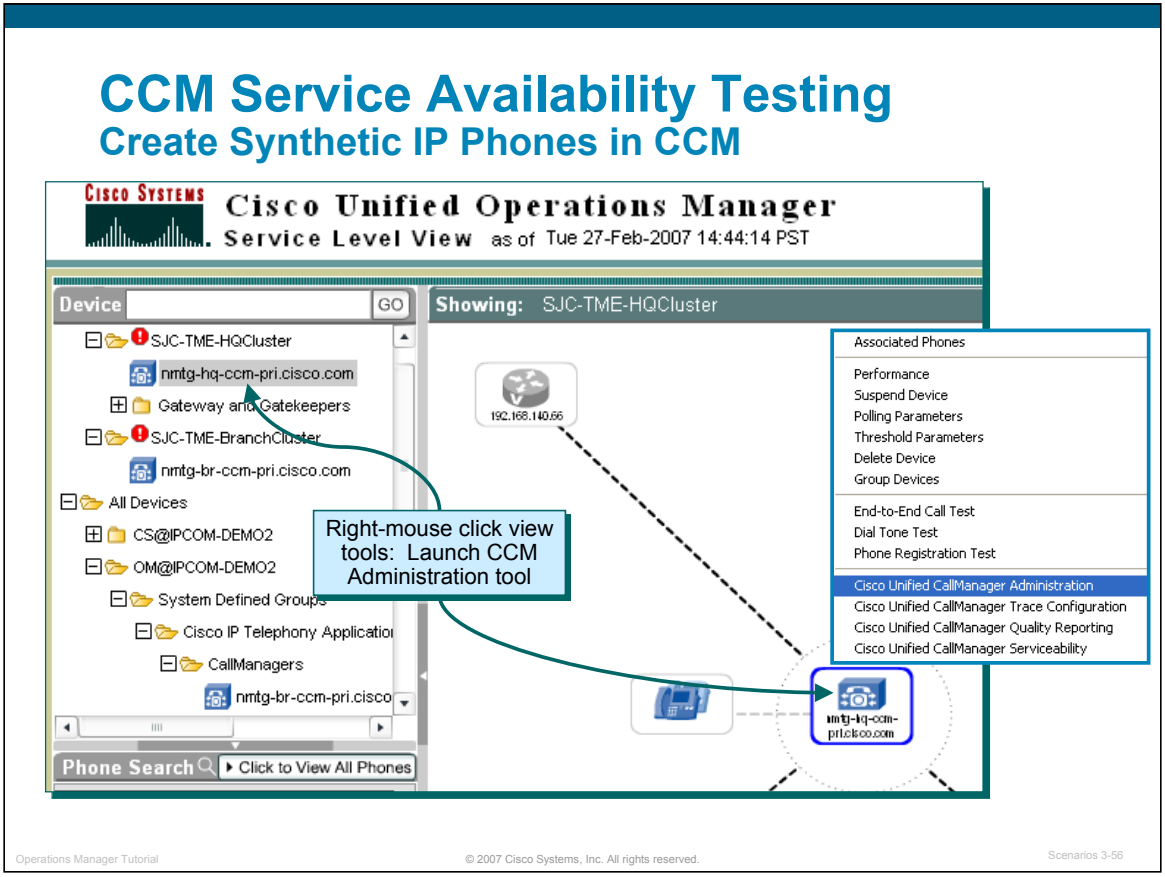


Select Headquarters CCM to Test

To configure this test, first locate the Cisco CallManager (CCM) to test. Susan will use the following steps:

Open the Service Level View, if not already opened.

Susan can either locate the CCM of interest and select it using the tree hierarchy in the Service Level View or by drill down into the graphical cloud that represents the CCM cluster. Either method produces the logical topology of the CCM cluster illustrated above. The CCMs are always located in the center circle and its logical relationships to other devices are shown with dashed lines.



Create Synthetic IP Phones in CCM

To create a synthetic test, Operations Manager must simulate other phones. The phone number and MAC address that Operations Manager uses as the simulated phone must be unique on the CCM (no other tests can use it) and configured in the CCM database as a Cisco 7960 phone. The MAC address for simulated phones must be between 00059a3b7700 and 00059a3b8aff.

To define these simulated phones in CCM, launch the CCM Administration tool. To launch the tool, Susan will follow these steps:

From the Service Level View locate the CCM as described in the previous step.

Right-mouse click on the CCM. This opens a menu of options which varies for different device types.

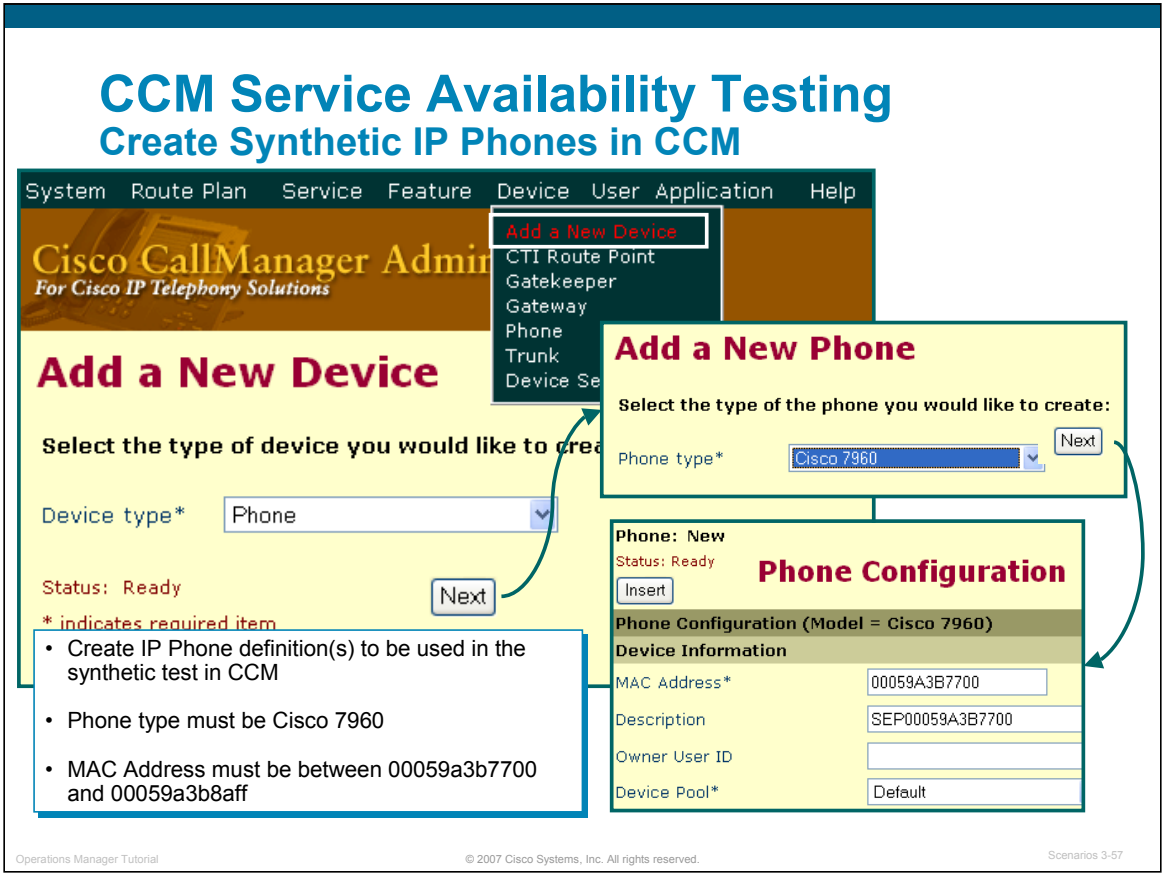
Select the option More Tools. This displays more options.

Select Launch CallManager Administration.

Note(s):

Create one phone extension number and one MAC address for each test and use it for that test only.

Make sure that the combination of the phone extension number and the MAC address used in a test is unique across the voice cluster.



Create Synthetic IP Phones in CCM

Now, create a new phone definition in the CallManager to be used in the synthetic test. This phone is a simulated phone and not a real phone. Using the CallManager Administration tool, define the IP Phone. It must be a Cisco 7960 phone and the MAC address for simulated phones must be between 00059a3b7700 and 00059a3b8aff.

To define a simulated phone in CCM, Susan will follow these steps:

Launch and login to the CallManager Administration as described in the previous step.

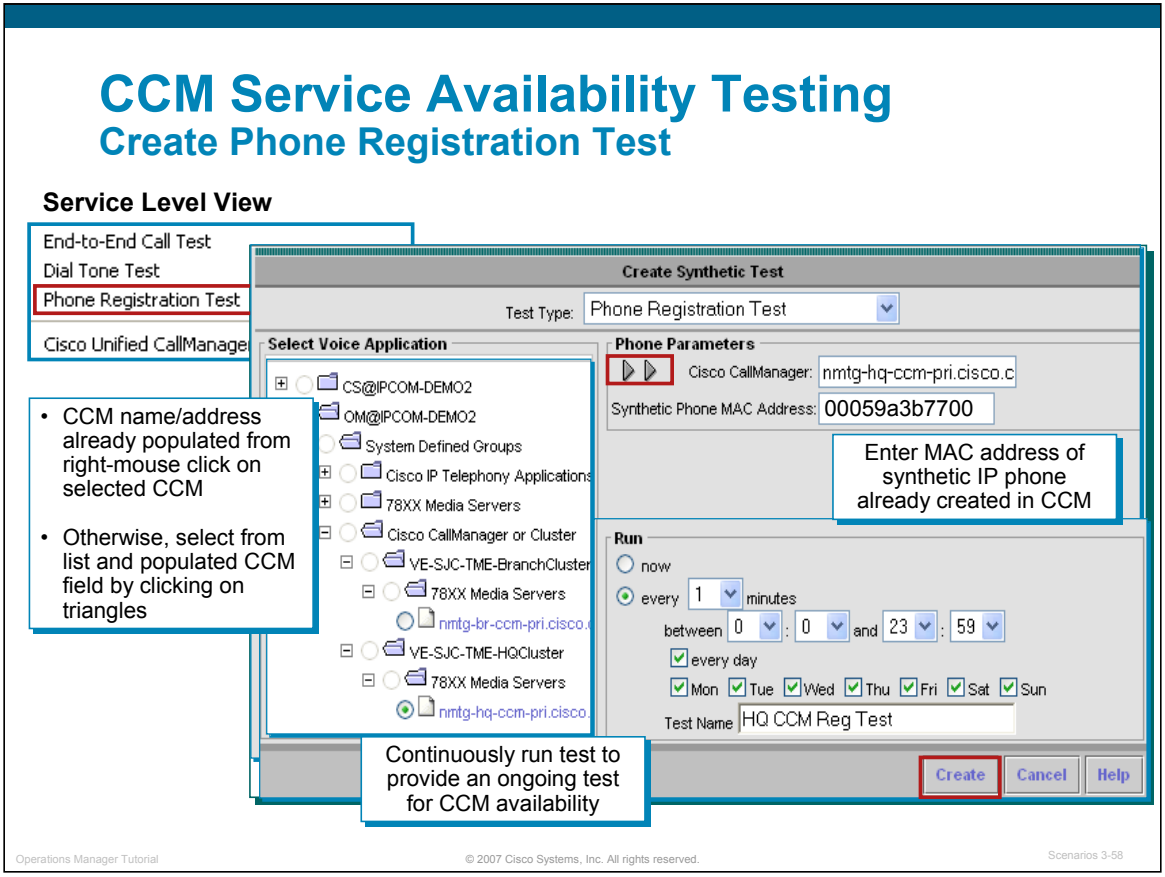
From the CCM Administration tool, select from the menu Device> Add a new Device.

Change the Device Type from the pull-down menu to Phone. Click Next.

The Phone type for the simulated phone must be a Cisco 7960. Select this model as the Phone type. Click Next.

In the Phone Configuration window, enter a MAC address between 00059a3b7700 and 00059a3b8aff. The Description field will be automatically filled in by the tool. Other required fields are the Device Pool and Button Template. Use the default. Click Insert.

The new IP Phone to be used in the synthetic test has been created.



Create Phone Registration Test

Once the simulated IP Phone(s) have been defined in the CCM, Susan will use Operations Manager to configure a synthetic test to occur on a regular basis to test the service availability for registering phones with the CCM. The phone registration test is a diagnostic test in Operations Manager using synthetic transactions. The transactions are tests that can be used to measure the availability of voice applications in the network. These tests verify whether the voice application can service requests from a user, such as verifying that phones can register with a Cisco CallManager (CCM).

The test configured here will continuously test whether the CCM at the headquarters can register the simulated IP Phone just created. To create the Phone Registration Test, Susan will follow these steps:

From the Service Level View locate the headquarters CCM as described in the earlier steps.

Right-mouse click on the CCM. This opens a menu of options which varies for different device types.

Select the option Phone Registration Test. The Create Synthetic Test window is displayed and the test type is set to Phone Registration Test.

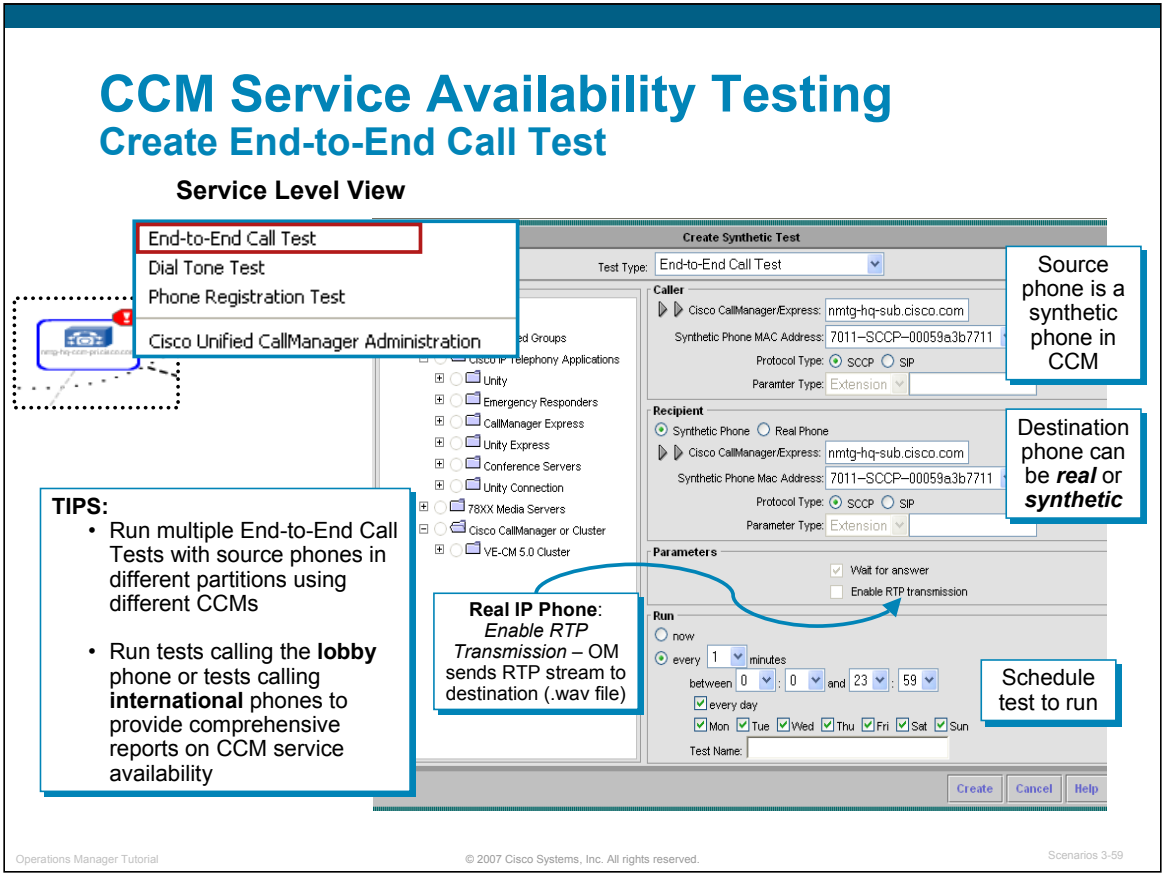
Since the test configuration was launched using the right-mouse click on the CCM of choice in the Service Level View, the Cisco CallManager field is already filled in. However, if the test is launched from the Operations Manager home page, the user can select the CCM using the tree hierarchy on the left of the window.

Enter the MAC address of the IP Phone that was defined in CCM and created on the previous page. Remember the MAC address must be between 00059a3b7700 and 00059a3b8aff.

Define the frequency for running the test. Susan wants to continuously run the test everyday to check for CCM service availability.

Click Create when done.

An additional test can be created using the above steps to also check the service availability of the Cisco CallManagers at the branch office.



Create End-to-End Call Test

Again, once the simulated IP Phone(s) have been defined in the CCM, Susan will use Operations Manager to configure a synthetic test to occur on a regular basis to test the service availability for making end-to-end calls in different partitions of the network.

The End-to-End Call Test verifies whether the CCM can initiate and complete end-to-end calling: phone requests/receives a dial tone from CCM, digits sent, ring indication received. To create the End-to-End Call Test, Susan will follow these steps:

From the Service Level View locate the headquarters CCM as described in the earlier steps.

Right-mouse click on the CCM. This opens a menu of options which varies for different device types.

Select the option End-to-End Call Test. The Create Synthetic Test window is displayed and the test type is automatically set to End-to-End Call Test.

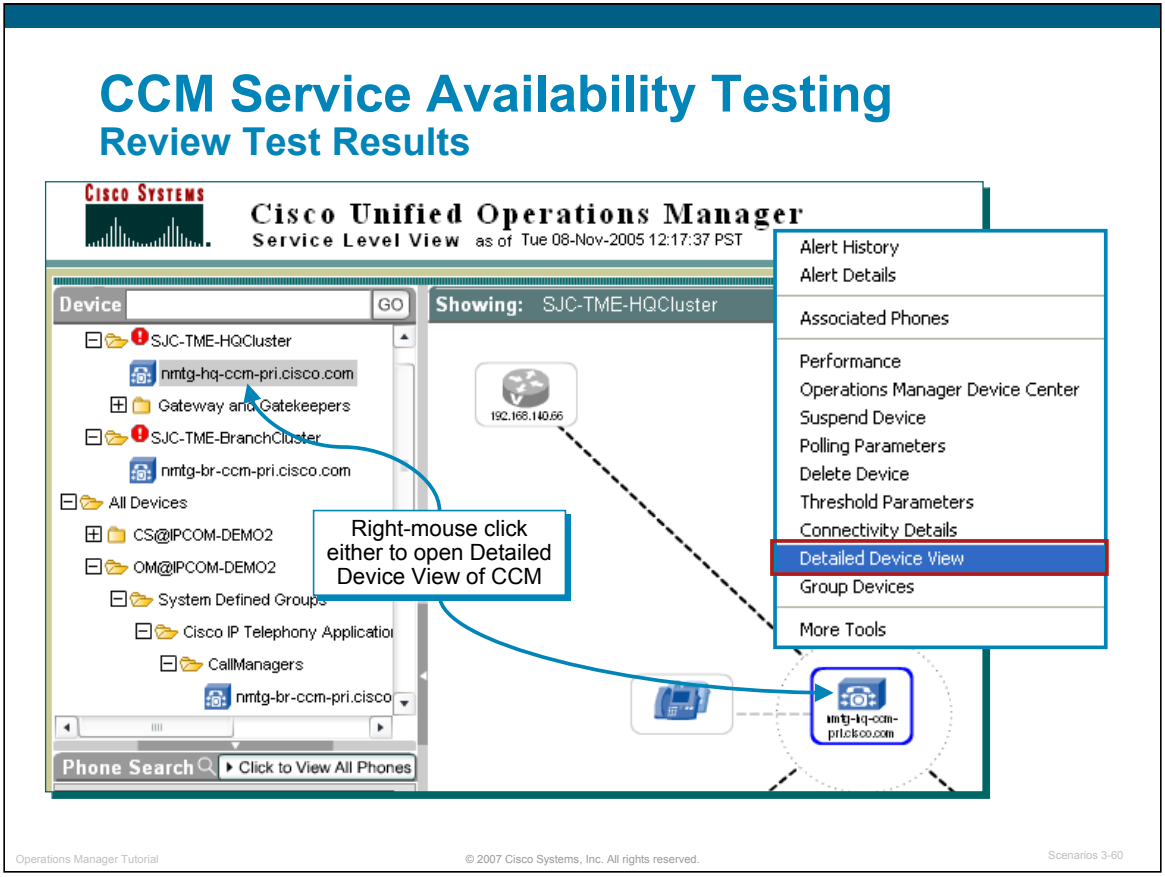
Since the test configuration was launched using the right-mouse click on the CCM of choice in the Service Level View, the Cisco CallManager field is already filled in. However, if the test is launched from the Operations Manager home page, the user can select the CCM using the tree hierarchy on the left of the window.

Enter the MAC address of the **source IP Phone** that was defined in CCM and created earlier. Remember the MAC address must be between 00059a3b7700 and 00059a3b8aff.

Define the **destination phone** for the test. The destination can be another synthetic phone defined in the same or another CCM or the destination can be a real device. Based on which type you choose, the parameters will change and be grayed-out for what is not needed. If synthetic, provide a CCM, MAC address, and extension; if real, provide only the phone extension;

Define the frequency for running the test. Susan wants to continuously run the test everyday to check for CCM service availability. Click Create when done.

A valuable use of this test is to create multiple tests that simulate the calls of phones in different partitions of the network. Run tests to ensure that calls be made to the phone in the lobby, to the phones in remote locations, and to international phones.



Review Test Results

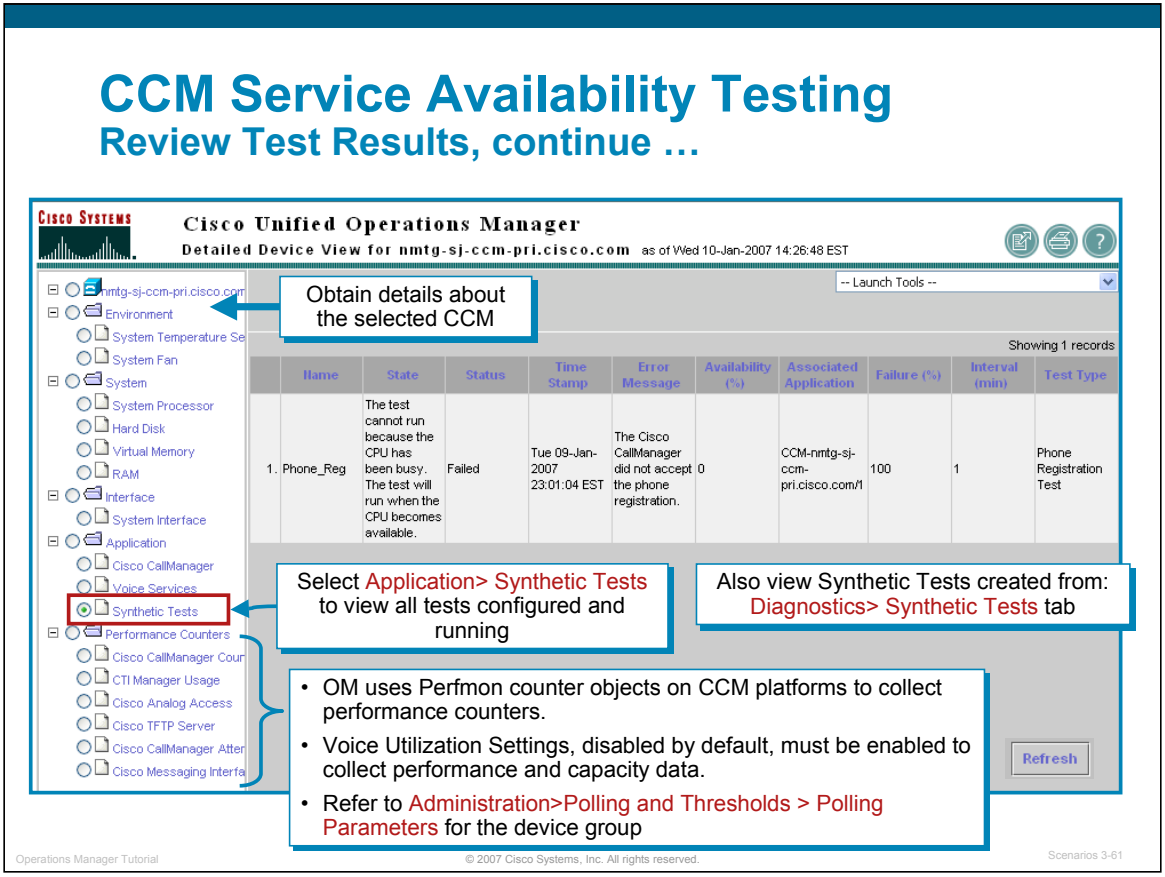
The Phone Registration Test is now up and running on a continuous basis. To view information about the test and the results, as well as other information about the CCM, Susan will use the Detailed Device View in Operations Manager. One way to launch this view is by following these steps:

From the Service Level View locate the headquarters CCM as described in the earlier steps.

Right-mouse click on the CCM. This opens a menu of available options for the CCM.

Select Detailed Device View from the pop-up menu. (see next page)

The Detailed Device View can be started in several other ways. For example, click the Device Name in a report or the device link in another view.



Review Test Results, continue …

The Detailed Device View provides extensive information on the selected device and the device's components. Susan launched the Detailed Device View on the CCM with the Synthetic Tests. To review the test and the test results, follow these steps.

From the Detailed Device View (started in the earlier steps), use the tree hierarchy and open the Application tree.

Locate and select Synthetic Tests in the tree hierarchy, as illustrated above. This will display all the synthetic tests configured and running on the device.

Review the test information. Notice that Susan will receive an alert in Operations Manager if either of the tests fail more than 50% of the time.

In the Detailed Device View, you can do also do the following:

View hardware and software information on system, environment, connectivity, and interface components

View hardware and software information on subcomponents of aggregate devices

View application status for Cisco CallManager, Voice Services, Work Flow, and Synthetic Tests (illustrated above), and provide launch points for administrative pages, if appropriate

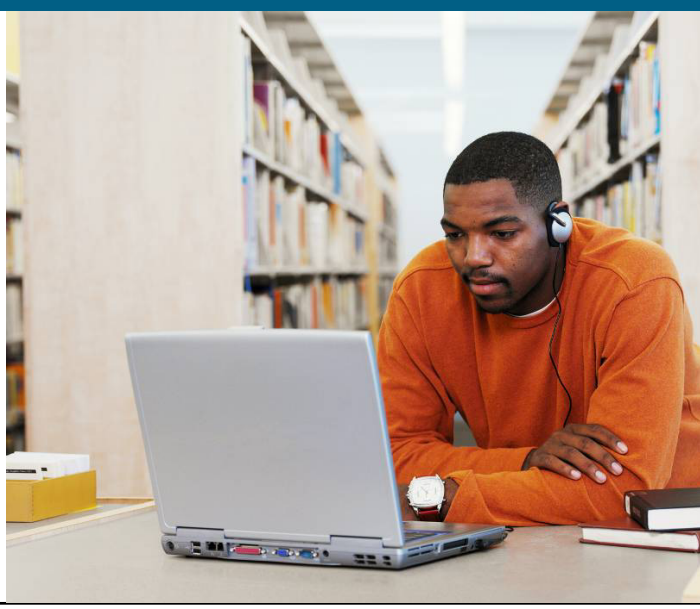
Suspend or resume management of a device or a device component so the device is no longer polled, or polling is resumed

Launch other Operations Manager tools

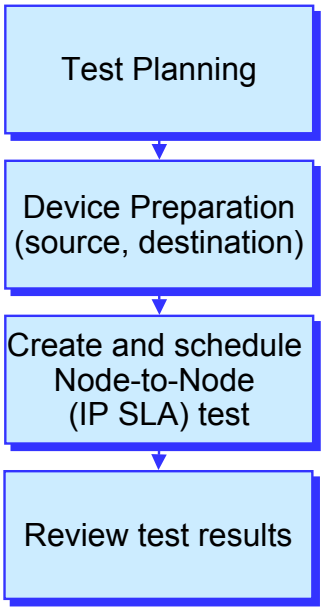
<Intentionally Left Blank>

Node-to-Node (IP SLA) Testing

- Getting Started
- Preparing OM for Initial Use
- Normal Operational Status
- Service Availability Testing
- **Node-to-Node (IP SLA) Testing**
- Experiencing Phone Outages
- Performance Monitoring



Scenario 5: Node-to-Node Testing
Outline



Node-to-Node (IP SLA) Testing

Node-To-Node tests monitor the response time and availability of multi-protocol networks on both an end-to-end and a hop-by-hop basis.

At Company ABC site-to-site communications is being deployed across the IP network. Continuously monitoring of its quality is crucial to its business operations. Susan knows that voice and video are more sensitive to network delays. Thus, the Node-to-Node test in Operations Manager (test type Data Jitter) can be used to simulate voice traffic from the headquarters to the remote site and measure the response time of the traffic. After collecting this data, Susan can use the graphing function in Operations Manager to examine changes in network performance metrics in real-time.

This scenario will look over the shoulder of Susan and watch her select the devices used in the test, ensure that they are properly configured, create the Node-to-Node test (Data Jitter), and look at the preliminary results.

Other tests besides Data Jitter are also available in Operations Manager. Chapter 2 of this tutorial provides additional details on all the Node-to-Node tests available.

Node-to-Node (IP SLA) Testing
Test Planning

Reason for Test

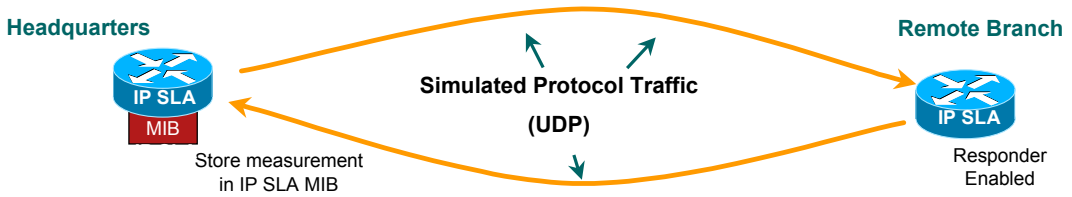
- Ensure Voice Quality is acceptable in the network (headquarters to remote branch) by running a Data Jitter Test

Measurements / Metrics

- Round Trip Latency | Packet Loss | Network Jitter | Dist. of Stats | Connectivity

Test Parameters

- End Points: Select IP SLA device at headquarters to initiate test traffic
- Protocol to Simulate (UDP)
- Threshold to detect condition – 3% packet loss, 40 ms jitter (either direction)



Node-to-Node (IP SLA) Testing – Test Planning

Start with a plan, and the rest will be easy. In this scenario, Susan, our network engineer, came up with a monitoring plan and has highlighted the following key points:

- Site-to-site communications is being deployed across the IP network. Continuous monitoring of voice quality is crucial to business operations.
- The Node-to-Node test in Operations Manager (test type Data Jitter) will be used to simulate voice traffic from the headquarters to the remote site and measure the response time of the traffic.
- Since many network design changes will be occurring throughout the year, the end-to-end network latency tests will run continuously to ensure consistency in the network latency.
- Cisco's IP SLAs feature embedded in Cisco IOS routers will be used to simulate the traffic and measure the latency and jitter. Since the test will be continuously run for a long period of time, the network administrators may wish, at a later date, to deploy some unused Cisco 2500 routers that they have sitting on the shelf for the source device and the target device instead of production routers. The target device at the remote branch must also be a IP SLA capable router to monitor voice traffic and report on Jitter statistics.
- Susan knows that voice and video are more sensitive to network delays. Thus, running additional tests and varying the IP Precedence level from 5 to other values can help to evaluate the importance of using varies QoS features in routers by prioritizing delay sensitive traffic in the network.
- The conditions to look for will be a 3% packet loss or 40 ms jitter (either direction). For more information on what jitter is, please refer back to Chapter 2 of this tutorial.

Node-to-Node (IP SLA) Testing
Device Preparation

Source Device (Headquarters)

- IP SLA capable and enabled; verify IOS version supports IP SLA test operation
- SNMP community strings (RO, RW) configured on device
- SNMP trap recipient defined (I.e. Operations Manager server)
- Device managed in the Operations Manager inventory and the device credentials configured in the DCR match those on device

Step	Action
1	router> **enable**
2	router# **configure terminal**
3	router(config)# **snmp-server community** <*string*> **ro**
4	router(config)# **snmp-server community** <*string*> **rw**
5	router(config)# **snmp-server host** <*IP_address*> <*trap_community_string*> **rtr**
6	router(config)# **snmp-server enable traps rtr**

Node-to-Node (IP SLA) Testing – Device Preparation

Once the source of the test operation has been identified and the device has been selected at our headquarter location, the source device will need to to be configured.

First, check the IOS version of the source device. IOS release 11.2 is the earliest and first release that support the IP SLAs (formerly known as RTR or SAA). Note that not all SLAs test operations are supported in later IOS releases.

Additionally, a few device configuration commands need to be configured in order to configure IP SLAs using Operations Manager and have IP SLA-related traps forwarded to a network management station (NMS). These commands are outlined in the figure above and discussed below.

- Operations Manager uses SNMP to define the IOS IP SLA and to extract the data in the IP SLA MIB in the source device. Both the SNMP read-only (ro) and read-write (rw) community strings need to be configured on the source device.
- Optionally, to receive traps at a NMS, like the Operations Manager server, when a test exceeds a specified latency threshold, verify that the source device is set up to send IP SLA-generated traps. The SNMP keyword rtr limits the traps sent to the specified address to IP SLA-related traps. If the keyword rtr is omitted, all default SNMP traps are sent to the named network management host including IP SLA-related traps.

Step	Action
1	router> **enable**
2	router# **configure terminal**
3	router(config)# **snmp-server community** <*string*> **ro**
4	router(config)# **snmp-server community** <*string*> **rw**
5	router(config)# **snmp-server host** <*IP_address*> <*trap_community_string*> **rtr**
6	router(config)# **snmp-server enable traps rtr**

Node-to-Node (IP SLA) Testing
Device Preparation

Target Device (Remote Branch)

- This scenario uses the Data Jitter Test:
  - Target device must also be an IP SLA capable device,
  - Responder must be enabled (refer to notes)
  - Cisco IOS version 12.1(2)T or later
- Other tests (Echo, Path Echo): Target device can be any reachable IP host

Step	Action
1	*router>* **enable**
2	*router#* **configure terminal**
3	router(config)# **snmp-server community** *<string>* **ro**
4	*router(config)#* **rtr responder**

Starting with IOS 12.3(14)T, the keyword "rtr" in the IOS command line interface will be replaced with "ip sla".

Node-to-Node (IP SLA) Testing – Device Preparation

Once the target or destination of the test operation has been identified and the device has been selected at our headquarter location, the target device may also need to to be configured.

In most test operations (Echo, Path Echo), the destination can be any IP host. Of course, the host must be reachable by the source device, but no other configuration is needed.

In this scenario, we want to use the Data Jitter test to measure voice quality. This type of test requires a Cisco IOS Device with the IP SLA Responder enabled - A target device that is running Cisco IOS software can be configured as a Responder, which processes measurement packets and provides detailed timestamp information. The device must be reachable by the source device. If the SNMP read community string is configured, then Operations Manager can read the device information, the IP SLA version, and determine if the responder is enabled. To use the IP SLAs Responder feature, it must be enabled, using the command below.

Note(s):

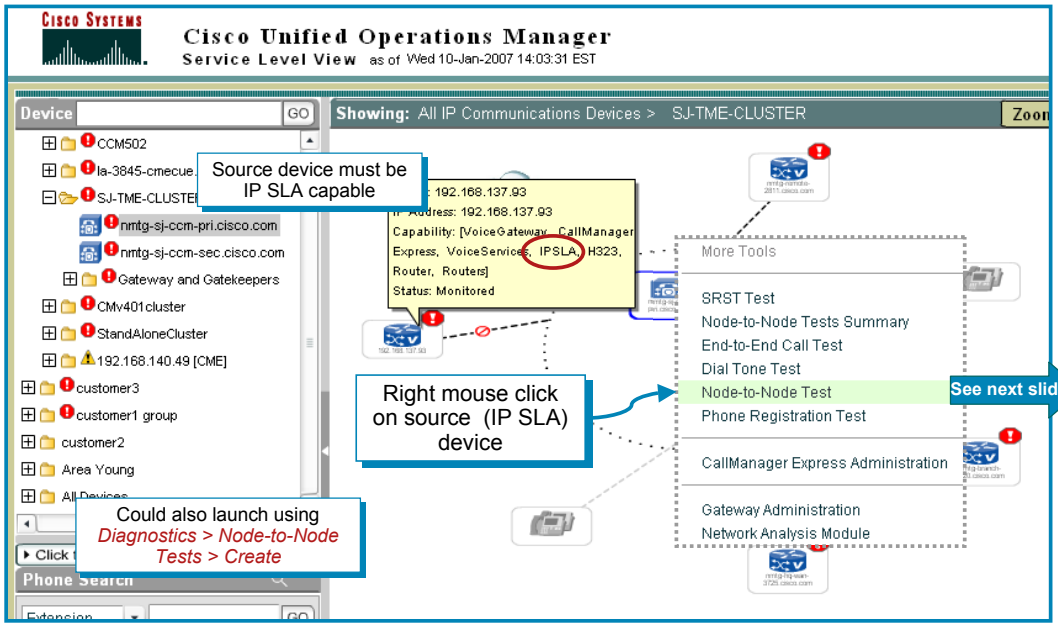
- Starting with IOS 12.3(14)T, the keyword "rtr" in the IOS command line interface will be replaced with "ip sla".
- Certain test operations, like Data Jitter, use the IP SLA functionality in Cisco routers at the destination device. To enable the RTR responder in the IP SLA router, issue the following command under the global configuration mode:

```
router(config #) rtr responder
router# show rtr responder
```

- Use the following show command to verify which IP SLA operations are available in the Cisco IOS device.

```
router# show rtr application
```

Node-to-Node (IP SLA) Testing
Select Source Device to Configure Test



Select Source Device to Configure Test

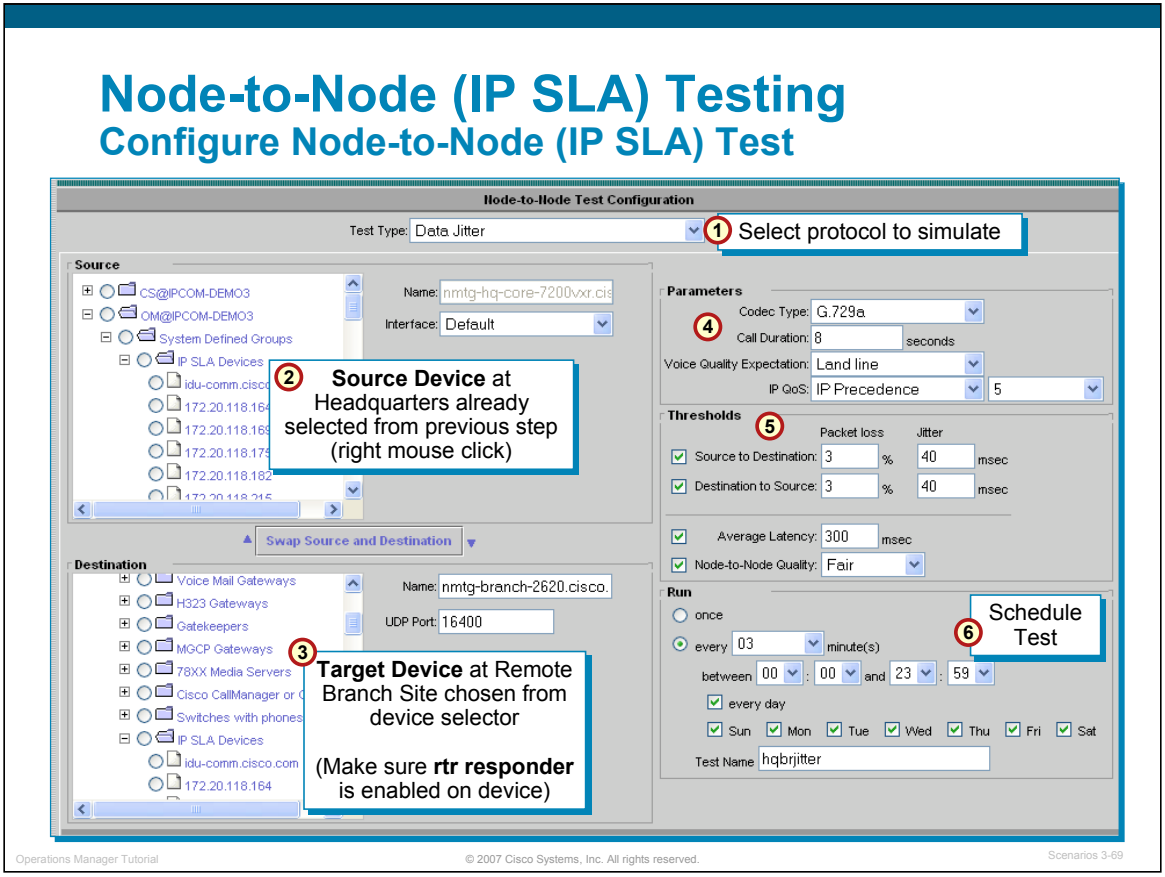
Operations Manager has several ways to create a Node-to-Node diagnostic test.

One way is to use the home page of Operations Manager.

1. Select **Diagnostics > Node-to-Node Tests**. The Node-to-Node Tests page appears and lists all currently configured tests, if any exist.
2. Click **Create** to configure a new test. (Illustrated on next page.)

Another way is to use the context sensitive menus in the Service Level View dashboard, as illustrated above. If a device is capable of generating a Node-to-Node test, the test will be displayed in the menu options when you right-mouse click on it.

1. Locate the source device in the **Service Level View** dashboard. Ensure that the device is IP SLA capable by simply placing the cursor over the device in the view.
2. Right-mouse click on the device.
3. Select **Node-to-Node Test**. The Node-to-Node Tests page appears and will have the source device field completed with the device that you selected in the Service Level View dashboard. (The **Node-to-Node Test Summary** menu option displays all tests currently configured, if any exist.)



Configure Node-to-Node (IP SLA) Test

The information required for creating a Node-to-Node test are different for each test operation type. In this scenario, Susan wants to ensure that voice quality is acceptable in the network (headquarters to remote branch) by using a Data Jitter test. Susan will follow these steps to configure this test on the source device.

1. In the Test Type pull-down menu select **Data Jitter**.
2. In the **Source** pane, the source device should already be entered since the test was started by right-mouse clicking on the device from the Service Level View. If not the right device, use the device selector to the left and select a source device that meets the requirements stated earlier.

   Select a **source interface** setting. You can leave it as **Default**, or enter a new setting.
3. In the **Destination** pane, use the device selector on the left to select a destination device that meets the requirements stated earlier for the target device.

   Enter a **UDP port** for the destination device (the default value is **16400**). This is the port on the destination device to which packets are sent by the source device.

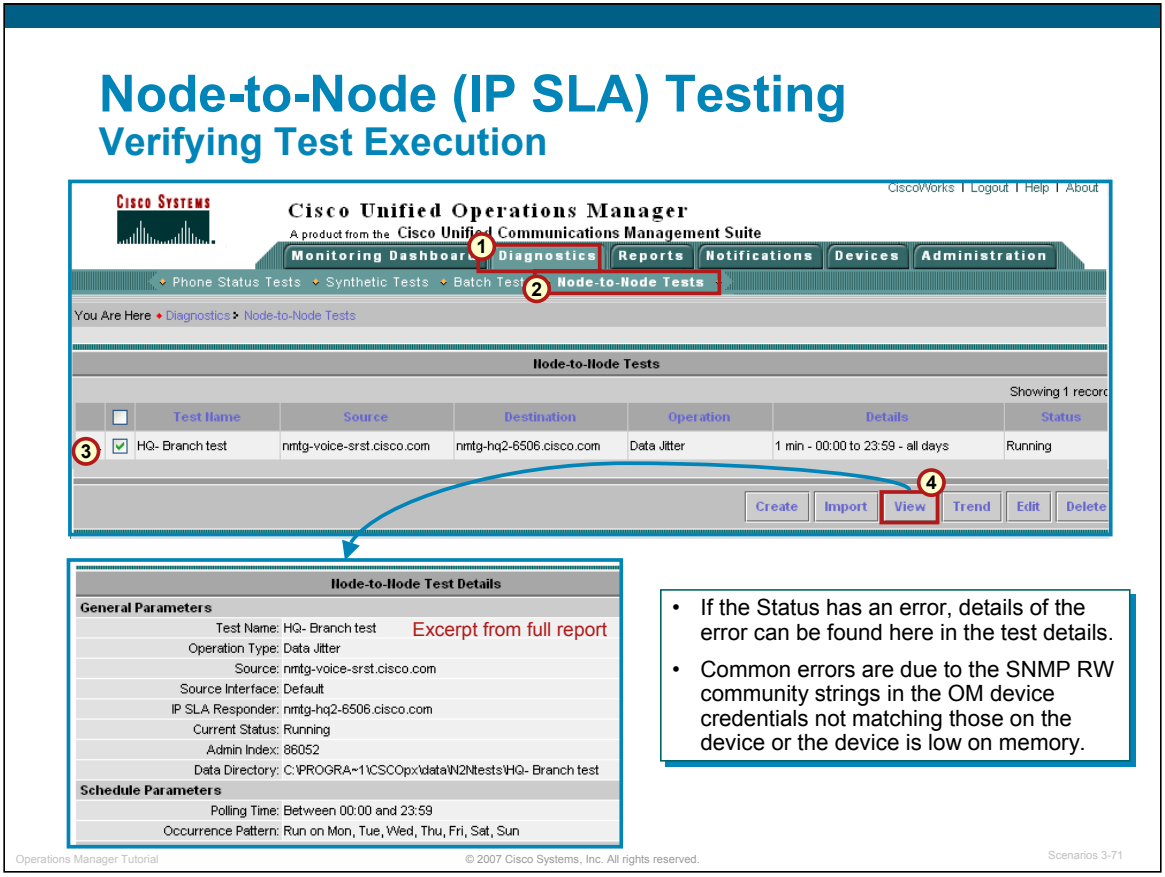
   Note that if you want to switch the source and destination devices with each other, click the *Swap Source and Destination* button.
4. In the **Parameters** pane,set the following parameters:
   - Codec – Select one type. It is used to determines the packet interval and the request payload.
   - Call Duration – must be less than 60 seconds and is the time of the call simulated
   - Voice Quality Expectation – Select one. This selection corresponds to the Access Advantage factor of Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF).
   - IP QoS – Defines the packet header settings for the simulated traffic and is used by the interconnect devices prioritize packets based on quality of service policies.

<steps continue from previous page… >

5. In the **Threshold** pane you can change the following settings:
    a. Source to Destination threshold – the default threshold setting is 3% (packet loss) and 40 msec (jitter)
    b. Destination to Source threshold – the default threshold setting is 3% (packet loss) and 40 msec (jitter)
    c. Average Latency – the default threshold setting for latency is 300 m/secs
    d. Node-to-Node Quality – the setting can range from Excellent to Poor is the the threshold setting for the test's quality. Set the field to **Fair**.
6. In the **Run** pane, configure when the test should run. In this scenario, we want the test to continuously run at defined interval. Therefore, do the following.
    a. Select the schedule radio button.
    b. Choose to run the test every 3 minutes to provide a level of granularity desired.
    c. Run the test all day.
    d. Choose to run the test everyday, including weekends.
    e. Enter a test name. The test name cannot contain tabs, question marks, quotation marks, asterisks, semicolons, commas, colons, forward slashes, straight slashes, or backslashes.
7. Click **OK** when ready to configure.
8. If the SNMP RW community string credential has not been set for the source device, you will be prompted for it. You can also define these credentials by using the Operations Manager task **Devices>Device Credentials.**

Note(s):

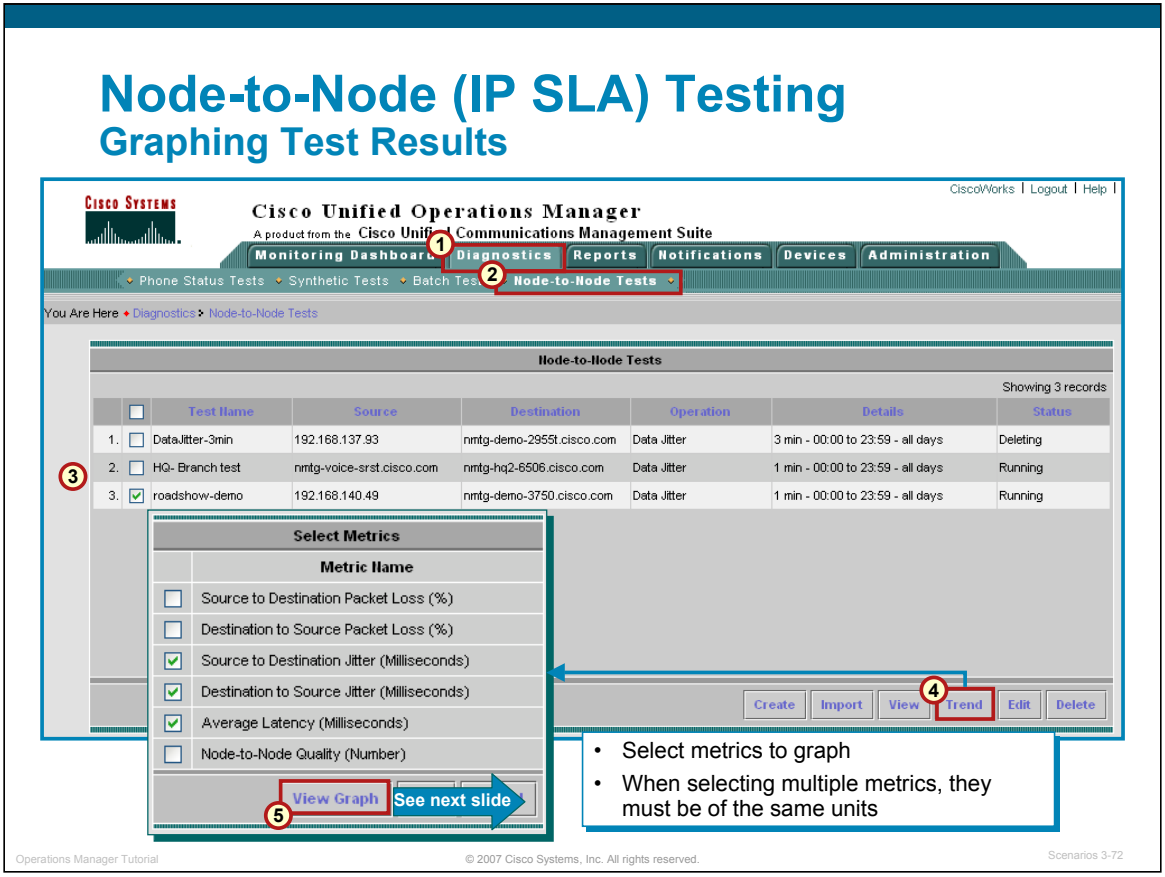
- The other Echo tests also provide response time information and do not require another IP SLA device as the target, but they do not provide the Jitter measurement.
- Also note that there is a test to measure call setup time using SIP or H323 and a test to measure the time required for a gateway to register with a gatekeeper.



Verifying Test Execution

You can verify whether a test ran and completed correctly. You can also troubleshoot the test, if necessary, by following these steps:

1. Select **Diagnostics > Node-To-Node Tests**. The Node-To-Node Tests page appears. All current Node-To-Node tests appear in this page. The last column in the table shows the status of each test.
    - Configuring - Either the device is not responding or configuration of the test is under way.
    - Scheduled - Displays after you create or update a test. The status will change to “Running” at the first polling cycle.
    - Running - The test is active and collecting data.
    - Delete Pending - Intermediate state, before the test is deleted. No actions can be performed on the test.
    - Suspended - The test is suspended from data collecting or polling. This occurs because the device was suspended.
    - Dormant - The test is active but not currently collecting data. Tests are in the Dormant state between polling cycles.
    - Error - The test was not configured correctly. Possible problems include incorrect device credentials or low device memory. You can see more information on why the test configuration failed by viewing the details in the Current Status field when selecting the ***View*** button.
2. Click **View** to review the test configuration parameters. The illustration above only displays some of the parameters; the other parameters that are viewable are the operation-specific parameters (IP Precedence value, Codec, UDP port used, threshold values, and more.



Graphing Test Results

Node-To-Node tests monitor the response time and availability of multi-protocol networks on both an end-to-end and a hop-by-hop basis.

The Data Jitter test, created in this scenario, uses the UDP protocol to measure latency, one-way jitter, and packet drop. Jitter is interpacket delay. The source device sends a number of packets from the source device to the destination device with a specified interpacket delay. The destination (an IP SLA Responder) time stamps the packet and sends it back. Using this data, the one-way positive and negative jitter (from the source to the destination and back again), packet loss (also from the source to the destination and back again), and round trip latency are obtained.

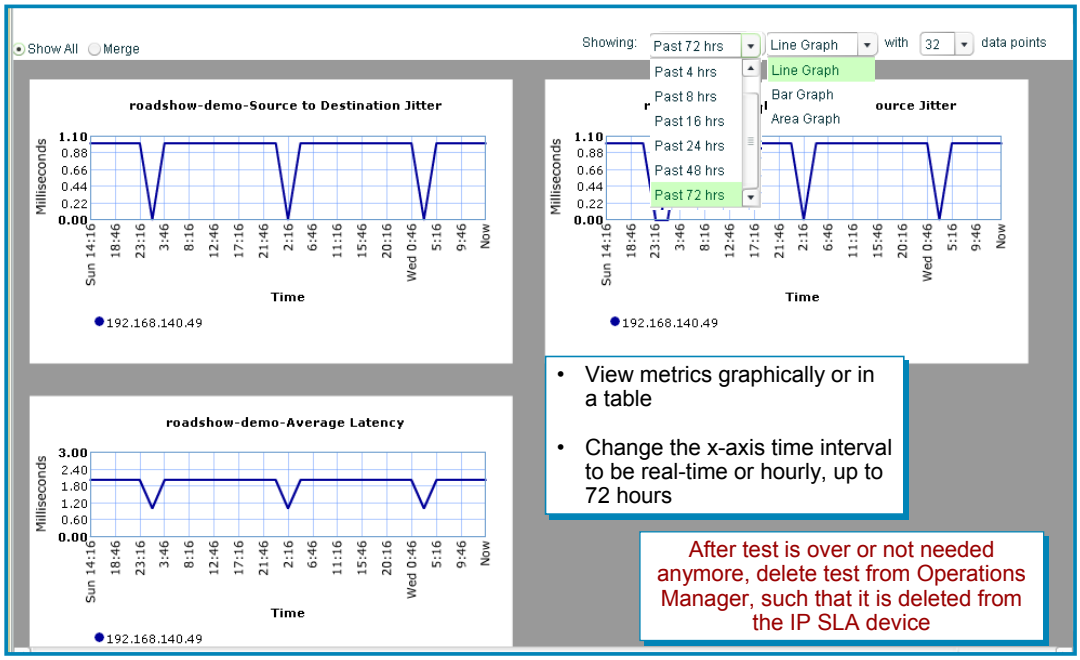
Positive jitter occurs when the one-way delay for a packet is longer than the previous packet delay. Negative jitter occurs when the one-way delay for a packet is shorter than the previous packet delay. If the sequence numbers become jumbled, the test reflects the error.

After running the test for awhile, Susan can use the Operations Manager graphing function to examine changes in network performance metrics. She can select, display, and chart network performance data in real-time. To view / graph the test results, Susan follows these steps:

1. Select **Diagnostics > Node-To-Node Tests**, if not already at the Node-To-Node Tests page. All current Node-To-Node tests appear in the page.
2. Select the Jitter test by selecting the checkbox next to its name.
3. Click the **Trend** button.
4. Select one or more metrics to graph. The metrics must be of the same units to graph together. The illustration above graphs the latency against the jitter in milliseconds.
5. Click the **View Graph** button.

Node-To-Node tests can also be configured to trigger events when certain thresholds are crossed. These events (Alerts on a device) appear in the Monitoring Dashboard displays.

Node-to-Node (IP SLA) Testing
Review Test Results



Review Test Results

Operations Manager allows Susan to select and examine changes in network performance metrics. She can select, display, and chart network performance data generated by the Node-to-Node test. By selecting the statistics from the previous dialog and selecting the View Graph button, Operations Manager displays the performance metrics as a graph or in tabular format.

Up to four graphs can be plotted at one time.

To choose either a graph or tabular display, choose the desired tab located at the top right of the page, under the window tools area. There are three types of graphs that you can display: line graph, bar graph, or area chart. Choose the type of graph you want displayed by selecting it from the Type of Graph pull-down menu located on the top right of the graph.

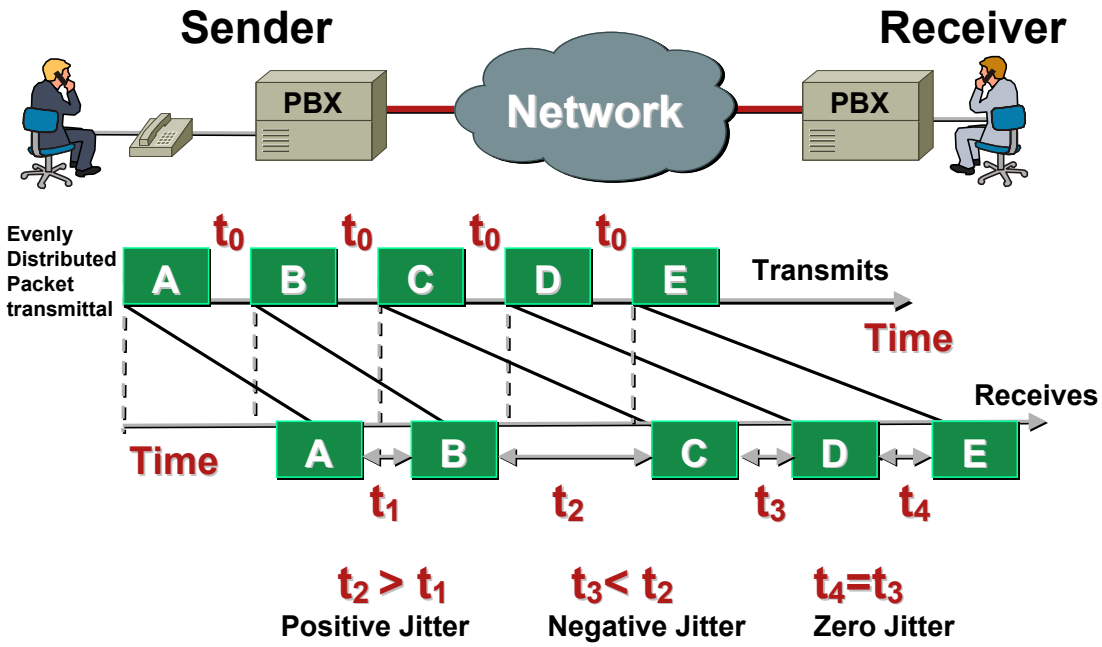
The information in a graph can be viewed as a snapshot in time or it can be refreshed at regular intervals by selecting a time interval or Real Time from the Time Interval pull-down menu located above the graph.

Susan is very pleased with the latency and jitter values seen here in real-time. She will leave the test running and if at any point certain thresholds are crossed, these events will appear in the Monitoring Dashboard displays as alerts on managed devices.

Note(s):

- The data files for the node-to-node performance metrics are located on the server, in the <OM installed directory>\data\N2Ntests directory. The data files in this folder are purged after 31 days.
- If you select a device that does not have data available for the selected time interval, a message appears stating such. An empty graph appears. The graphical display opens, but it does not automatically refresh even if Real Time is selected in the Time Interval pull-down menu. You must manually refresh the data by using the browser refresh after a period of time. Once the graph displays data, if Real Time is selected, the graph will refresh automatically. At any time, you can change the time interval to get historical information, if there is any.

Node-to-Node (IP SLA) Testing
Understanding Jitter



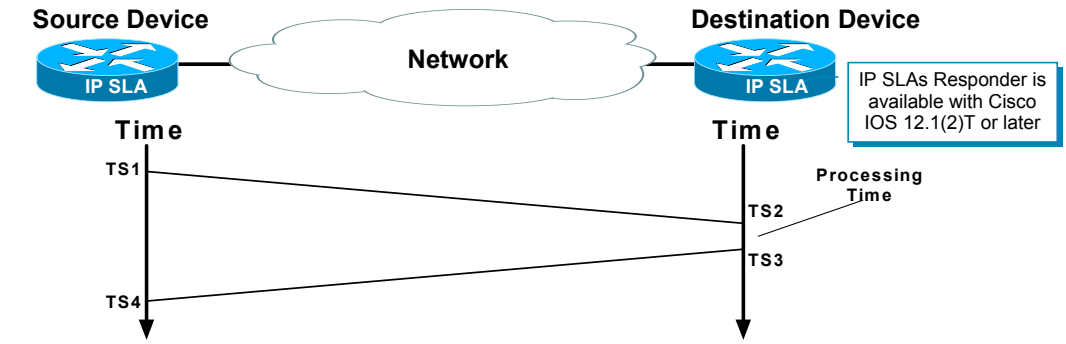
Understanding Jitter

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 a packet inter-arrival time greater that the inter-arrival time of the previous packet. If the previous packet arrived 10 milliseconds apart from its previous packet and this packet arrived 12 milliseconds from its previous packet, then positive jitter is equivalent to two milliseconds. Negative jitter is computed similarly. Greater value for positive jitter is undesirable for voice networks, and a jitter value of zero is ideal for delay-sensitive networks.

Node-to-Node (IP SLA) Testing
Understanding Round Trip Latency



Round-Trip Delay (With or Without IP SLAs Responder)

- (With IP SLAs Responder test eliminates processing time by destination device)
  - (TS4 – TS1) – (TS3 - TS2)
- (Without IP SLAs Responder enabled, the delay includes processing time by destination)
  - TS4 - TS1

One-Way Delay (Requires IP SLAs Responder enabled)

- TS2 – TS1

Understanding Round Trip Latency

This figure can help you to understand how the round trip latency values are computed.

As illustrated, when using the IOS Responder as the destination device (available in Cisco IOS version 12.1(2)T or later), processing delays can be minimized by computing the destination's processing delay time and subtracting it from the total round-trip time.

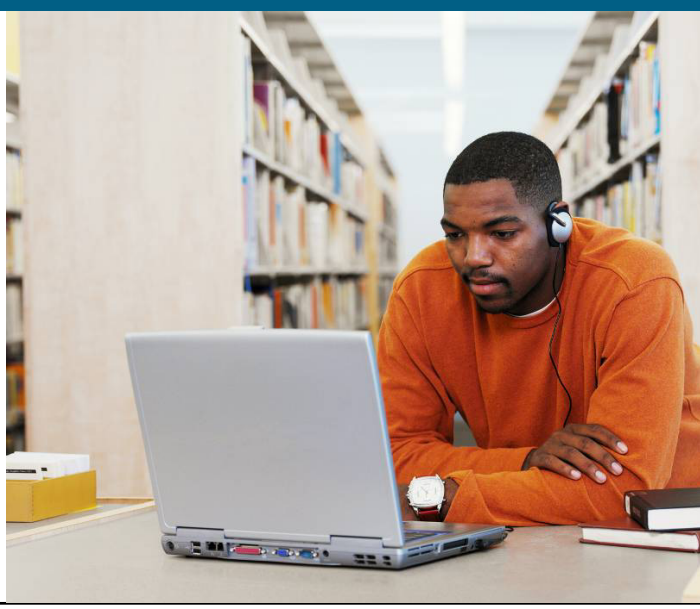
Routers sometimes take tens of milliseconds to process incoming test packets, due to other high priority processes. This delay affects the response times computed, because the reply to test packets might be sitting on queue while waiting to be processed. Therefore, the response times would not accurately represent true network delays.

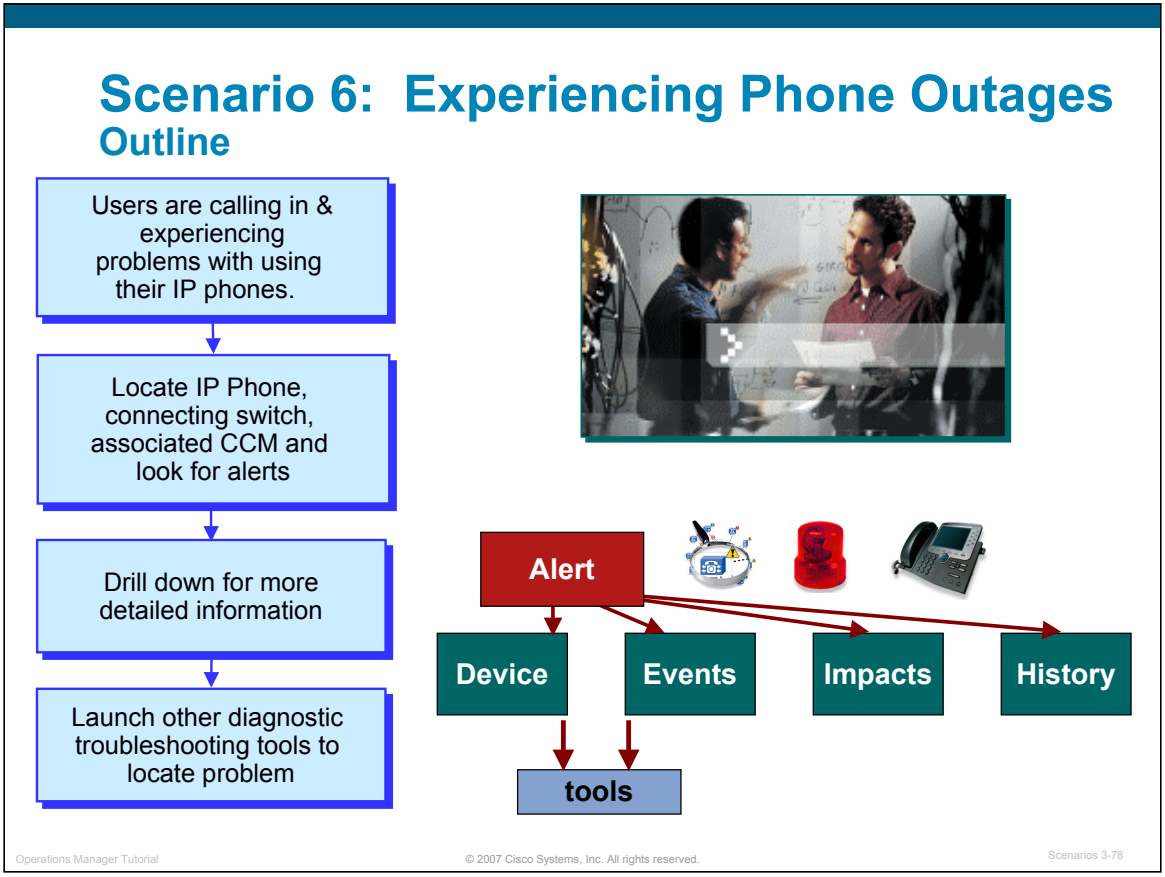
IOS IP SLAs minimize these processing delays on the source device as well as on the destination router (if the IOS Responder is being used), in order to compute true round-trip times. It does so by time stamping the test packets at the destination device.

<Intentionally Left Blank>

Experiencing Phone Outages

- Getting Started
- Preparing OM for Initial Use
- Normal Operational Status
- Service Availability Testing
- Node-to-Node (IP SLA) Testing
- **Experiencing Phone Outages**
- Performance Monitoring





Experiencing Phone Outages

This scenario looks at the work flow for helping to diagnose IP phone related problems using Operations Manager. Users are calling and reporting periodic clipping or outages. The Help Desk collects information from the users and then utilize the features in Operations Manager to help diagnose the problems.

Let's follow along. (This scenario assumes that the previous scenarios have been completed.)

Experiencing Phone Outages
Collect Important Information

Employee:

- Called to complain of poor quality using the IP phones.
- The Help Desk operator collects important information from the caller.

Help Desk:

- What is the employee's name and their extension? Bill, x1003
- What facility or location is the employee located in? Headquarters
- What is the type of problem that they are experiencing? Clipping of voice
- Using Operations Manager locate the IP phones, transport devices, and services having the problem.

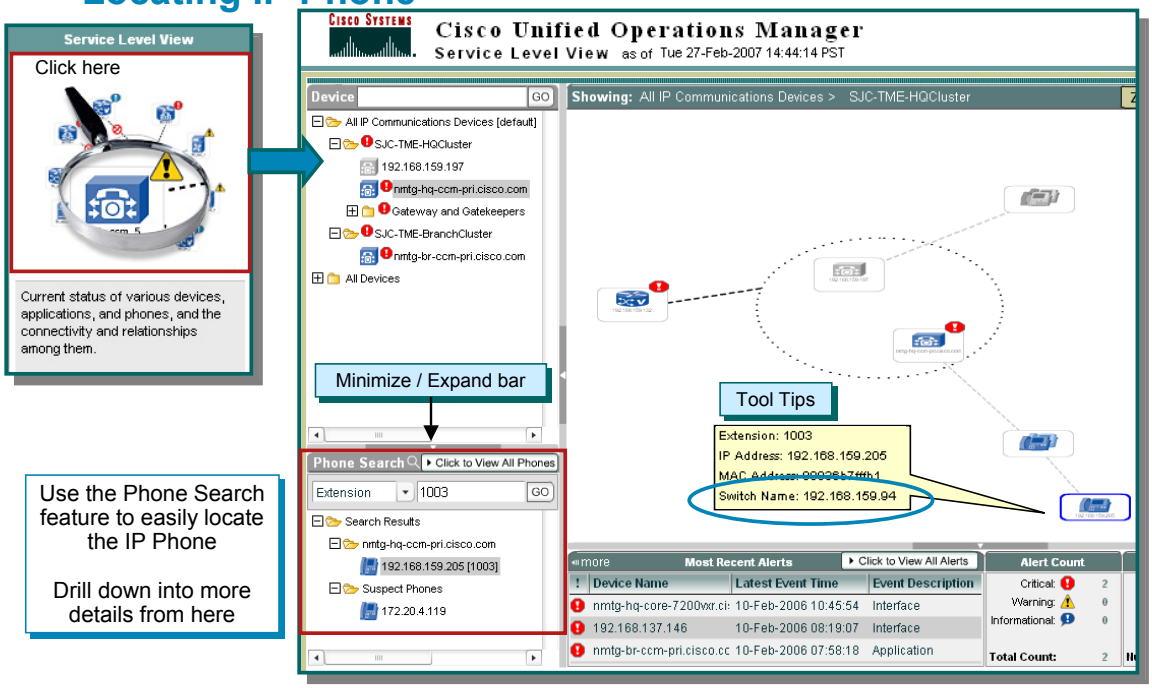
Collect Important Information

An employee of Company ABC is having problems with their their IP phone. The quality is poor, making it difficult to have a conversation using the phone. The employee decides to call the company Help Desk to see if they can locate the problem.

The Help Desk first collects important information from the caller, such as the employee's name, their phone extension, the type of problem they are having, and when the problem typically occurs (morning, afternoon, or after hours).

Once the information is collected, the Help Desk can use Operations Manager to locate the IP phones, transport devices, and services having the problem. In addition, diagnostic tests and be create to help troubleshoot the problem. So let's launch Operations Manager and follow along.

Experiencing Phone Outages
Locating IP Phone



Locating IP Phone

An IP phone has a physical relationship with a switch and a logical relationship with a Cisco CallManager (CCM). So the Help Desk can run IP phone reports to provide a combined view of both of these relationships, making it easy for them to track and resolve IP phone related problems.

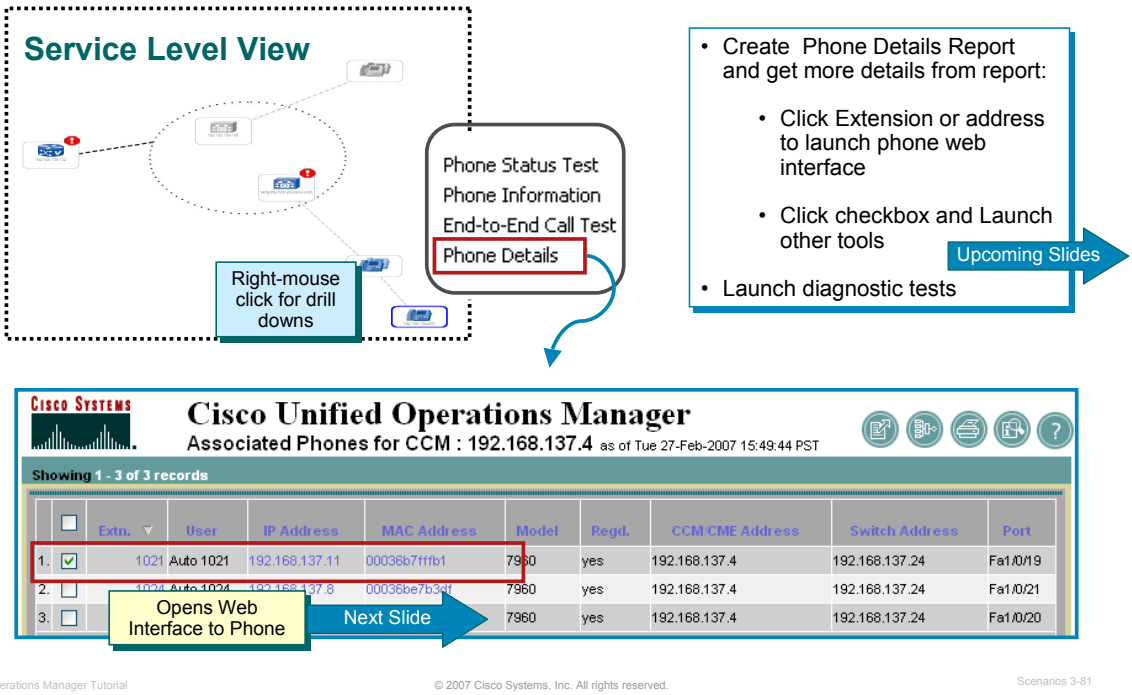
As illustrated above, locating the IP phone in question is easy from the Service Level View and by following these steps:

1. From the Service Level View, use the Phone Search feature in the lower left corner. (If you don't see this feature, it may be minimized. Click the Expand bar.)
2. In the Phone Search dialog, enter the Extension (I.e. 1003), IP or MAC address and click Go. The results are illustrated in the Search Results section.
3. Click on the phone in the Search Results section when found. The topology is updated, highlighting the phone in the topology (logical view).
4. Using the Tool Tips (place cursor over the phone), the connecting switch name is displayed.
5. Using the right-mouse drill down menus, more information on the phone and diagnostic tests are available. Let's look at these now.

Note(s):

- *Illustrated above in the Phone Search window is a Suspect Phone(s) folder. This folder contains the IP phones that:*
  - *Have not registered with a Cisco CallManager.*
  - *Have made an unsuccessful attempt to register with a Cisco CallManager.*

Experiencing Phone Outages
Gathering More Information



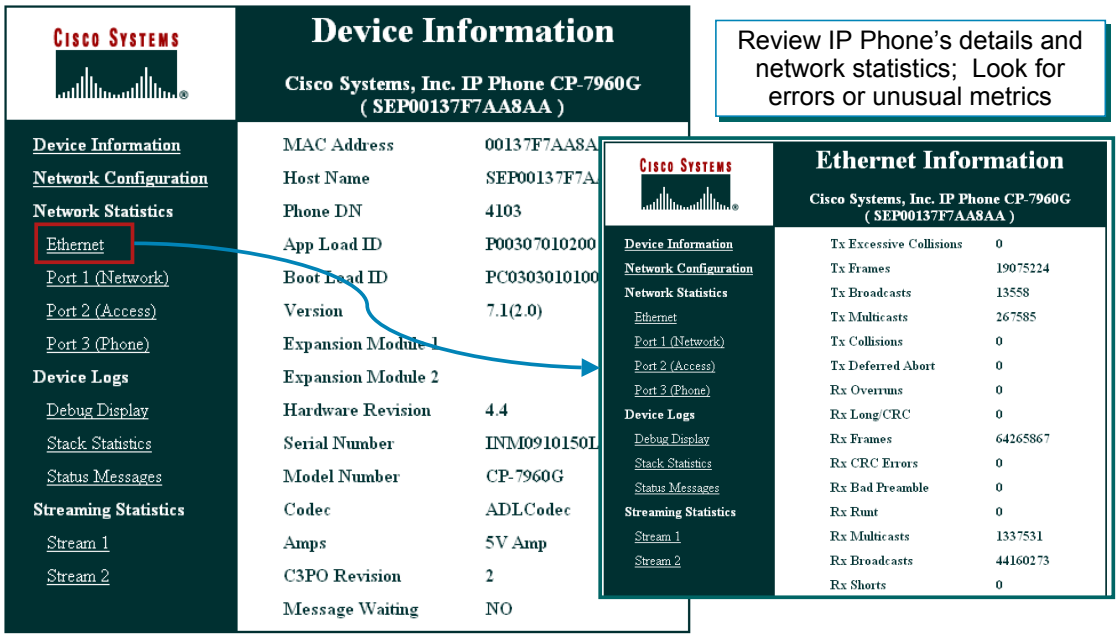
Gathering More Information

As illustrated, the Service Level View provides the Help Desk with reports and tools, making it easy for them to track and resolve IP phone problems. As illustrated above, diagnostic tests and reports can be quickly generated by right-mouse clicking on the IP phone in the Service Level View.

Above the Help Desk operator selects **Phone Details** from the drill down menu. An IP Phone report for just the selected IP phone is generated. The IP Phone report, illustrated above, provides:

- Access to the IP Phone's web interface by selecting either the phone's extension, IP address, or MAC address from the report.
- Information on the type of phone, protocol, and associated VLAN
- Information on the connecting switch
- Information on the registered Cisco CallManager
- Launch point for diagnostic tools

Experiencing Phone Outages
Access IP Phone Web Interface



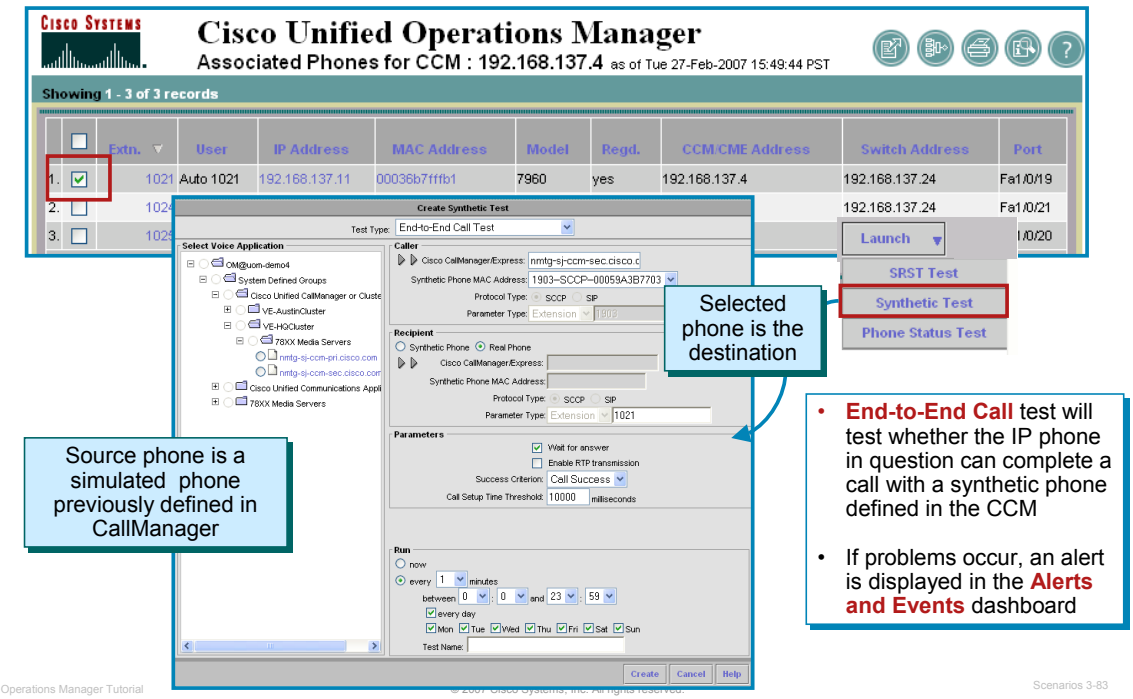
Access IP Phone Web Interface

When the Help Desk operator clicks on one of the following hyperlinks, it opens the IP phone web interface:

- Extension number
- IP address
- MAC address

Another window opens with information directly from the phone, including network configuration details, device, port, and Ethernet information for the specified IP phone. The Help Desk operator will review the information seen here including the logs and look for anything suspicious, such as: CRC errors, excessive collisions, and packet errors.

Experiencing Phone Outages
Schedule Diagnostic End-to-End Call Test



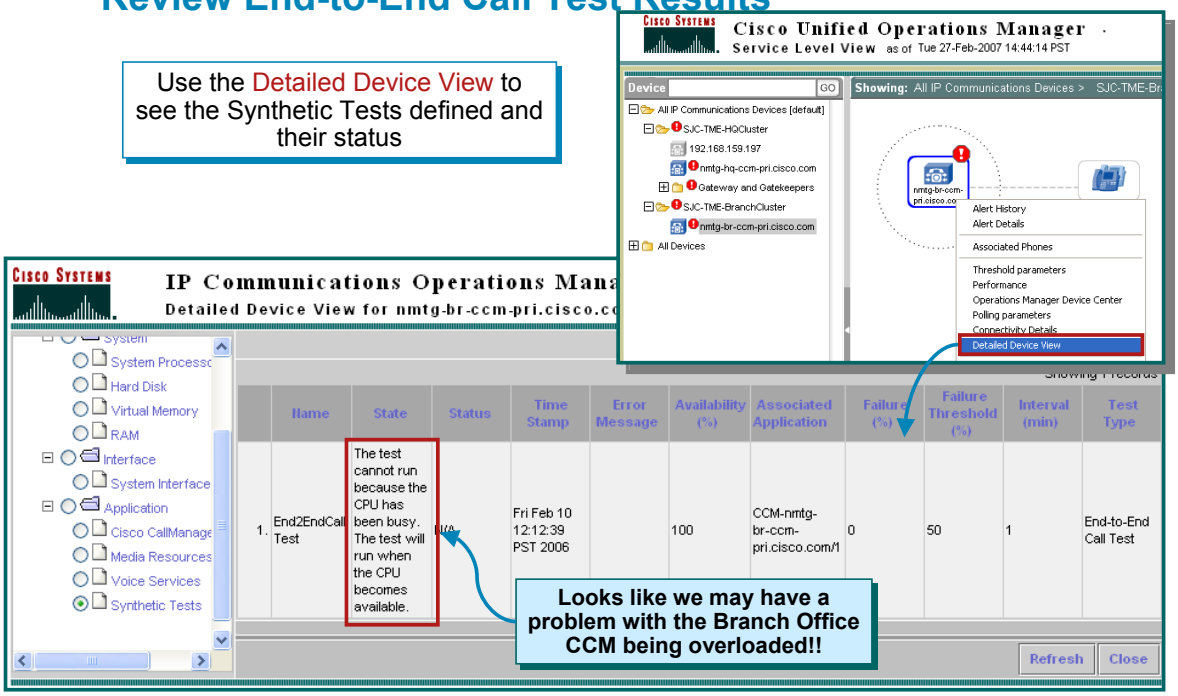
Schedule Diagnostic End-to-End Call Test

Remember that synthetic tests are used to measure the *availability* of voice applications. Synthetic tests verify whether the voice application can service requests from a user. In this scenario, the Help Desk operator will create a synthetic test to verify that the IP phone in question can register with its CCM and complete a call. The operator will run the test continuously to help detect the problem.

Follow these steps to define the synthetic test:

1. From the IP Phone Report, select the **checkbox** for the phone in question.
2. From the Launch button, select **Synthetic Test**.
3. The test type should be **End-to-End Call Test**. The Receipt fields will automatically be populated with the IP Phone selected in the IP Phone Report.
4. The Source Phone (Caller) will be a synthetic phone defined in a CCM. Use the same CCM or choose a different one from the device selection tree hierarchy. In this test, Susan chose the Branch Office CCM by selecting the CCM in the device selector and then clicking on the *triangles* next to the Caller >> Cisco CallManager / Express field.
5. The Caller MAC Address needs to be populated with a defined MAC address for a synthetic phone in the CCM. Remember, the MAC address for simulated phones must be between 00059a3b7700 and 00059a3b8aff.
6. Define the execution schedule and click **Create** when finished. A dialog message will display indicating if the test was created successfully.

Experiencing Phone Outages
Review End-to-End Call Test Results



Review End-to-End Call Test Results

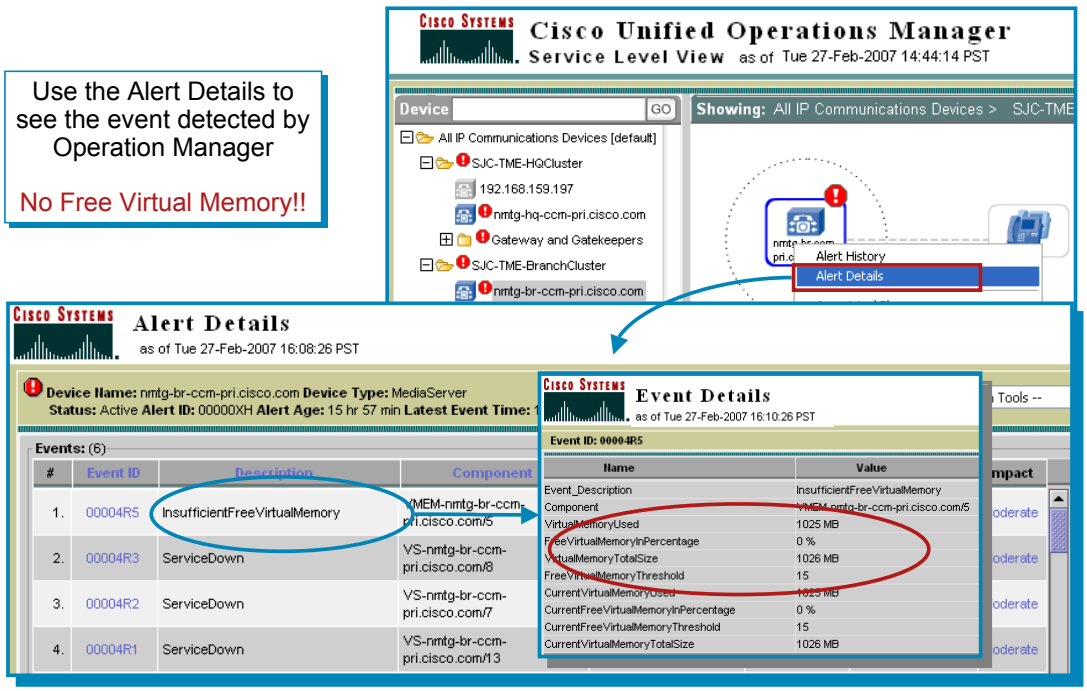
The synthetic test uses a synthetic phone configured in CCM to measure the availability of voice applications by emulating the employee's actions. For example, a synthetic test places a call between clusters and then checks to see if the call is successful.

If the synthetic test fails, Operations Manager generates a critical event. Such events are displayed in the Alerts and Events display.

To see the status of the test defined in the CCM, follow these steps:

1. From the Service Level View, locate and select the CCM for where the synthetic test has been configured.
2. Right-mouse click on the CCM; select **Detailed Device View**.
3. From the Detailed Device View, use the hierarchy to locate and select the radio button for **Application>Synthetic Tests**.
4. Information regarding the End-to-End Call test is displayed. This information is very important, because *although the test has not failed, it could not be run because the CPU has been busy*. If the test can not run, then how can the CCM properly handle voice services. Let's look for alerts on the CCM and try to isolate this problem.

Experiencing Phone Outages
CCM Alert Details



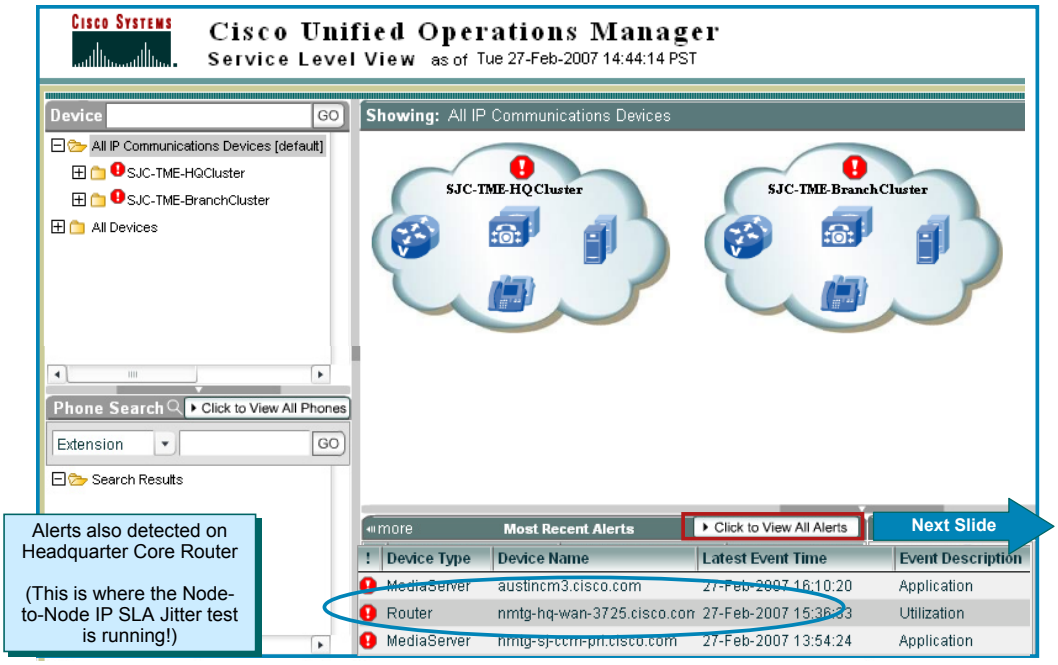
CCM Alert Details

The Service Level View can also be used to view alerts and associated events on the Unified Communications devices. To view alerts for the CCM, follow these steps:

1. From the Service Level View, locate and select the CCM for where the synthetic test has been configured.
2. Notice that there is a critical alert icon on the CCM. Right-mouse click on the CCM; select **Alert Details**.
3. The Alert Details report lists the one or more events detected on the CCM. The Service Down events were reviewed in a Scenario earlier and determined that these services did not need to be running. However, the ***Insufficient Virtual Memory*** event is critical and will cause increased page faults and thrashing and lead to lower performance.

   In this case, the event has caused the synthetic test to not run and will most likely cause services provided by the Branch Office CCM to fail as well.

Experiencing Phone Outages
More Alerts and Events



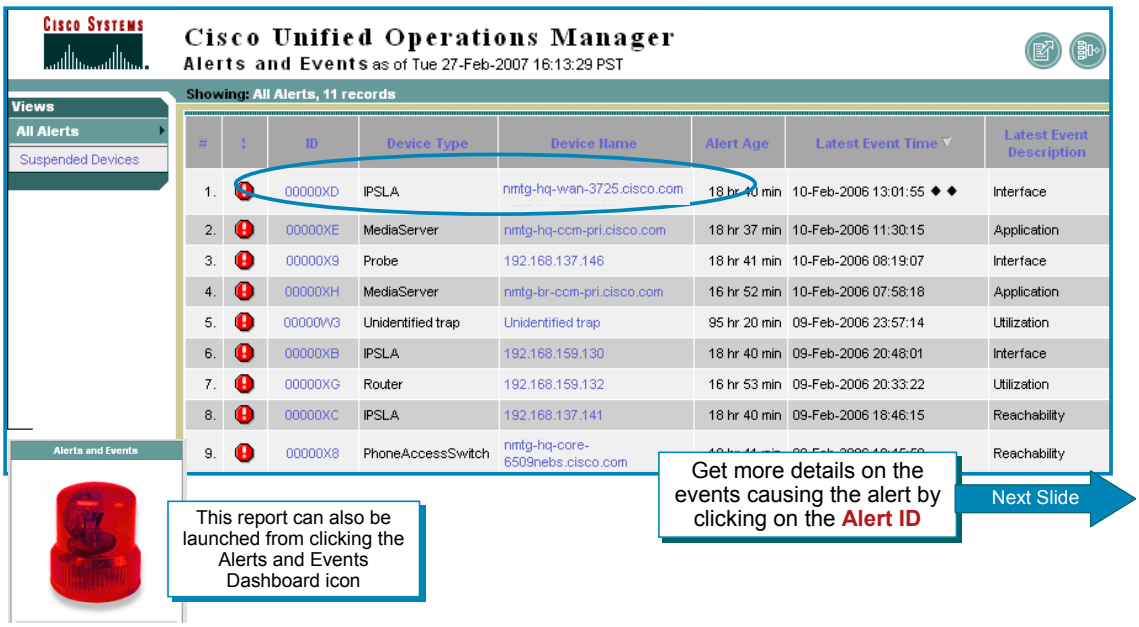
More Alerts and Events

So far from the reports seen, we have noticed one probable cause – the Branch Office CallManager lacks available virtual memory.

But look! From the Service Level View we can see that there's also alerts coming from the core router at the Headquarters. And since the user is located at the headquarters site, there may also be problems within connections between the company's headquarters and the branch office.

Let's drill down into this event for more information. Select "**Click to View All Alerts**" from the Service Level View.

Experiencing Phone Outages
More Alerts and Events, continue …



More Alerts and Events, continue …

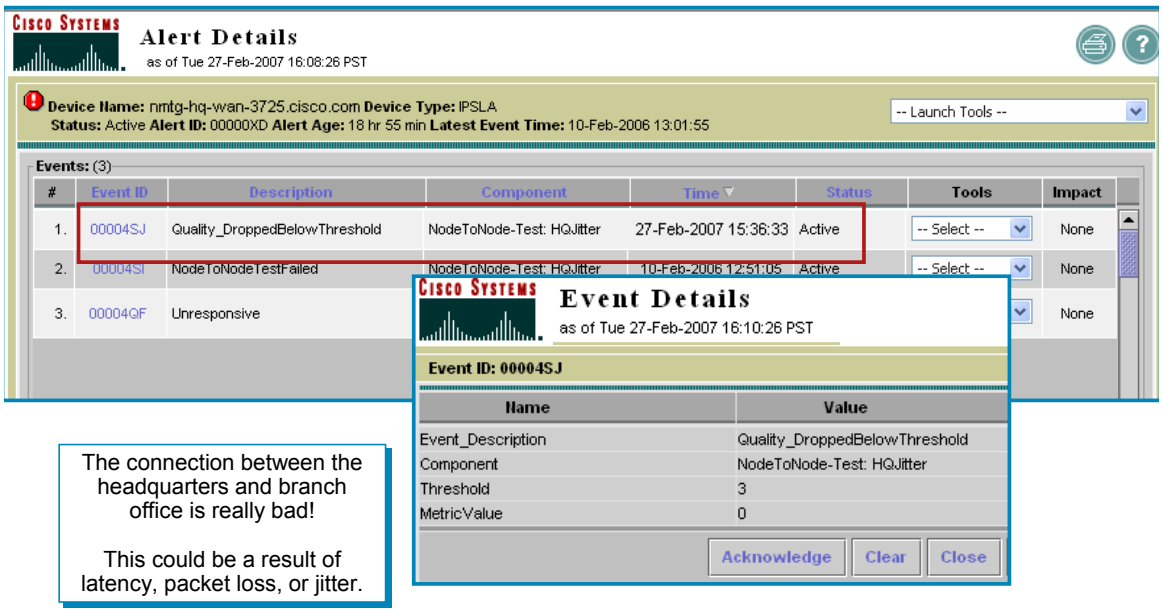
The Alerts and Events View is displayed. This view is also available by clicking on the **Alerts and Events Dashboard** icon from the Operations Manager home page.

Sure enough! There's an alert from the IP SLA feature on the router.

Remember Susan's proactive planning? She's on top of the game! In the previous scenario, she took the proactive steps to utilize the IP SLA feature in the IOS devices to setup a Node-to-Node test in Operations Manager (test type Data Jitter). The test is continuously simulating voice traffic from the headquarters to a remote site and measuring the response time of the traffic. Susan developed this test because she knew site-to-site communications is being deployed across the IP network and continuously monitoring of its quality is crucial to business operations.

Let's look at the alert by clicking on the alert ID.

Experiencing Phone Outages
More Alerts and Events, continue …



The connection between the headquarters and branch office is really bad!

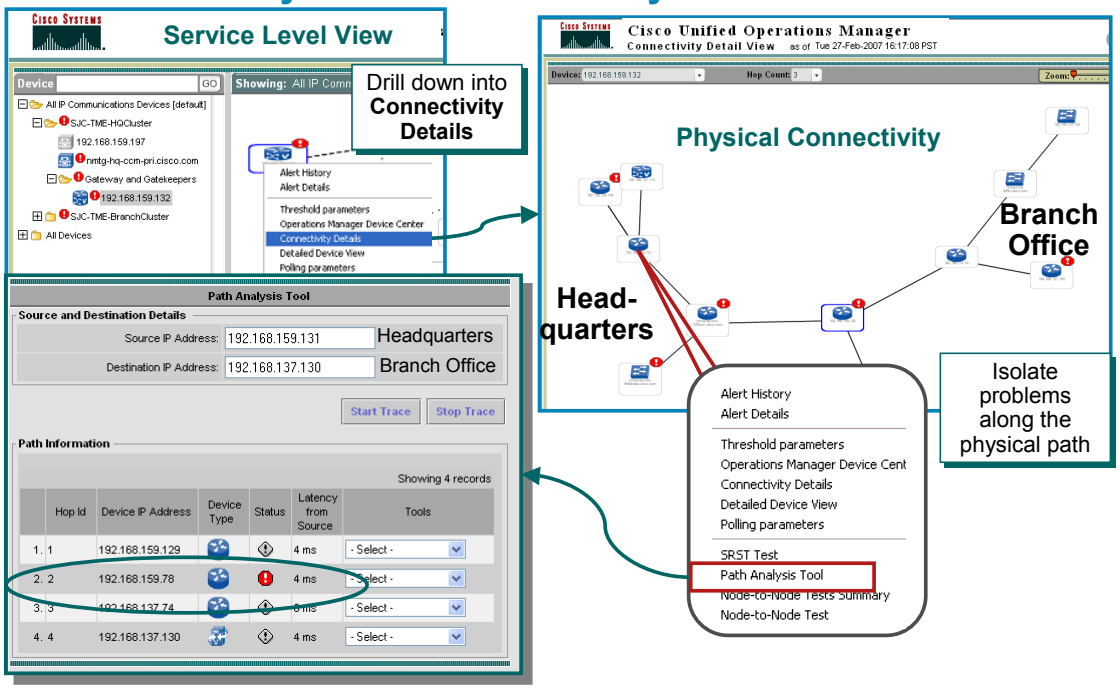
This could be a result of latency, packet loss, or jitter.

More Alerts and Events, continue …

Drilling down into the alert, Susan can see the quality of the test calls is horrible! The operator can now begin troubleshooting with a number of tools within Operations Manager. Let's start with these:

- Physical connectivity details between the test points
- Path Analysis

Experiencing Phone Outages
Connectivity Details / Path Analysis



Connectivity Details / Path Analysis

As seen in most of these tasks, the Service Level View provides an intuitive approach to obtaining more information and launching other tools.

The physical connections to a device and its connections several hops away can be displayed using the **Connectivity Details** drill down. Simply right-mouse click on a device and select it from the pop-up menu.

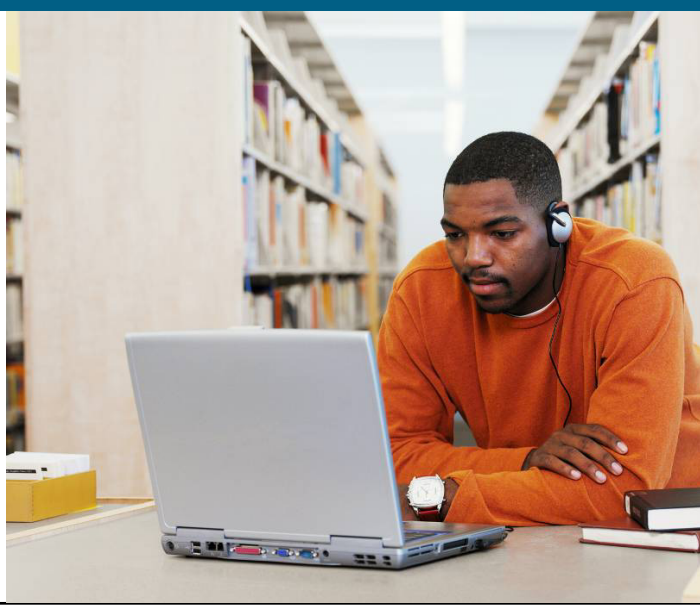
From here, Susan could launch a **Path Analysis** from the headquarters to the branch office. The Path Analysis tool provides hop-by-hop latency information for all the Layer 3 devices. It uses the ping path echo operation of IP SLA; thus, only devices that are IP SLA capable will display this menu item.

Susan can select an IP SLA-enabled source and/or a destination device from either the view pane or the map display pane and launch the tool. This will help Susan isolate the problem!

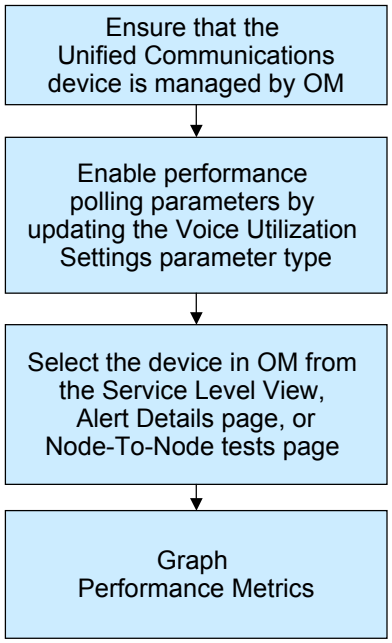
<Intentionally Left Blank>

Performance Monitoring

- Getting Started
- Preparing OM for Initial Use
- Normal Operational Status
- Service Availability Testing
- Node-to-Node (IP SLA) Testing
- Experiencing Phone Outages
- **Performance Monitoring**



Scenario 9: Performance Monitoring
Outline

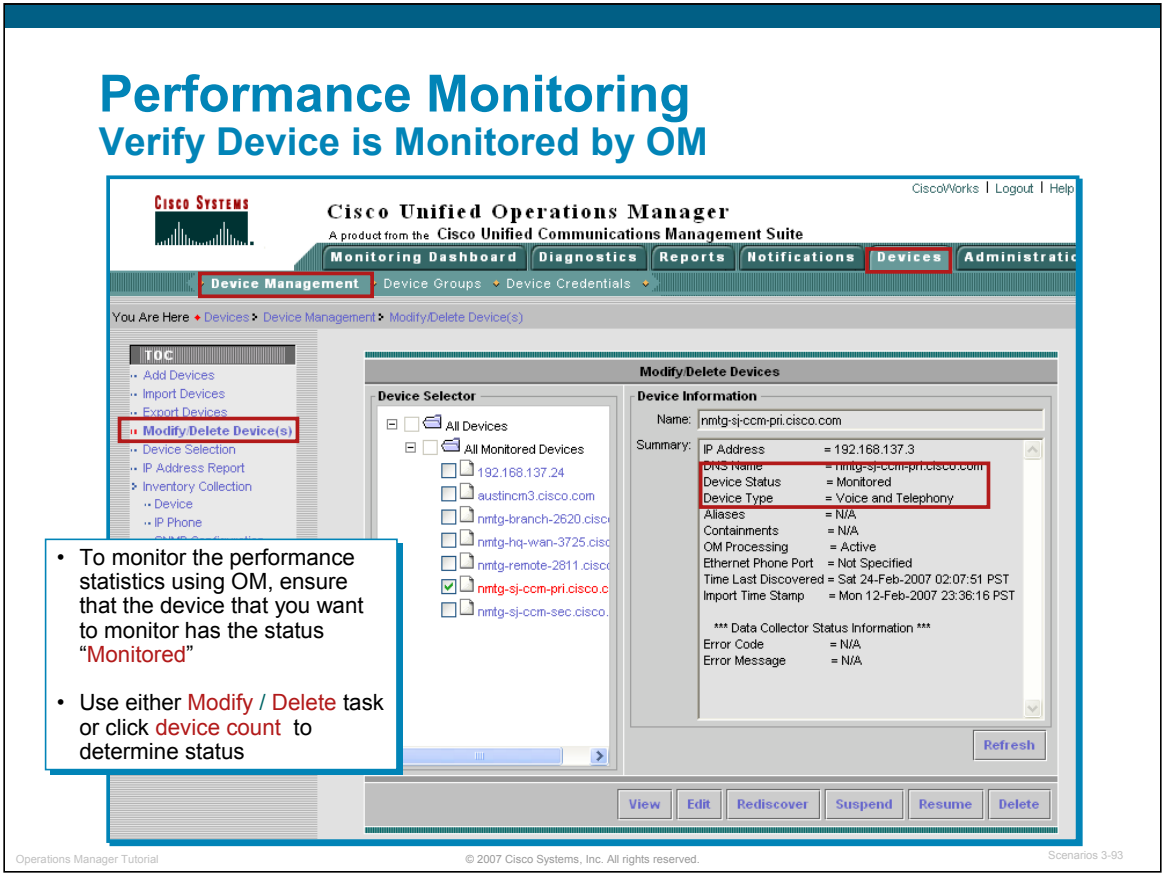


Performance Monitoring

In the first three scenarios, the user prepared the devices to be managed and configured Operations Manager. The system at that point was managing the Unified Communications devices and ready for day-to-day network management operations (reports and alert monitoring).

Since Operations Manager is continuously polling the managed devices in the OM inventory for various statistics and comparing them to defined thresholds, Susan Jones, the lead network engineer at Company ABC, is interested in reporting / graphing the metrics polled to evaluate the performance of the device or its interfaces for port or CPU utilization.

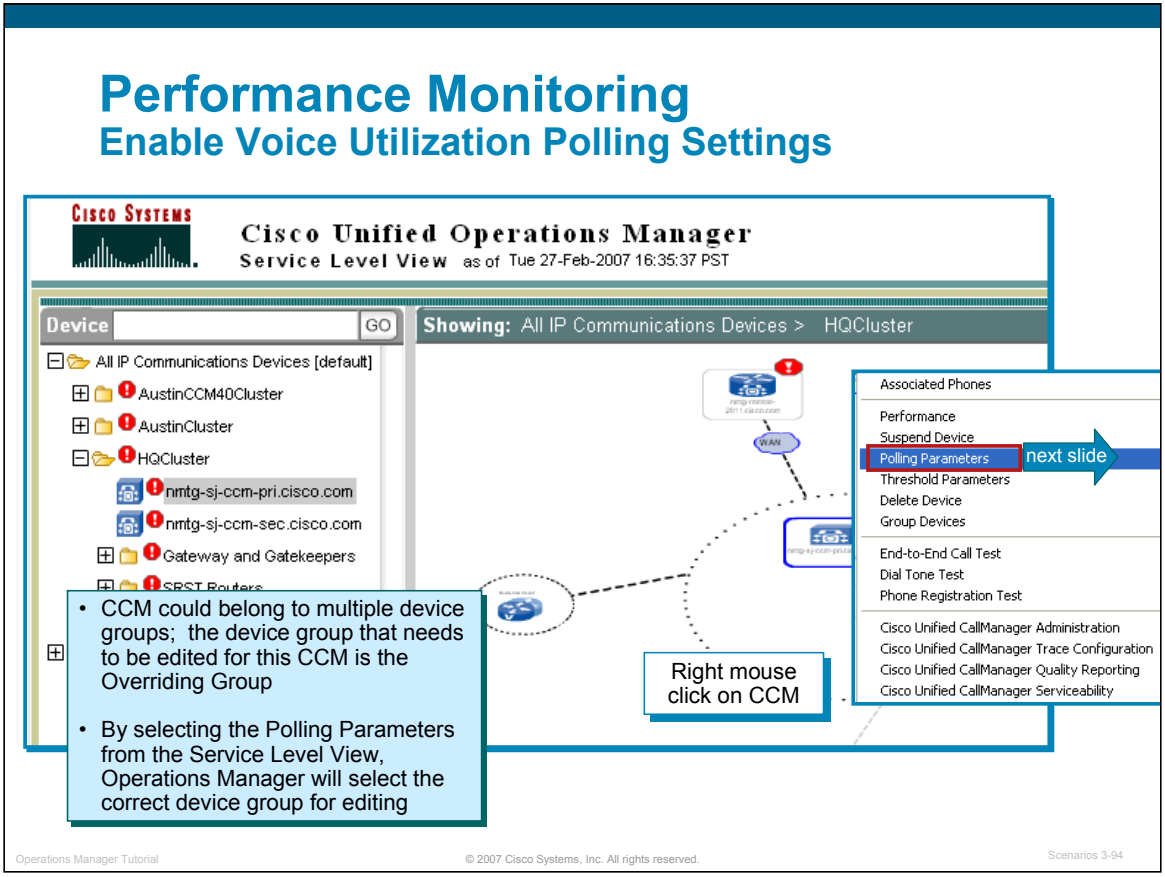
Operations Manager allows the network administrator to select and examine changes in network performance metrics. Susan can select, display, and chart network performance data in real time. The performance graphs are accessed through the Service Level View, Alert Details page, and Node-To-Node Tests page.



Verify Device is Monitored by OM

In order for Susan to use OM for Performance Monitoring, the device must be managed by OM; which means that it must be in the Operations Manager's inventory by importing it from the DCR. Susan can verify that it has been imported by using the **Modify/Delete Devices** page and by following these steps below:

1. From the OM home page, select **Devices > Device Management**.
2. As seen previously, the user could click on the device count for the devices in the Monitored status. Or, the user could click on the task, **Modify/Delete Devices**. The Modify/Delete Devices page opens, as illustrated above.
3. Susan wants to monitor the CCMs located at both the company's headquarters and branch office. In the device selector, she locates the device(s) that she is interested in.
4. Susan clicks on the device. The device information appears in the right pane, as illustrated above. Verify that Device Status is **Monitored**. A Monitored state on the device indicates that it was imported successfully and being managed by OM.
5. If the device is not in the Monitored state, refer to the on-line Help "Troubleshooting Device Import and Inventory Collection". Only the devices in the All Partially Monitored Devices group and the All Unreachable Devices group were not imported fully into Operations Manager.
6. Click **View** to get more information on the device, such as when the last Inventory Collection occurred.



Enable Voice Utilization Polling Settings

Operations Manager uses the statistics gathered during Voice Utilization polling for charting network performance. The Voice Utilization settings control polling for performance and capacity data and is disabled by default. To collect the utilization statistics desired, *enable the Voice Utilization polling settings* for the device group that the device belongs to.

If Susan knows which Device Group that the CCM belongs to, she could enable the utilization polling settings by following this step:

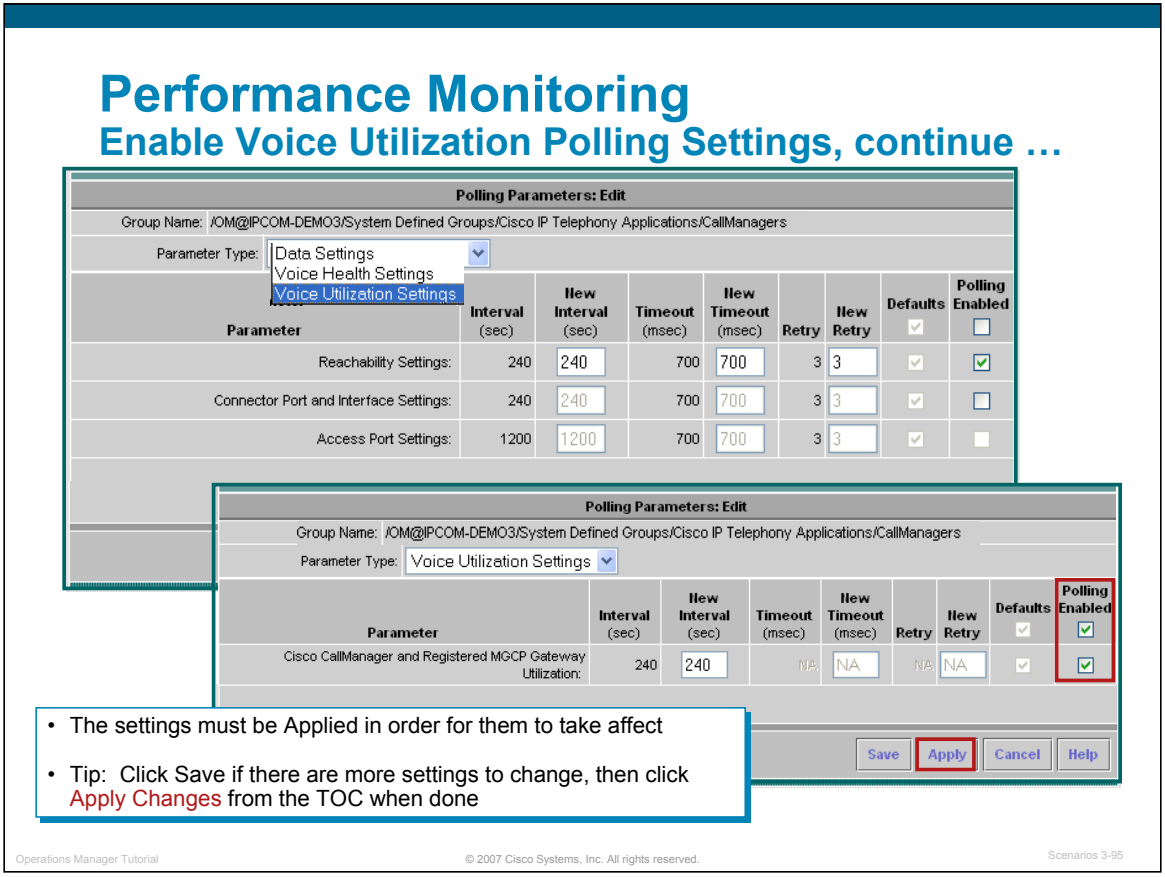
1. Select **Administration > Polling and Thresholds**. Select **Polling Parameters** from the TOC.

But too use this method, you now need to select the appropriate device group for the CCM. *Remember, the device may belong to more than one device group because of its capabilities* and you need to select the "overriding"device group.

Susan is not sure of the "overriding" device group for the CCM. Therefore, Susan uses an easier way! The following steps (illustrated above) make sure that the correct device group is being edited to enable Voice Utilization polling:

1. From the Service Level View, right-mouse click on the device. Select **Polling Parameters**.
2. The Polling Parameters:Edit dialog is displayed and the correct device group System Defined Group called "*Cisco IP Telephony Applications> CallManagers*" is selected.

   (If Susan had to guess, she would have guessed wrong and selected the "78xx Media Servers", which is the device group for the CCM, but not the overriding device group.)



Enable Voice Utilization Polling Settings, continue …

Susan will edit the utilization polling settings by continuing with these steps:

1. Using the Edit:Polling Parameters dialog, change the Parameter Type to **Voice Utilization Settings**, as illustrated above.

   Note: This changes the settings for the entire device group, not just the device of interest.
2. Enable polling by checking the checkbox, **Polling Enabled**
3. Click Save if making more changes to the settings; otherwise, click **Apply** to save the settings, close the Polling Parameters: Edit dialog box, and apply changes to the system. When a confirmation dialog box appears, click **Yes**.

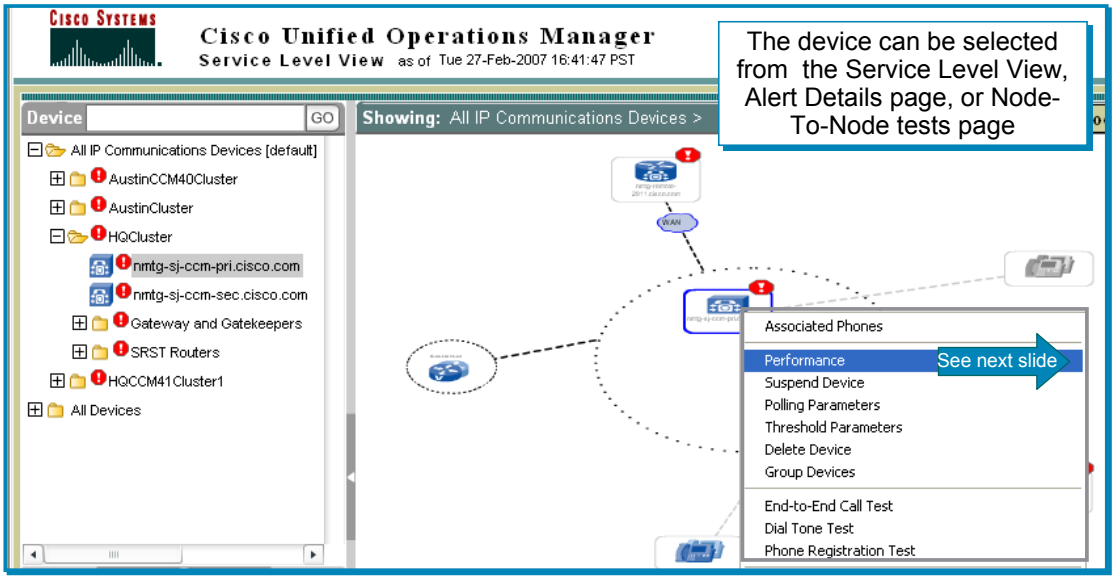
Review the other settings as well.

- *Data Settings--Control polling for devices and those ports and interfaces that are not voice-enabled.*
- *Voice Health Settings--Control polling for voice-enabled devices, ports, and interfaces.*
- *Voice Utilization Settings--Control polling for performance and capacity data; disabled by default.*

Additional *Note(s):*

- *When you click Apply, Operations Manager performs the following tasks:*
  - *Recalculates group membership, based on group priority.*
  - *Uses the new polling and threshold settings to gather information from the devices.*
- *You must also apply changes after resuming a device, so that Operations Manager will begin polling the device depending on the appropriate settings.*
- *You can apply changes by selecting **Administration > Polling and Thresholds > Apply Changes** in the TOC menu.*
- *When you click Save, Operations Manager sets the polling and threshold settings in the selected group. Click Save if you plan to make more changes shortly, it would be more efficient since applying changes is a CPU-intensive event that might take between one and ten minutes to complete.*

Performance Monitoring
Graph Performance Statistics

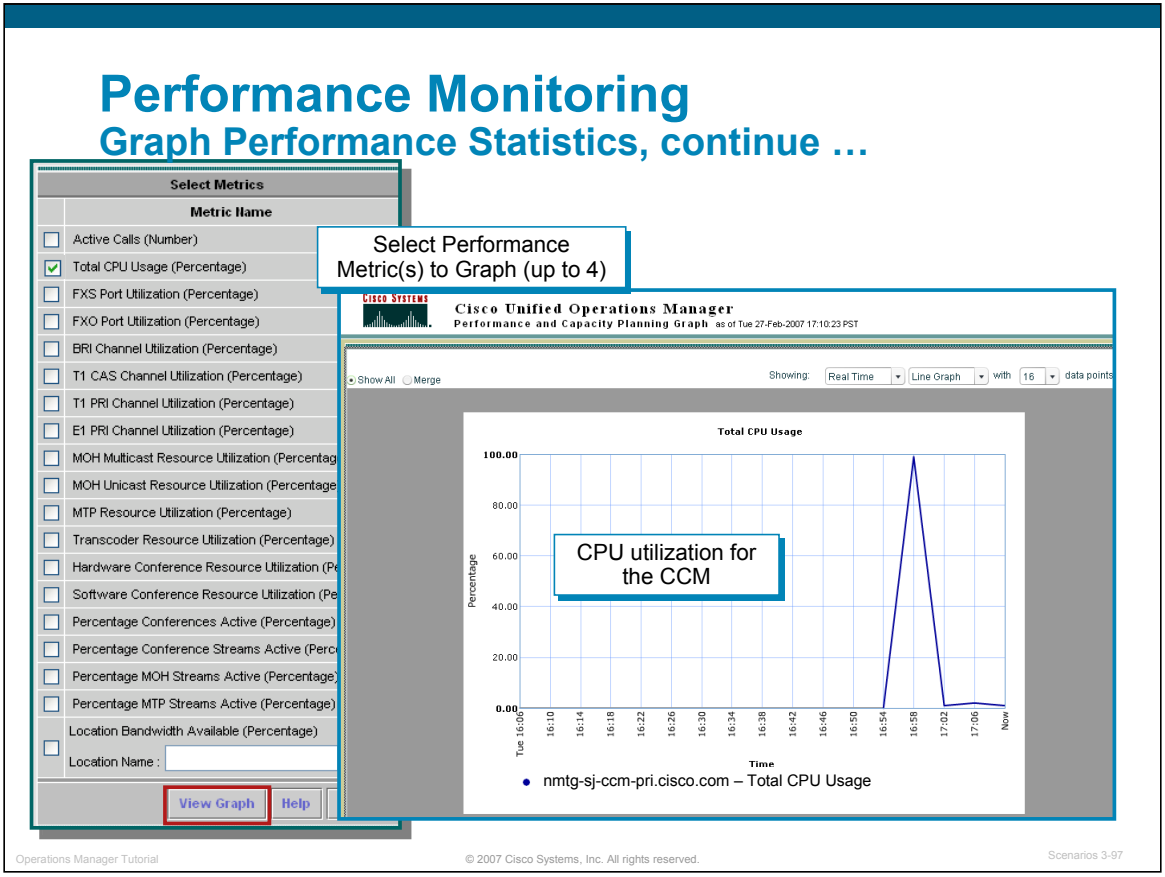


Operations Manager Tutorial © 2007 Cisco Systems, Inc. All rights reserved. Scenarios 3-96

Graph Performance Statistics

When graphing performance metrics for a device, follow these steps:

1. As illustrated above, select the device for which you want to graph performance metrics. In this case, Susan right-mouse clicked on the CCM of interest. You can select, display, and chart network performance data in real time. The performance graphs are accessed through the Service Level View, Alert Details page, and Node-To-Node Tests page.
2. Select **Performance**. A metrics dialog box appears, as illustrated on the next page.



Graph Performance Statistics, continue …

From the list of metrics to graph, follow these steps:

1. Select the desired metric(s), and click **View Graph.** If selecting multiple metrics (up to four), they must be of the same units.
2. Review the graph results. It displays the performance metrics as a graph or in tabular format. To choose either a graph or tabular display, choose the desired tab located at the top right of the page, under the window tools area. The information in a graph can be viewed as a snapshot in time or it can be refreshed at regular intervals by selecting a time interval or *Real Time* from the Time Interval pull-down menu located above the graph.

The types of utilization statistics collected and saved vary per device type. The OM on-line help on Performance Graphing helps you to understand the types of statistics that are available. For example, on a CCM, Susan can graph the following statistics:

- CPU Utilization
- Active Calls
- Port Utilization
- Various CCM Resource Utilization: MOH multicast and Unicast, MTP resource, Transcoder, hardware conference, software conference, percentage conference active, percentage conference streams active, and location bandwidth available

The data files for the performance metrics are located on the server, in the <OM installed directory>\data\gsu_#GSUdata#_ directory. You will need access to the server directory, where Operations Manager is installed to access these files. The filenames are created using the device name and the date. These files are kept for 72 hours, after which they are purged.

Thank You!

Continue on to Chapter 4 to learn about some of the system administrative tasks not yet discussed.

Cisco Systems

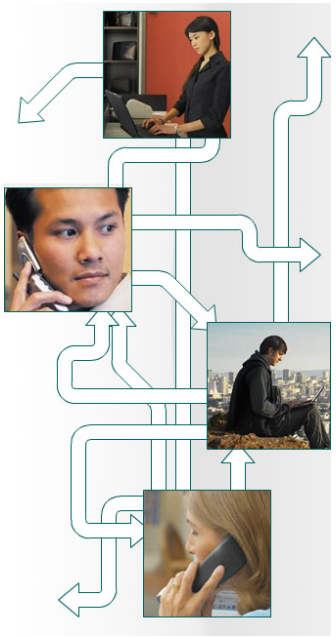
Cisco Unified Operations Manager

System Administration

Chapter 4

Chapter 4 Outline

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



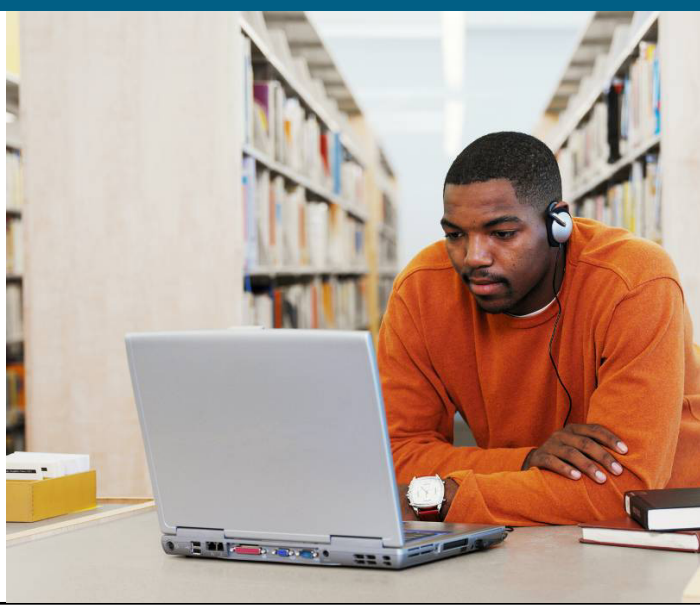
Chapter 4 Outline

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

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

Requirements

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



Requirements
OM Server Sizing

System Parameter	Capacity per Deployment Size		
	Small–Medium	Medium–Large	Large–Very Large
Monitored Phones	5,000	10,000	30,000
Monitored Voice Devices	300	1,000	2,000
Monitored CCM Clusters	10	15	30
Monitored CME Routers	100	250	500
Monitored SSRT Routers	10	100	500
Concurrent Synthetic Tests	25	100	250
Concurrent Node-to-Node (IP-SLA/SAA) Tests	25	100	250
Phone Reachability Tests	50	500	1000
Concurrent Client (Browser) Logins	5	5	5

Operations Manager Server Sizing

The actual requirements for a server depends on the number of objects to be managed by Operations Manager and the number of synthetic tests to be configured. This chart provides guidelines for small to medium, medium to large, and large to very large deployments. The size of the deployment will determine the requirement for the server as detailed on the next page.

Requirements
Standalone OM Server

Parameter	Deployment Size		
	Small–Medium	Medium–Large	Large–Very Large
Processor	• Intel Pentium or Xeon processor > 2Ghz • AMD Opteron processor >2 Ghz	• Dual Intel Pentium or Xeon processor > 3Ghz • Dual AMD Opteron processor >3 Ghz	• Dual Intel Pentium or Xeon processor > 3Ghz • Dual AMD Opteron processor >3 Ghz
Memory	2 GB	4 GB	4 GB
Swap	4 GB	8 GB	8 GB
Disk Space (NTFS Format)	72 GB	72 GB	72 GB
Operating System	Windows 2003 Server SPK1	Windows 2003 Server SPK1	Windows 2003 Server SPK1

- Additional applications (i.e. Service Monitor) requires additional server resources (upcoming slide)
- Windows Terminal Services is supported in remote administration mode only
- 16 MB of space required in temp directory

Standalone OM Server Requirements

The chart above details the sizing requirements for the Operations Manager server depending on the size of the deployment. The only real difference being in the CPU horse power and the amount of memory.

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

Requirements
Co-resident OM-SM Server

Parameter	Deployment Size	
	Up to 1,000 IP Phones	Up to 5,000 IP Phones
Processor	• Intel Pentium or Xeon processor > 2Ghz • AMD Opteron processor >2 Ghz	• Dual Intel Pentium or Xeon processor > 3Ghz • Dual AMD Opteron processor >3 Ghz
Memory	4 GB	4 GB
Swap	8 GB	8 GB
Disk Space (NTFS Format)	72 GB	72 GB
Operating System	Windows 2003 Server SPK1	Windows 2003 Server SPK1

- More than 5,000 IP Phones requires standalone servers for OM and SM
- Windows Terminal Services is supported in remote administration mode only
- 16 MB of space required in temp directory

Co-Resident OM-SM Server

In some situations, you may want to install Operations Manager and Service Monitor (OM-SM) on the same server. For deployments of less than 5,000 IP phones, Operations Manager and Service Monitor can reside on the same platform.

The chart above details the sizing requirements for the Operations Manager/Service Monitor server depending on the size of the deployment. The only real difference in requirements is in the recommended CPU and the amount of memory (RAM).

Note(s):

- It is always a good idea to check the latest release notes for up-to-date information regarding system requirements.
- Windows Terminal Services is supported in remote administration mode only
- 16 MB of space required in temp directory

Requirements
Client Platform

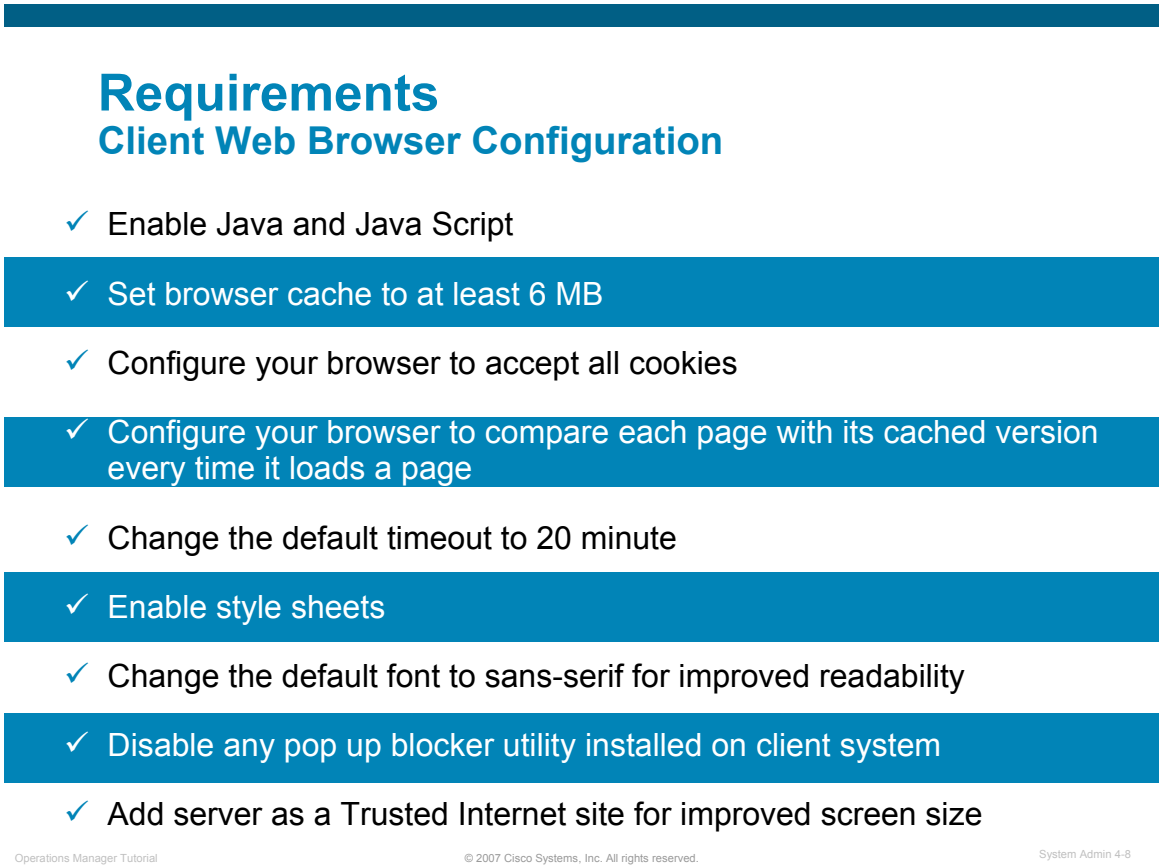
Client Requirements (minimum)	
Processor	Pentium IV > 1Ghz
Memory	1 GB
Swap	2 GB
Operating System	• Windows XP Home or Professional with SPK2 • Windows Server 2003, SPK1, Standard or Enterprise without terminal services
Additional Software	• Microsoft Internet Explorer 6.0.2600.0000, IE 6.0.2800.1106,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

Client Requirements

Access to an Operations Manager server is achieved using a standard web browser. Operations Manager has been tested and certified only on PC compatible systems running either Windows XP or Windows 2003, and using Microsoft Internet Explorer (6.0.28 or 6.0.37).

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

Note: 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.



Web Browser Configuration

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

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

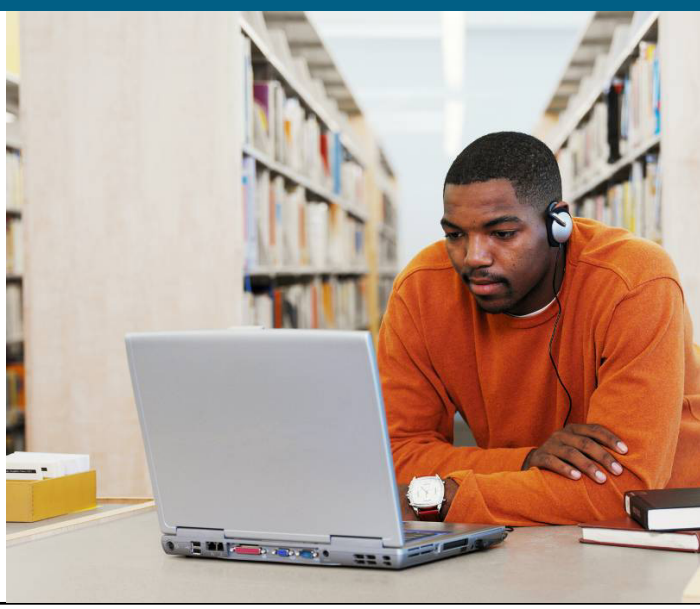
If you have browser problems after configuring your browser, increase your disk cache settings.

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

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

Installation Guidelines

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



Installation Guidelines
General

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

Installation Requirements

Installation of Operations Manager should be performed according to the steps detailed in the Installation and Setup Guide. (A link to this guide can be found in Chapter 5.)

- Operations Manager 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 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 serves in a multi-server setup.
- 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 the user is also issued a warning because when the IP address changes, the application will no longer work.
- If IIS (Microsoft's Internet Information Services) is enabled, the installation will abort due to a port conflict between Web Server 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 are available for use
- Refer to Installation and Setup Guide for Operations Manager for installation procedure
  - License file required
  - Refer to next section for more information on managing licenses

Installation Requirements

Refer to the previous section's notes for the ports used by Operations Manager and ensure they are not in use on the server.

And finally, Operations Manager requires a license file to be installed to work. The licensing mechanism is discussed next.

Operations Manager TCP and UDP Ports

Port Number / Type	Usage
162 / udp	Default port number used by Operations Manager for receiving traps
1741/tcp	Used for HTTP server
9002 / tcp	Used by the Broker to listen to both the IP telephony server and the device fault server
9009 / tcp	Default port number used by the IP telephony server for receiving traps from the device fault server
40000–41000 / tcp	Used by Common Transport Mechanism for internal application messaging
42344 / tcp	Used by Synthetic Testing web service
42350–42353 / tcp	Used by messaging software
43441–43459	Used as database ports: Operations Manager uses the following ports: • 43445--Used by Alert History database engine • 43446--Used by inventory service database engine • 43447--Used by event processing database engine • 43449--Used by IP Phone Information Facility database engine • 43459--Used by Service Monitor database engine

Installation Guidelines
CUOM v2.0 Licensing

- Installation ensures a registered and licensed copy of the product is being installed
  - Feature-based
    - Standard Edition
    - Premium Edition
  - Scale-based
    - 1000, 2000, 5000, 10000, 20000, 30000 phones
    - Up to 30,000 IP Phones per Operations Manager
- Following license information is shipped with product:
  - Product Identification Number (PIN) – indicates type of install
  - Evaluation Installation – Valid for 90 days; after message is displayed
  - Product Authorization Key (PAK) – Use to register product at Cisco.com, a license file is returned.
- Install will prompt for the location of the license file returned from the registration process; If upgrading from evaluation license, enter location of license file at Common Services > Server > Admin > Licensing

Licensing

Operations Manager requires a license to operate. If a license is not installed, Operations Manager 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 Operations Manager at Cisco.com. Operations Manager 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

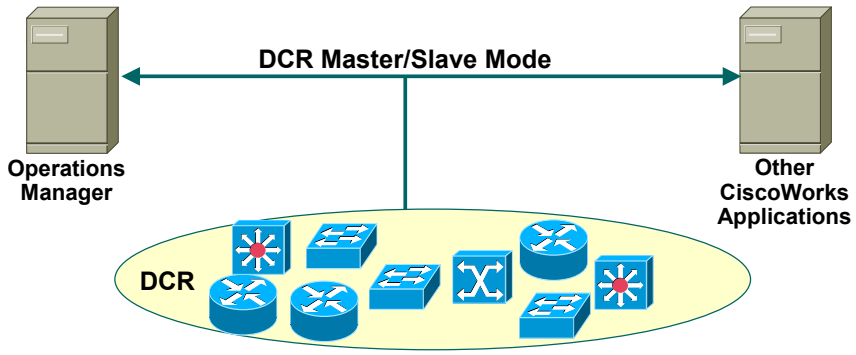
http://www.cisco.com/go/license/public (non-registered users)

use the PAK to register the product and download the license file to the server. (Users who are not registered users of Cisco.com will 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.

Installation Guidelines
Sharing Devices with other CiscoWorks Applications

Share devices between servers by creating a common DCR on both servers



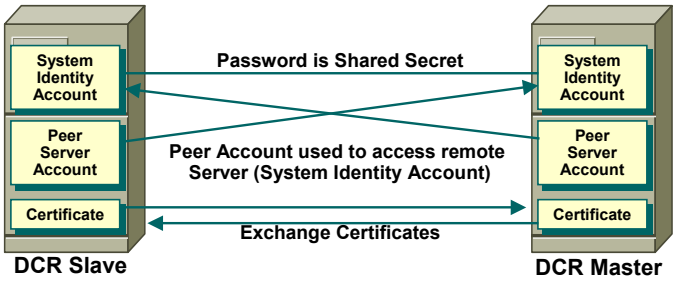
Sharing Devices with other CiscoWorks Applications

Operations Manager requires the services provided by the underlying software, Common Services. One task of Common Services is to keep the Device and Credentials Repository (DCR). Because all CiscoWorks applications use Common Services, it is possible to configure Common Services to share devices in their DCR with other server's DCRs. This effectively creates a common set of devices and credentials between all CiscoWorks servers and applications, thus minimizing device maintenance on separate platforms.

If this feature is to be used, it is suggested that administrators first configure Operations Manager device selection to be manual (From the DCR, select specific devices to be managed) to avoid over population of Operations Manager with devices with no IPC features.

Installation Guidelines
Trust Environment

Creating a common DCR requires the configuration of a trust environment



Trust Environment also enables:

- Single Sign-On (SSO) – Sign on once for access to all servers in domain
- Import remote applications to local homepage
- Sharing of group information between servers

** See Common Services Tutorial for more details*

Trust Environment

To share devices among other servers using Common Services, a Trust Environment between servers must be established. This requires the swapping of certificates and the creation of common System Identity and Peer Server Accounts. Details for creating the Trust Environment and sharing DCRs can be found in the Common Services Tutorial.

Once the Trust Environment is established, the user can realize other benefits besides the sharing of all devices via common DCRs.

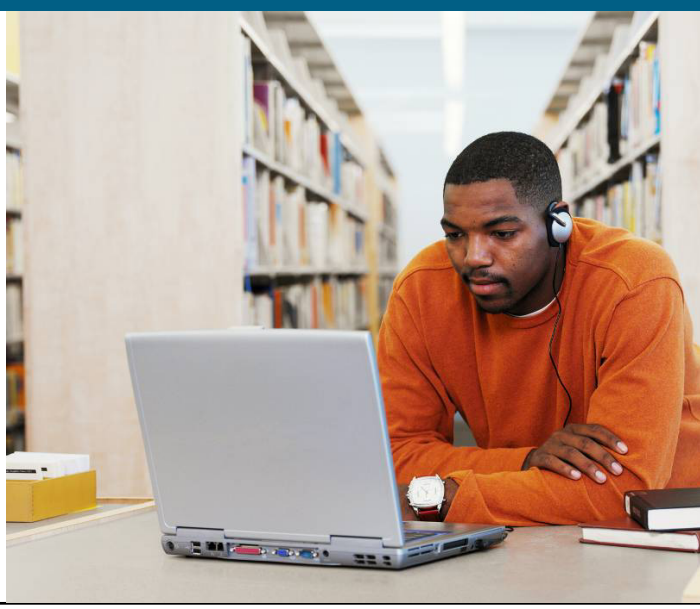
The first multi-server feature is Single-Sign-On (SSO). This allows for a user to authenticate once and then browse and use any server in the management domain without having to authenticate with every server. SSO mode requires one server to be the authentication master. Since all others servers must now securely access this server to process logins, trust must be setup between the servers.

Another multi-server feature is to have the homepage of one server registered the applications on all other servers to facilitate browsing and task execution.

<Intentionally Left Blank>

User Security Administration

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



User Security Administration
Login Modes

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

ACS adds increased security and flexibility!

Login Mode

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

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

User Security Administration
Pre-defined User Roles

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

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

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

Pre-defined User Roles

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

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

System Administrator – Can perform Operations Manager system administration tasks

Network Administrator – Can perform all Operations Manager tasks

Network Operator – Can perform all Operations Manager tasks

Approver – Not used in Operations Manager

Help Desk – View only

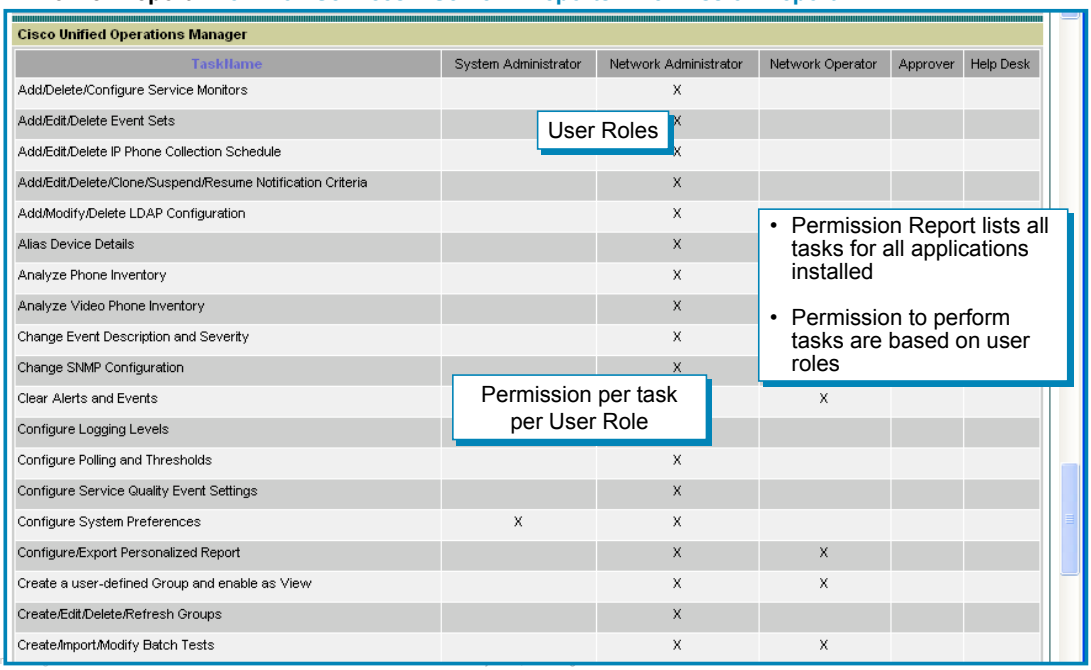
In Non-ACS mode (local server authorization) users can be assigned more than one user role, and all are assigned the basic user role – Help Desk. The roles cannot be modified. See next page for user roles assigned to Operations Manager tasks.

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

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

User Security Administration
Permission Report

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



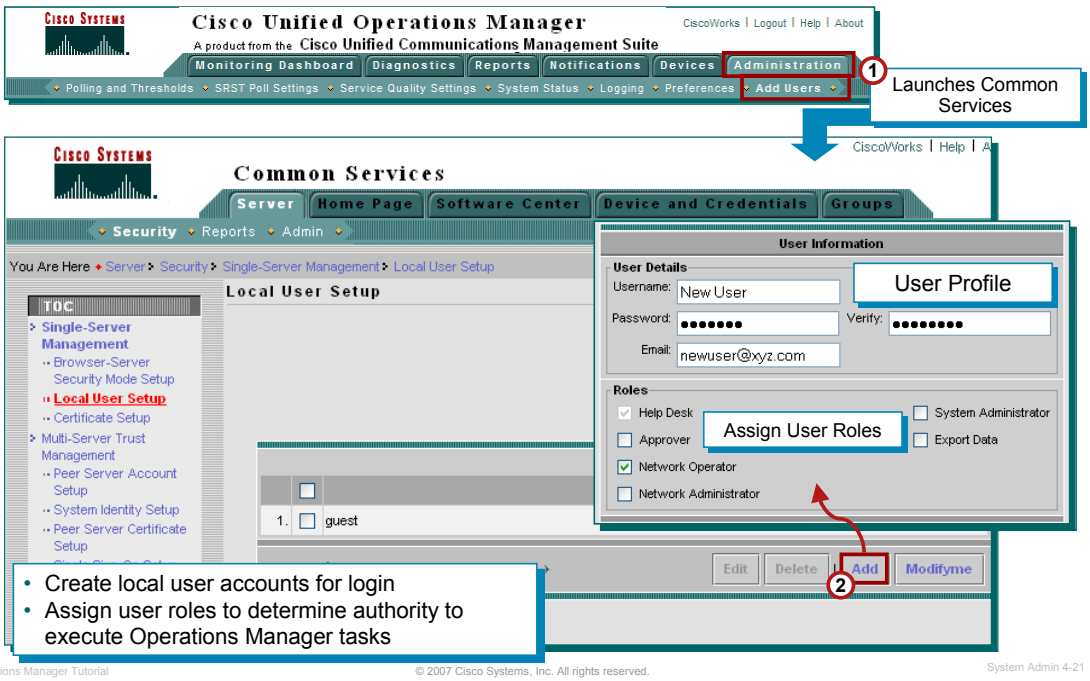
Permission Report

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

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

The above picture displays the Permission Report for Operations Manager.

User Security Administration
Creating Users (Common Services Authentication)



Creating Users (Common Services Authentication)

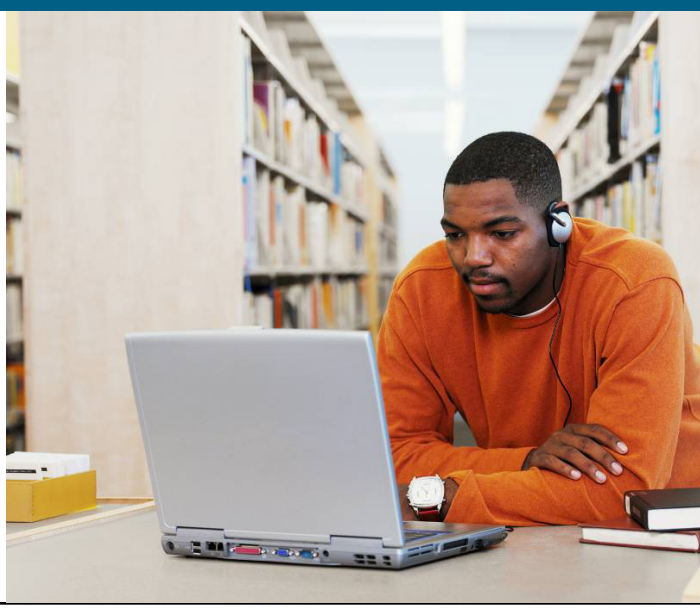
Common Services allows users with the System Administration user role to create user accounts and assign user roles to the account. Creating a new user is simple and straight forward using the ***Common Services > Server > Security > Single-Server Management > Local User Setup*** task. A dialog is displayed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

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

<*Intentionally Blank*>

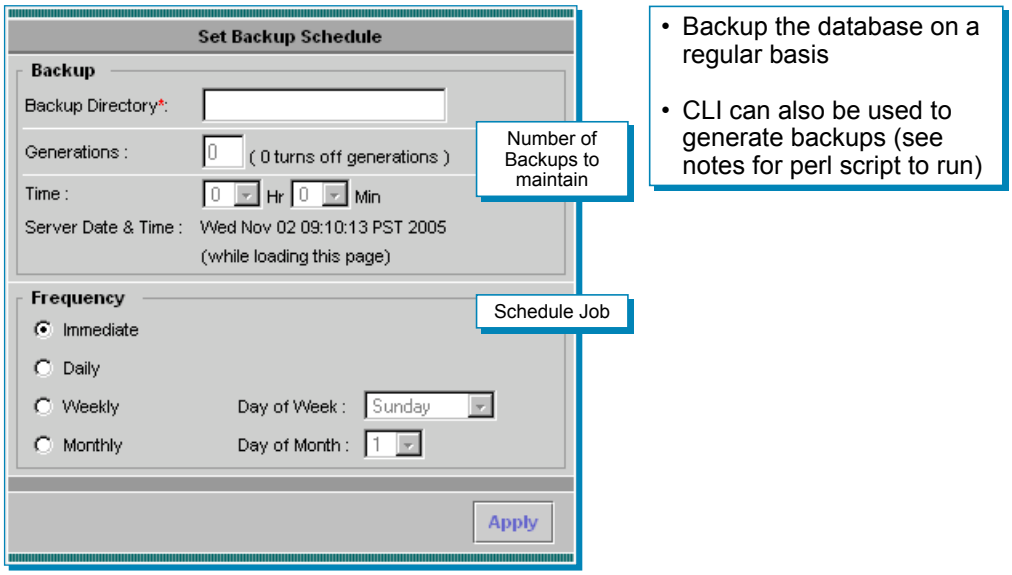
Periodic Maintenance

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



Periodic Maintenance
Database

Common Services > Server > Admin > Backup



Database Management

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

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

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

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

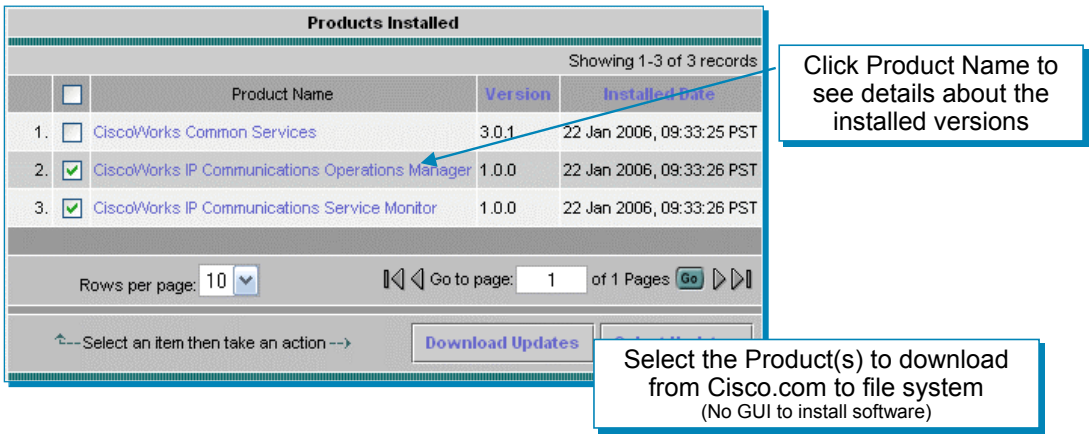
NMSROOT/log/dbbackup.log

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

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

Periodic Maintenance
Software Updates

Common Services > Software Center > Software Update



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

Software Updates

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

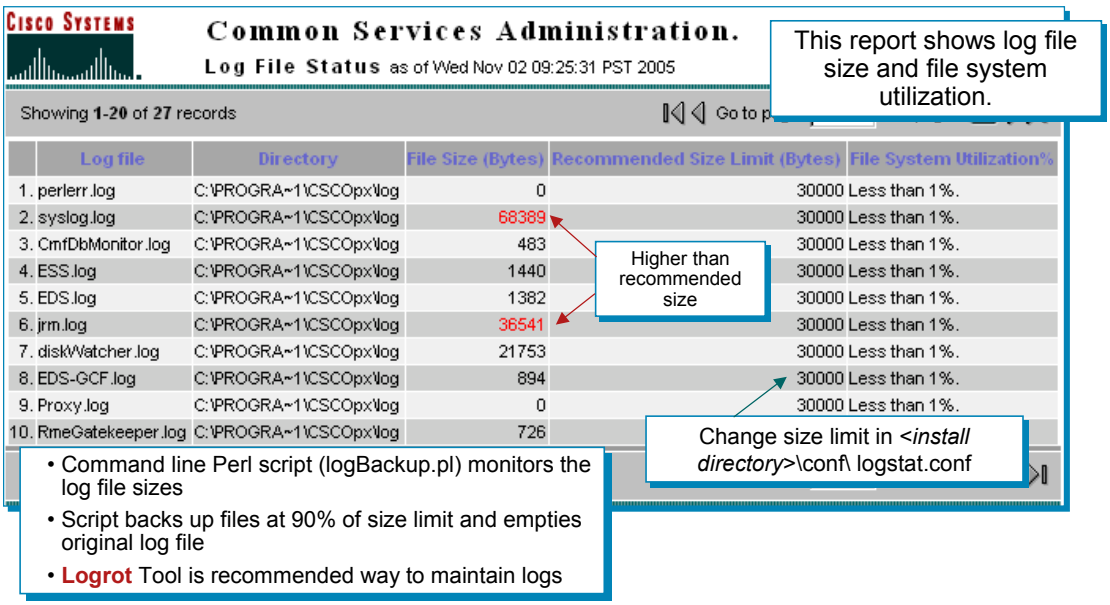
When accessing the ***Common Services > Software Center > Software Updates*** task a dialog is displayed showing the bundles and individual applications installed. Clicking on an application will give the details about the Applications and Packages installed with a *Product* page that gives the details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

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

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

Periodic Maintenance
Log Files – Common Services

Common Services > Server > Reports > Log File Status



Log File Management – Common Services

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

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

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

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

Stop all Operations Manager processes first before using the script.

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

Logrot Utility

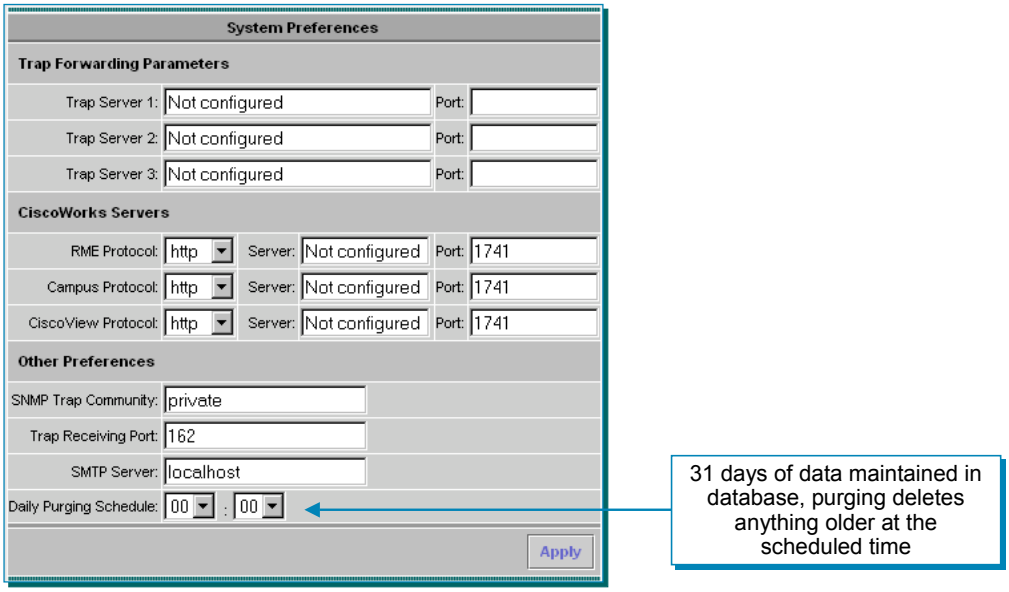
The **logrot utility** helps you manage the log files in a better fashion **and is the recommended approach**. Logrot is a log rotation program that can:

- Rotate log when Operations Manager 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
Data Purge

Operations Manager > Administration > Preferences



Preferences

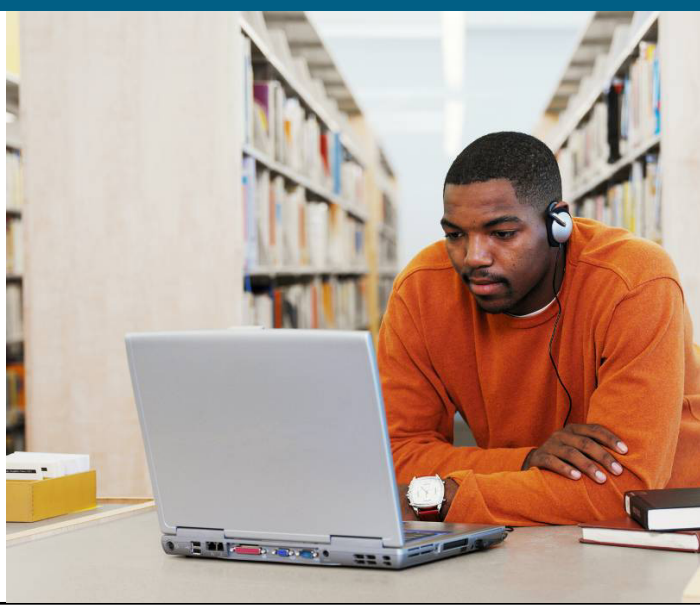
Alert and Event History Service Quality History data provides lots of useful information. However, the storing of this data must be maintained to manage the size of the database. Operations Manager is configure to keep and display 31 days of data. Once a day a purging task is executed deleting all data older than 31 days from the database. The administrator can determine when this task is executed by selecting ***Operations Manager > Administration > Preferences***. The Daily Purging Schedule can be found and set at the bottom of the dialog.

Note: Ensure that no other scheduled task interferes with this task.

<*Intentionally Blank*>

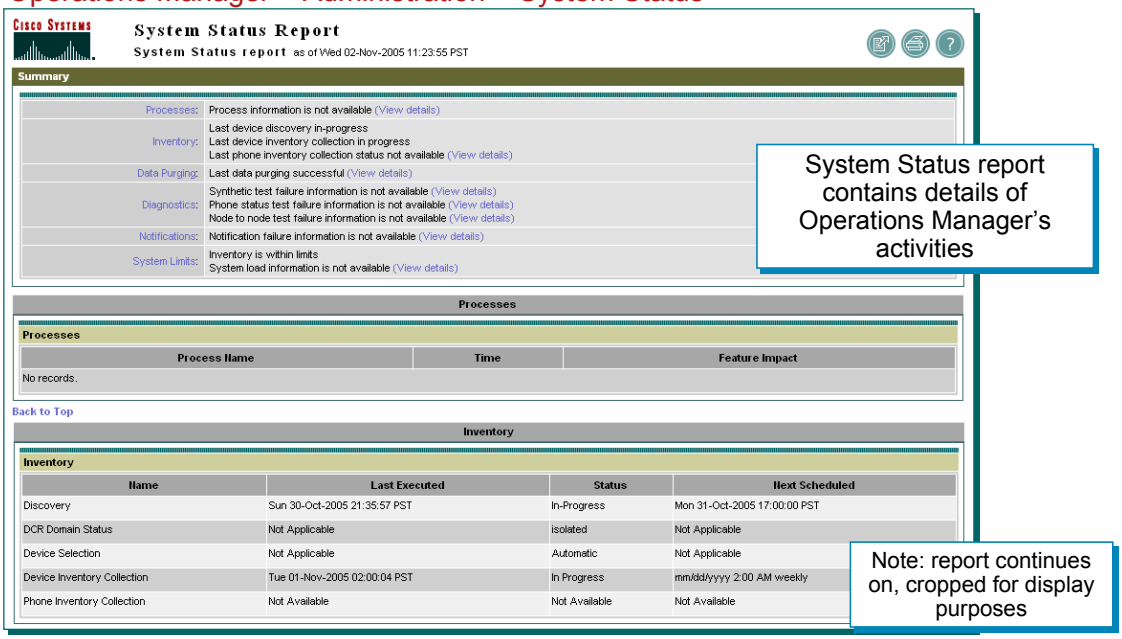
Helpful Troubleshooting Tips

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



Helpful Troubleshooting Tips
System Status

Operations Manager > Administration > System Status



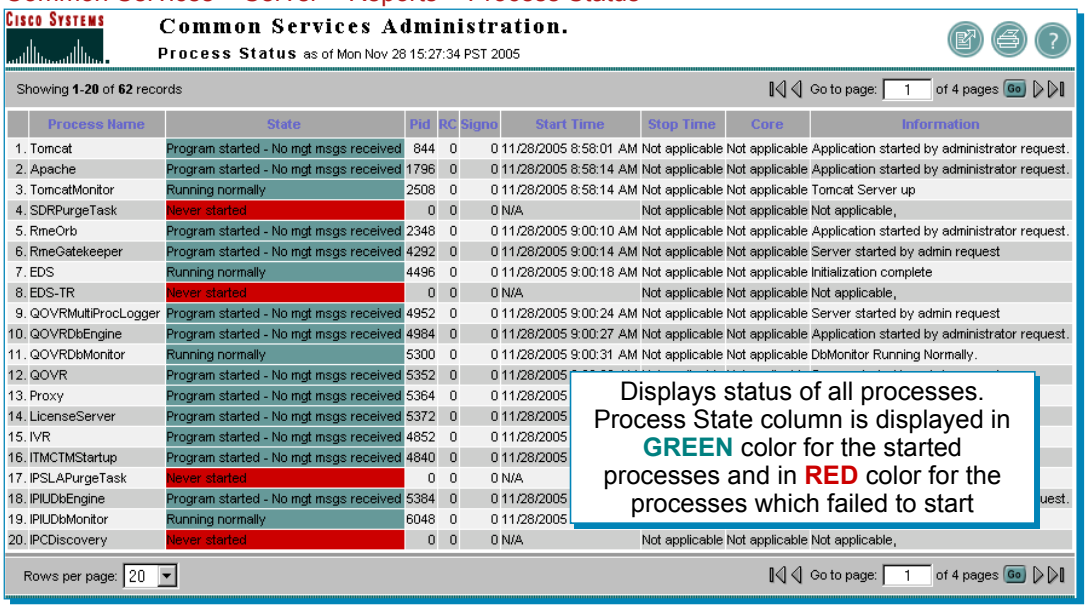
System Status

The System Status Report is useful for troubleshooting purposes in that it contains nearly all facets of Operations Manager configuration and operations. The report is launched by selecting ***Operations Manager > Administration > System Status***, and contains the following sections:

- **Processes Status**--Names of processes that failed.
- **Inventory Status**--Displays the name, last execution time, status, and next scheduled time for the following types of data collection: Discovery, DCR Domain, Device Selection, Device Inventory Collection, and Phone Inventory Collection.
- **Data Purging**--Start and end time for database purging task.
- **Diagnostics**--Lists diagnostic tests that failed to execute: Synthetic Tests, Phone Status Tests, and Node-to-Node Tests.
- **Notifications**--Device Event Description, Event ID, Destination(s), Failure Time, Reason.
- **System Limits**--Current value, Limit value, and Limited By for the following parameters: Devices, Phones, IP Communications Monitor, Synthetic Tests, Phone Reachability Tests, Node-to-Node Tests, Devices monitored for Performance and Capacity, and Devices monitored for SRST.

Helpful Troubleshooting Tips
Process Status

Common Services > Server > Reports > Process Status



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

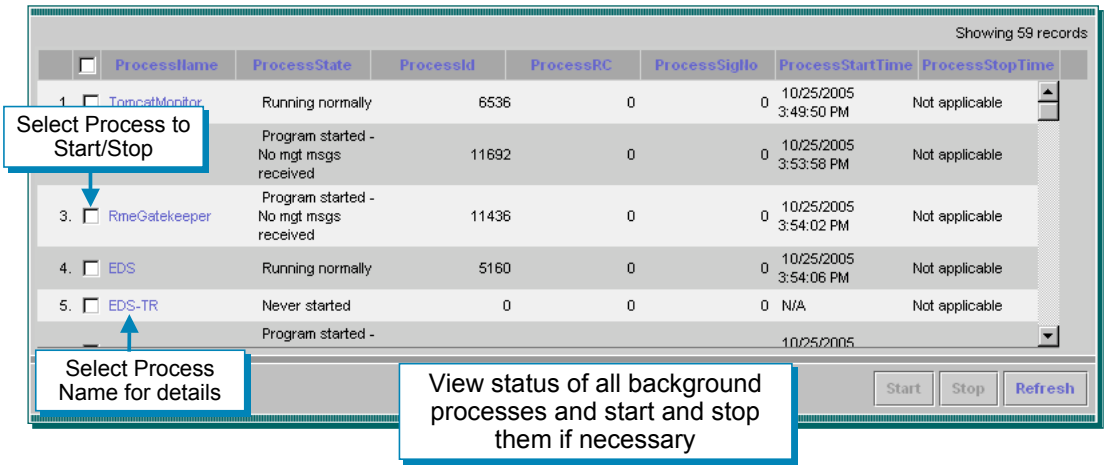
Process Status

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

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

Helpful Troubleshooting Tips
Process Management

Common Services > Server > Admin > Processes



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

Process Management

Process Management is a Common Services task used to monitor and start/stop one or more background processes. In the event something doesn't quite seem right with Operations Manager, 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 Operations Manager processes, open a Command Prompt on the server and enter:

net stop crmdmgtd

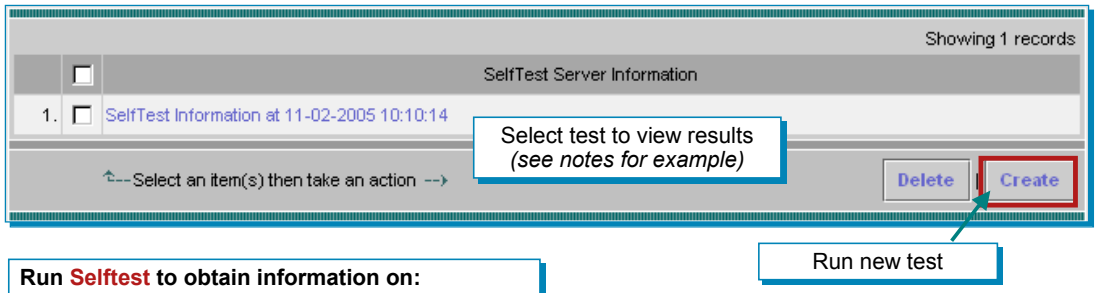
To restart all the Operations Manager processes enter:

net start crmdmgtd

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

Helpful Troubleshooting Tips
Server Self-Test

Common Services > Server > Admin > Selftest



Run Selftest to obtain information on:

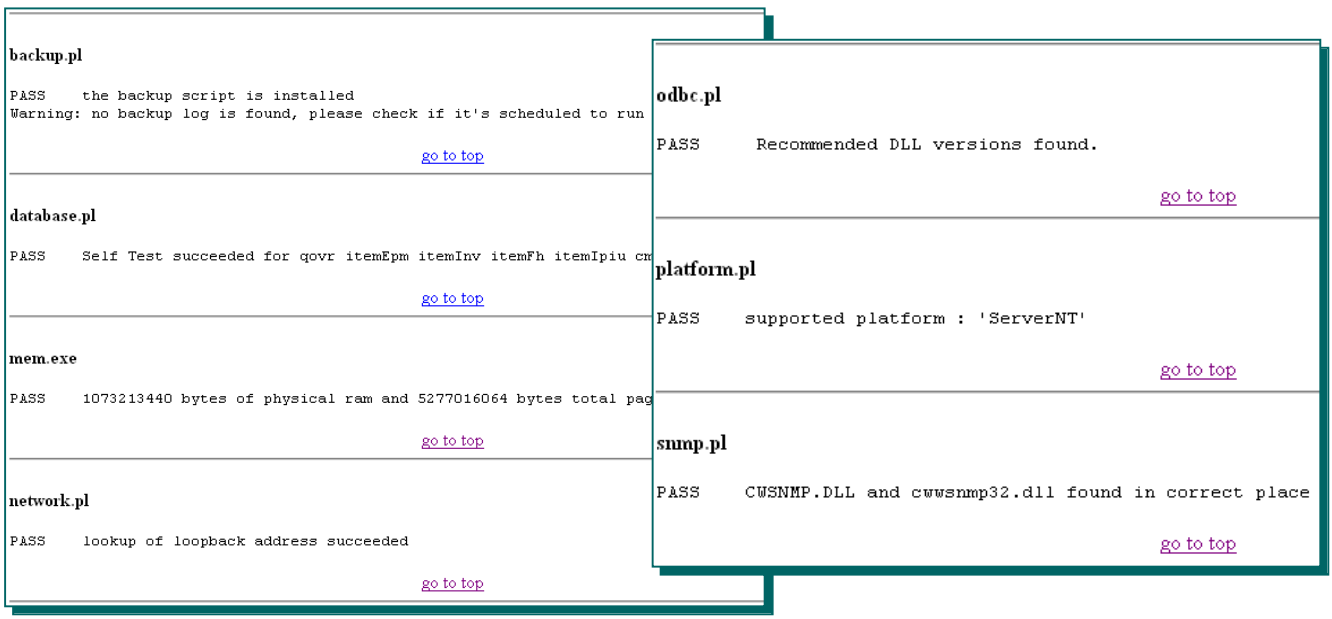
- Backup script available and if scheduled
- Test on database processes
- Check on available memory
- Test of lookback address
- Check on recommended DLL versions
- Check platform type supported
- Check SNMP processes

Server Self-Test

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

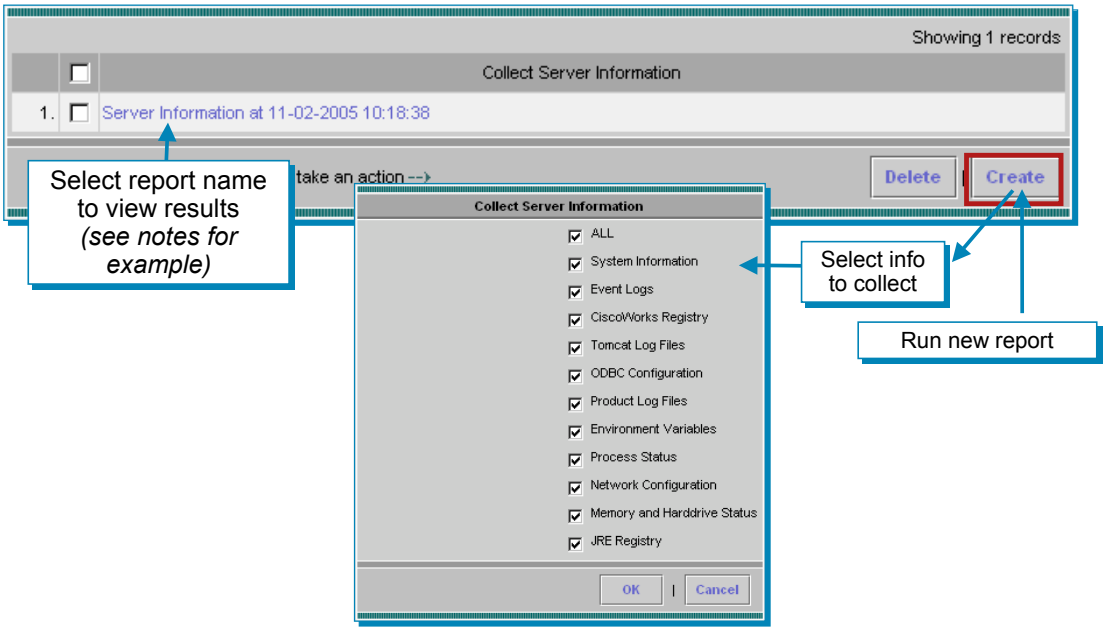
Launch the task by selecting ***Common Services > Server > Admin > Selftest***. To create a new report, click **Create**. To display the new report or a previously generated report, click the report name. Self-test reports indicate whether the tests passed or failed. Reports reflect the server time.

Excerpts from a selftest report are illustrated below.



Helpful Troubleshooting Tips
Collect Server Information

Common Services > Server > Admin > Collect Server Information



Collect Server Information

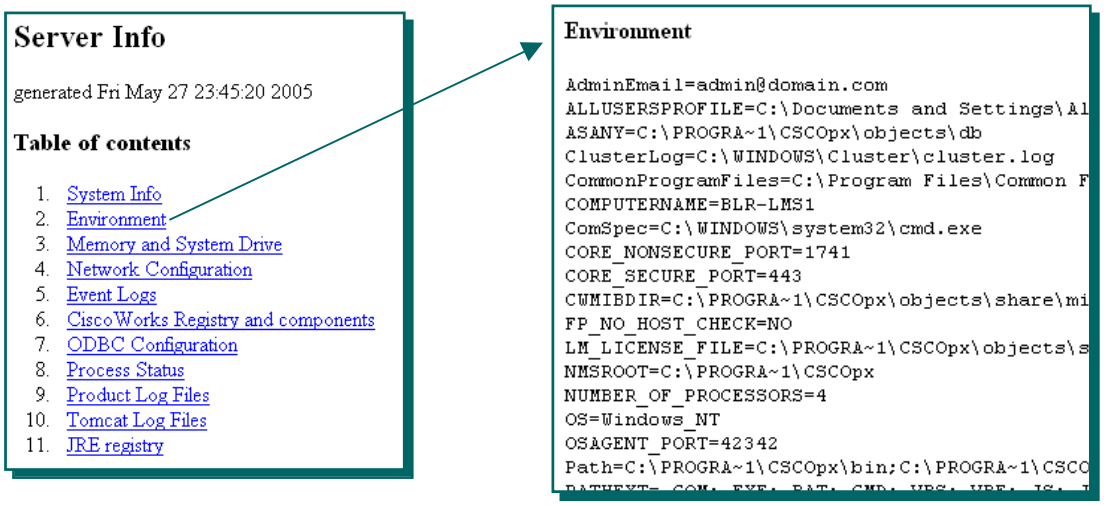
The System Administrator can gather troubleshooting information about the status of the server using this option. (*A command line script is also available at …/CSCOpx/bin/collect.info*). If you collect server information through the user interface, data is stored in …/CSCOpx/htdocs/collect.

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

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

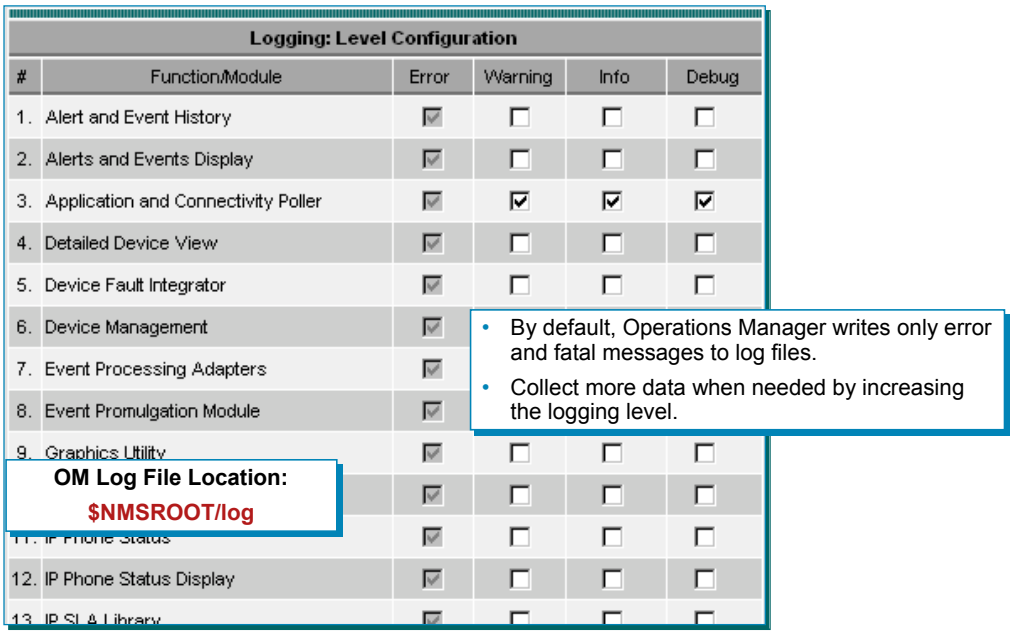
To display a report, click its name in the list of available reports. The report appears with information about the product database, the operating system, disk utilization statistics, Tomcat log files and so on. Reports reflect the server time.

Excerpts from a report are illustrated below.



Helpful Troubleshooting Tips
Log Files – Operations Manager

Operations Manager > Administration > Logging



Log File Management – Operations Manager

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

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

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

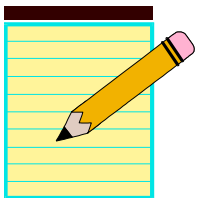
Review your changes. To cancel your changes, click the **Cancel** button. Otherwise, click the **Apply** button. Clicking the **Apply** button starts immediately resetting the changed logging levels for the Operations Manager functional modules.

Notes(s):

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

Helpful Troubleshooting Tips
MDC Support Utility

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



MDC Support Utility

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

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

Windows:

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

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

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

Thank You!

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

Cisco Systems

<*Intentionally Blank*>

Cisco Unified Operations Manager

References

Chapter 5

<Intentionally Left Blank>

Reference Materials

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

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

  - **Cisco Unified Operations Manager (URL)**
    http://www.cisco.com/en/US/products/ps6535/index.html

  - **Data Sheet (URL)**
    http://www.cisco.com/en/US/products/ps6535/products_data_sheets_list.html

  - **Install and Upgrade Guides (URL)**
    http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html

  - **Release Notes (URL)**
    http://www.cisco.com/en/US/products/ps6535/prod_release_notes_list.html

  - **User Guide (URL)**
    http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html

  - **Frequently Asked Questions (URL)**
    http://www.cisco.com/en/US/products/ps6535/prod_qandas_list.html

  - **Deployment Guide (URL)**
    http://www.cisco.com/en/US/products/ps6535/prod_presentation_list.html

- **Other Related Material**

  - **Service Monitor (URL)**

    http://www.cisco.com/en/US/products/ps6536/tsd_products_support_series_home.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 (URL)**

    http://www.cisco.com/en/US/partner/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 **Operations Manager** 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).