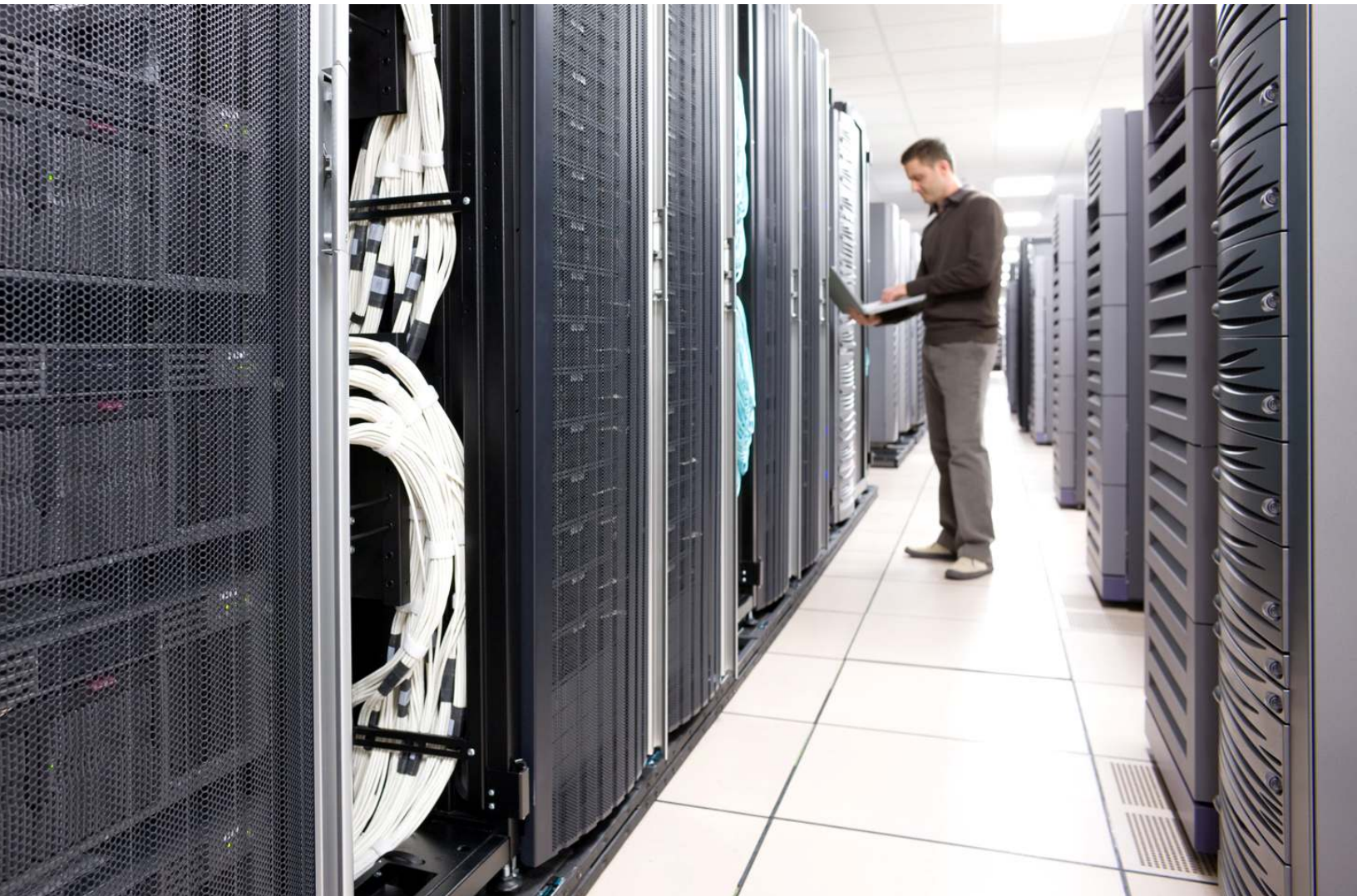
Best Practices for Monitoring Cisco Unified Contact Center Enterprise with Cisco Unified Operations Manager

White Paper



Contents

Introduction

This document highlights suggested best practices for field personnel and customers. It will help enable you to effectively use Cisco® Unified Operations Manager to monitor Cisco Unified Contact Center Enterprise (Unified CCE).

Other documents that address the monitoring of the other Cisco Unified Communications components are available. This document does not replace the Cisco Unified Operations Manager user guide, which is available on Cisco.com at http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html.

In addition, you will find the best-practices document for deployment topics such as initial device setup, installation guidelines, server sizing, and so on, at http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html.

About Cisco Unified Operations Manager

Cisco Unified Operations Manager (referred to as Operations Manager from this point forward) provides a unified view of the entire IP communications infrastructure. It presents the current operational status of each element of the IP communications network. Operations Manager continuously monitors the current operational status of different IP communications elements, such as:

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager Express
- Cisco Unity® software
- Cisco Unity Express
- Cisco Unified Contact Center
- Cisco Unified Contact Center Express
- Cisco Unified Presence Server
- Cisco Emergency Responder
- Cisco Unified MeetingPlace® Express
- Cisco gateways, routers, switches, and IP phones

Operations Manager also provides diagnostic capabilities for faster trouble isolation and resolution. It monitors and evaluates the current status of both the IP communications infrastructure and the underlying transport infrastructure in the network. It 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 your IP communications deployment. Because Operations Manager does not deploy any agent software on the devices being monitored, it is nondisruptive to your system operations.

Managing Cisco Unified Contact Center Enterprise

This document will focus primarily on the management aspects of Cisco Unified Contact Center Enterprise (CCE) products. While there are a number of references to Cisco Unified Intelligent Contact Management Enterprise (Unified ICME), and many components are identical between Unified ICME and Unified CCE, the content herein is intended for Unified CCE management.

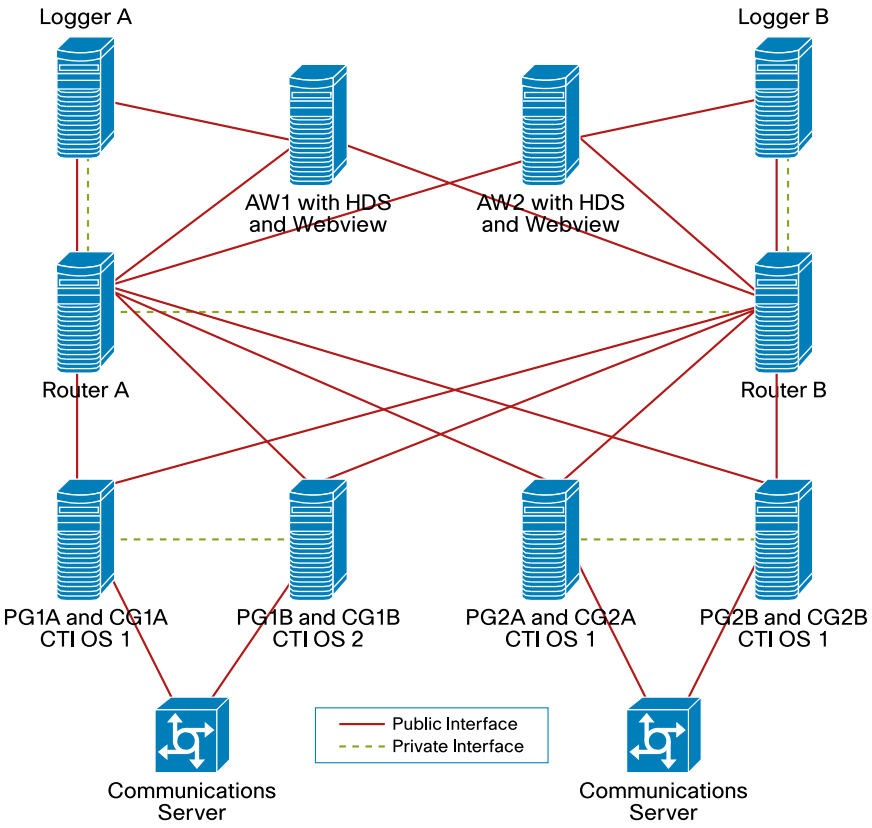
The following are the four major components of a Unified CCE deployment, and their basic functions:

- **Router:** Makes the routing decisions. Select a peripheral or agent to receive an inbound contact (voice call, email, chat).
- **Logger:** Stores and replicates all configuration, real-time, and historical data.

- **Peripheral Gateway:** Acts as a gateway to a peripheral device—an IP PBX or an Interactive Voice Response (IVR) unit—as well as a Computer Telephony Interface (CTI) gateway, linking agent desktops.
- **Admin Workstation:** A server implementation that provides a copy of configuration data from the logger, an interface for real-time data, and a platform for the historical data server (HDS). The Admin Workstation also offers an interface for administrators to generate reports (Webview) and alter configuration and routing scripts (Script Editor, Internet Script Editor).

Figure 1 shows a typical Cisco Unified CCE deployment from a device standpoint.

Figure 1. Typical Unified CCE Deployment



Unified CCE is a distributed solution. The component set, to be installed on separate servers, comprises:

- Router
- Logger
- Peripheral Gateway
- Admin Workstation/HDS
- Peripheral Interface Manager (PIM)

Each server (Side A) will have a redundant server running on the other side (Side B).

For Operations Manager to manage Unified CCE, you must add the primary and redundant servers running Unified CCE components to Operations Manager using **Devices > Device Management > Add Devices**. When you want to add a device to Operations Manager, keep the following information nearby:

- The IP address or hostname
- The SNMP read-only credentials

- Windows administrator credentials

Note: The Microsoft Windows SNMP service for processing SNMP requests is disabled as part of Unified CCE setup and replaced by the Unified CCE SNMP Management service. The Unified CCE SNMP Management service is provided for more sophisticated SNMP capabilities than are offered by the standard Microsoft Windows SNMP service.

Follow the instructions in the SNMP guide for Cisco Unified Contact Center Enterprise and Hosted editions to install the correct SNMP components required for managing Unified CCE devices using Operations Manager.

You can configure Cisco SNMP Agent Management settings using the Microsoft Management Console snap-in.

Once the Unified CCE devices have been added and Operations Manager has collected the required inventory details from the device, Operations Manager marks the devices as Monitored. This signals that the Unified CCE devices have been successfully added and are being managed by Operations Manager.

If your devices are not going into the Monitored state, see the sections "Why Does a Device go into the Partially Monitored State?" and "Why Does a Device Go into the Unreachable State?" in the User Guide for Cisco Unified Operations Manager at http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html.

Once a Unified CCE device is in the Monitored state, you can open the Service Level View from the Operations Manager Monitoring Dashboard. You can find the Unified CCE device that you have just added in the tree view on the left, by navigating to **All IP communications devices > IPCC**.

Figure 2 shows one of the main entry points for managing devices. By right-clicking a device in the tree/map view, you can see a list of context-sensitive tools that can be used on that device (Figure 3).

Figure 2. Entry Point for Managing Unified CCE Devices

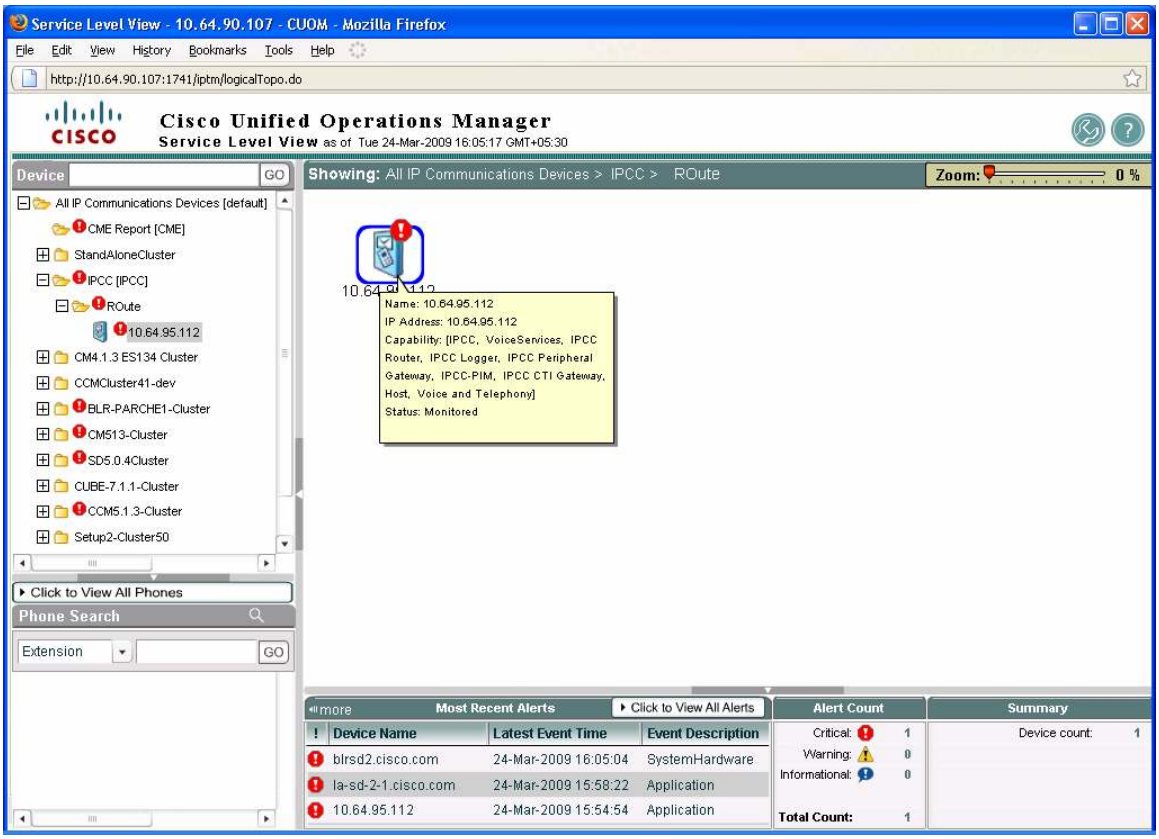


Figure 3. List of Context-Sensitive Tools

Basic Health Monitoring

Operations Manager monitors the system and environment parameters of a Unified CCE device listed in Table 1.

Table 1. Basic Health Monitoring

Monitored Parameters	Description
System	Usage of processor and device memory along with status of interfaces on the Unified CCE device
Environment	Status of system fan, system temperature sensor, voltage sensor, and system power supply of the Unified CCE device

You can see the details of these parameters by selecting the **Detailed Device View** right-click option on the device from the Service Level View.

Fault Monitoring

View the list of active alarms on a Cisco Unified Contact Center device by selecting the Alert Details right-click option on the device from the Service Level View. Clicking the Event ID displays the Event Details, indicating the exact nature of the event.

You can also view the alarm history on a Cisco Unified Contact Center device by selecting the **Fault History** right-click option on the device from the Service Level View.

Operations Manager performs monitoring and generates events on fault conditions detected on a Cisco Unified Contact Center device. (See Table 2: Fault Monitoring.)

Table 2. Fault Monitoring

Fault Condition	Event Details
Processor utilization	**HighUtilization** • Event Description: This event indicates that current utilization exceeds the utilization threshold configured for this network adapter or processor. • Default Threshold: 90 percent • Recommended Actions (Processor related): The most common reason is that one or more processes are using excessive CPU space. Once the process is identified, you may want to restart the process.

Memory utilization	**InsufficientFreeMemory** • Event Description: This event indicates that the system is running out of memory resources. Also reported if there has been a failure to allocate a buffer due to lack of memory. • Default Threshold: 15 percent • Recommended Actions: Use Unified CM Windows Task Manager to check memory utilization. Sometimes high memory utilization is indicative of a memory leak. It is important to identify which process is using excessive memory.
System fan is down or degraded	**FanDown** • Event Description: This event indicates that a required fan is not operating correctly. The event is based on processing the SNMP trap cpqHeThermalSystemFanFailed received from monitored Cisco Unified Communications Managers. • Default Threshold: N/A • Recommended Actions: Check the status of the reported fan and contact Cisco for hardware replacement. **FanDegraded** • Event Description: This event indicates that an optional fan is not operating correctly. The event is based on polling or processing the SNMP trap cpqHeThermalSystemFanDegraded received from monitored Cisco Unified Communications Managers. • Default Threshold: N/A • Recommended Actions: Check the status of the reported fan and monitor for recurrence.
System chassis temperature is high	**TemperatureHigh** • Event Description: This event is generated if a temperature sensor's current temperature exceeds the Relative Temperature Threshold. • Default Polling Interval: 4 minutes • Default Threshold: 10 percent • Recommended Actions: Verify that environmental temperatures are set up optimally. Check other events, such as FanDown or FanDegraded, to verify that fans are operating normally. If fans are not operating normally, you should contact Cisco for hardware replacement.
System temperature sensor is down or degraded	**TemperatureSensorDown** • Event Description: This event indicates that the server's temperature is outside of the normal operating range and the system will be shut down. The event is based on processing the SNMP trap cpqHeThermalTempFailed received from monitored Cisco Unified Communications Managers. • Default Threshold: N/A • Recommended Actions: Verify that environmental temperatures are set up correctly. Identify the reported temperature sensor location (ioborad/cpu) and verify status. Check other events, such as FanDown or FanDegraded, to verify that system fans are operating normally. Contact Cisco for hardware replacement, if needed. **TemperatureSensorDegraded** • Event Description: This event indicates that the server's temperature is outside of the normal operating range. The event is based on polling or processing the SNMP traps cpqHeThermalTempDegraded received from monitored Cisco Unified Communications Managers. • Default Threshold: N/A • Recommended Actions: Identify the reported temperature sensor location (ioborad/cpu) and verify status. Check other events, such as FanDown or FanDegraded, to verify that system fans are operating normally. Contact Cisco for hardware replacement, if needed.
System power supply is down or degraded	**PowerSupplyDown** • Event Description: Power supply state is down. • Default Polling Interval: 4 minutes • Default Threshold: N/A • Recommended Actions: Check the status of reported power supply and contact Cisco for hardware replacement if the primary power supply is down. **PowerSupplyDegraded** • Event Description: Power supply state is degraded. • Default Polling Interval: 4 minutes • Default Threshold: N/A • Recommended Actions: Check the status of reported power supply and monitor for recurrence.
System interface or hardware is operationally down	**Operationally Down** • Event Description: ◦ Interface: Card or network adapter's operational state is not normal. ◦ System Hardware: Disk's operational state is not normal. • Default Polling Interval: 4 minutes • Default Threshold: N/A • Recommended Actions: Check the status of the indicated interface and investigate the root cause.

NIC is down	**nicDown** • Event Description: This event indicates that the Network Interface Controller (NIC) is down on a Unified CCE device. This affects Time Division Multiplexing (TDM)–based telephony services. • Default Polling Interval: 4 minutes • Default Threshold: N/A • Recommended Actions: Verify that the NIC service is running. Try restarting the service if it has stopped. If the service does not start, contact the Cisco Technical Assistance Center (TAC).
PIM is down	**pimDown** • Event Description: The Peripheral Interface Manager module acts as a gateway to a peripheral device (a Unified CM, an IVR, or a CTI Agent). This event indicates that the PIM is down on a Unified CM device, and connectivity to peripheral devices is lost. • Default Polling Interval: 4 minutes • Default Threshold: N/A • Recommended Actions: Verify that the PIM service is running. Try starting the service if it has stopped. If the service does not start, contact the Cisco Technical Assistance Center. Check network connectivity across the peripheral devices and Unified CCE.
A critical application stops running	**ServiceDown** • Event Description: This event is generated when one of the critical services (any of the services in the Detailed Device View) is not running. The problem could be due to someone manually stopping the service. If you intend to stop the service for a long period of time, disabling monitoring for the service is highly recommended and is needed to avoid this alert. Go to Service Level View > Detailed Device View, select the specific service, and change the managed state to False. • Default Polling Interval: 30 seconds • Default Threshold: N/A • Recommended Actions: Identify which services are not running. You can start the service manually from the Administrator page.
Unified CCE Notifications	**IPCCDualStateNotification** • Event Description: The Unified CCE logger component sent a notification. • Trigger: Processed SNMP trap • Recommended Actions: See Recommendations on Monitoring Cisco Unified Contact Center Enterprise Notifications. **IPCCSingleStateNotification** • Event Description: The Unified CCE logger component sent a notification. • Trigger: Processed SNMP trap • Recommended Actions: See Recommendations on Monitoring Cisco Unified Contact Center Enterprise Notifications.

Polling and Thresholds

You can configure the interval at which Operations Manager polls specific information from the Cisco Unified Contact Center device, as well as set the thresholds based on which alerts should be raised by Operations Manager.

Configure polling intervals by selecting the **Polling Parameters** right-click option on the device from the Service Level View. For Cisco Unified Contact Center devices, the polling parameters are defined in the group /System Defined Groups/Cisco Unified Communications Applications/IP Contact Center. Configure the polling setting related to basic health monitoring by selecting the **Voice Health Settings** parameter type (Table 3).

Table 3. Polling Settings for Cisco Unified Contact Center Devices

Parameter	Polling Settings
System	• Hard Disk and Virtual Memory • Processor and Memory Utilization
Environment	• Power Supply • Fan • Temperature Sensor
Interface	• Connector Port and Interface • Access Port
Application	Application Polling
Device Specific	Cisco IP Contact Center

You can configure the thresholds by selecting the **Threshold Parameters** right-click option on the device from the Service Level View. For Contact Center devices, the threshold parameters are defined in the group System Defined Groups/Cisco Unified Communications Applications/IP Contact Center. You can configure the threshold setting related to basic health monitoring by selecting **Voice Health Settings** as the parameter type. You can choose from two threshold categories, depending on the exact threshold that you need to configure (Table 4).

Table 4. Threshold Settings

Parameter	Polling Settings
System	• Processor and Memory • Disk Usage and Virtual Memory
Environment	Temperature Sensor

Performance Monitoring

Operations Manager performs trending of the following categories on a Cisco Unified Contact Center device:

- Processor and Memory Usage (Percentage)
- For the given router instance name:
  - Agents Logged On (Number)
  - Call in Progress (Number)
  - Inbound Calls per Sec (Number)

You can view the performance report or graphs over the past 72 hours by selecting the **Performance** right-click option on the device from the Service Level View, and then selecting the performance parameter that you want to view. You can view multiple performance reports or graphs in a single screen.

By default, performance polling for a Unified CCE device is disabled in Operations Manager. To enable it, open the Polling Parameters page as described, select **Voice Utilization Settings** as the parameter type, and then check the **Polling Enabled** check box. Click **Apply** for the changes to take effect.

You can also configure the thresholds for the performance parameters by opening the Thresholds Parameter page and selecting Voice Utilization Settings as the parameter type.

Synthetic Tests

To test IP-IVR reach, you can set a synthetic test by selecting the End-to-End Call Test right-click option on the Cisco Unified Communications Manager device from the Service Level View. An End-to-End Call test initiates a call to an IP-IVR to verify that it is alive. The call passes the test if the simulated phone registers, goes off-hook, and places the call to the IP-IVR. There is a ring indication, and the destination IP-IVR goes off-hook to accept the call.

You can run this test on demand or on a scheduled basis for proactive monitoring.

Note: You cannot test the real-time protocol (RTP) transmission part of a synthetic phone-to-IVR setup. You can test only the answering part (Wait for Answer).

To run a synthetic test, you must have the necessary number of simulated Cisco 7960 phones configured in the Cisco Unified Communications Manager database; however, if autoregistration is enabled in Cisco Unified Communications Manager, this step is not necessary. To define simulated phones in a Cisco Unified Communications Manager for the synthetic tests, do the following:

Step 1. Open and log in to the Cisco Unified Communications Manager Administration page.

Step 2. From the Cisco Unified Communications Manager Administration page, select Device > Add a New Device.

Step 3. From the Device Type drop-down list, select Phone. Click Next.

Step 4. Select Cisco 7960 as the phone type for the simulated phone. Click Next.

Step 5. In the Phone Configuration page, enter a MAC address between 00059a3b7700 and 00059a3b8aff. The tool automatically fills in the Description field. Other required fields are Device Pool and Button Template. Use the defaults. Click Insert.

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

Physical Connectivity

View the Layer 2 or Layer 3 connectivity of the network in which the Cisco Unified Contact Center resides by selecting the Connectivity Details right-click option on the device from the Service Level View.

Logical View

Search the Cisco Unified Contact Center device in the Service Level View by providing the managed name of the device. Clicking the device opens the Map View in the right pane, showing the Logical Connectivity View.

Device Troubleshooting

Open the Cisco Unified Contact Center Administration page by selecting the **Device Administration** right-click option on the device from the Service Level View.

Device Administration

Suspend monitoring of a Cisco Unified Contact Center device, by selecting the **Suspend Device** right-click option on the device from the Service Level View. When the device is in the Suspended state, it no longer communicates with Operations Manager. You might want to suspend the device to avoid false alarms when the Cisco Unified Contact Center is in Maintenance mode.

You can resume monitoring of a Cisco Unified Contact Center device, by selecting the **Resume Device** right-click option on the device from the Service Level View.

You can also delete the Cisco Unified Contact Center device from Operations Manager by selecting the **Delete Device** right-click option on the device from the Service Level View.

Recommendations on Monitoring Cisco Unified Contact Center Enterprise Notifications

SNMP notifications generated by the Unified CCE application are always generated as SNMP traps from the logger component; only generic traps or traps from other subagents (such as the platform subagents provided by Hewlett Packard or IBM) are generated from Unified CCE nodes other than the logger.

This section includes examples of Unified CCE notifications (Figure 4 and Figure 5).

Figure 4. Alarm Example – Raise Alarm

```
snmpTrapOID.0 = cccaIcmEvent
cccaEventComponentId = 4_1_CC-RGR1A_ICM\acme\RouterA
cccaEventState = raise(4
cccaEventMessageId = 2701295877
cccaEventOriginatingNode = CC-RGR1A\acme
cccaEventOriginatingNodeType = router(1)
```

```
cccaEventOriginatingProcessName = nm
cccaEventOriginatingSide = sideA(1)
cccaEventDmpId = 0
cccaEventSeverity = warning(2)
cccaEventTimestamp = 2006-03-31,14:19:42.0
cccaEventText = The operator/administrator has shutdown the ICM software on
ICM\acme\RouterA
```

Figure 5. Alarm Example – Clear Alarm

```
snmpTrapOID.0 = cccaIcmEvent
cccaEventComponentId = 4_1_CC-RGR1A_ICM\acme\RouterA
cccaEventState = clear(0)
cccaEventMessageId = 1627554051
cccaEventOriginatingNode = CC-RGR1A\acme
cccaEventOriginatingNodeType = router(1) cccaEventOriginatingProcessName = nm
cccaEventOriginatingSide = sideA(1)
cccaEventDmpId = 0
cccaEventSeverity = informational(1)
cccaEventTimestamp = 2006-03-31,13:54:12.0
cccaEventText = ICM\acme\RouterA Node Manager started. Last shutdown was by
operator request.
```

You can see the processed Unified CCE notifications on the Cisco Unified Operations Manager – Alerts and Events display. A Unified CCE notification message is uniquely identified with its component and message ID as shown in Figure 6.

Dual-State Notification

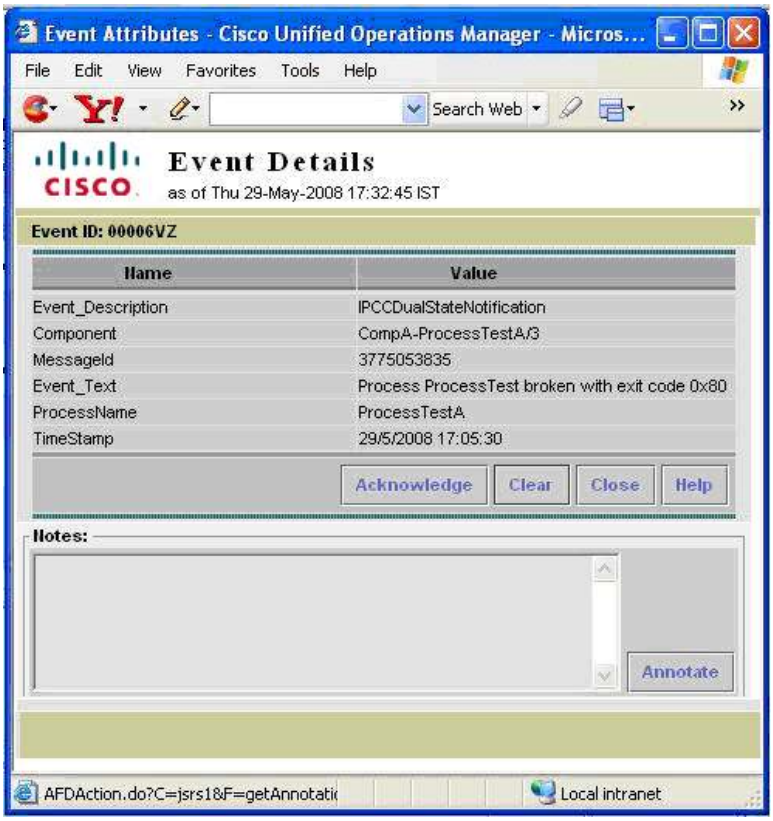
Dual-state notification can show either the Raise or Clear state of an incident. A trap in the Raise state indicates an operational issue, while a trap in the Clear state indicates that a specific operational issue has been resolved. Cisco Unified Operations Manager clears an event in the Raise state when its associated Clear state event has been processed (Table 5).

Table 5. Dual-State Unified CCE Notification

Event ID	State	Description
3775053835 (0xE102C00B)	Raise	Terminating process %1.
3775053836 (0xE102C00C)	Raise	Process %1 exited after having detected a software failure.
2701312013 (0xA102C00D)	Raise	Process %1 detected failure and requested that it be restarted by the Node Manager.
3775053838 (0xE102C00E)	Raise	Process %1 exited with unexpected exit code %2.
2701312015 (0xA102C00F)	Raise	Process %3 exited after %1 seconds. Process restart will be delayed for a minimum of %2 seconds.
2701312016 (0xA102C010)	Clear	Process %1 successfully reinitialized after restart.
1627570193 (0x6102C011)	Clear	Process %1 successfully started.

For example, if Cisco Unified Operations Manager receives a Unified CCE Raise event with message ID = 3775053835 on an IPCC component, say CompA, the event details will have the information shown in Figure 6.

Figure 6. Alerts and Events Alarm Example – Raise Alarm



If Cisco Unified Operations Manager receives another IPCC Raise event with message ID = 2701312013 on the same component (CompA), then the details for the same event (CompA; message ID = 3775053835) are updated. This particular Raise event on CompA is cleared when Cisco Unified Operations Manager processes a Clear event (message ID 2701312016 or 1627570193), as shown in Table 5. You can see the cleared event on the Cisco Unified Operations Manager Event History with its clear state information, as shown in Figure 7.

Figure 7. Event History Alarm Example – Clear Alarm

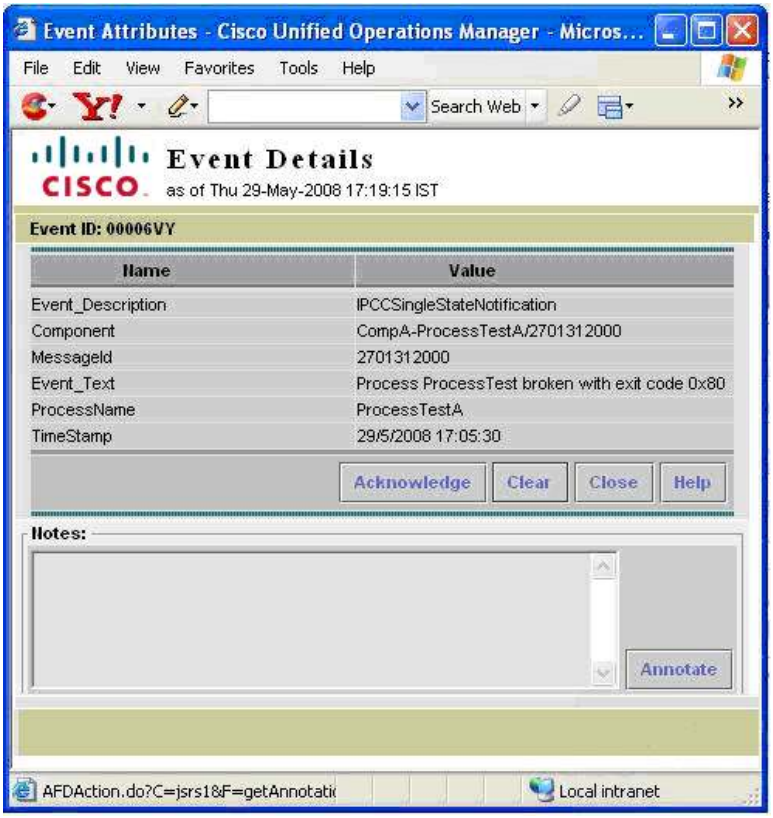
Single-State Notification

Single-state notification is another type of IPCC notification. Single-state notifications are not associated with any Clear state notifications. The following are the differences between Raise and single-state Raise:

- **Raise:** The Raise state identifies a notification received as a result of a health-affecting condition, such as a process failure. A subsequent clear state notification will follow when the error condition is resolved.
- **Single-State Raise:** The single-state Raise state indicates that a health-affecting error has occurred and that a subsequent Clear state notification will not be forthcoming. An example of a single-state Raise condition is an application configuration error that requires the system to be stopped and the problem resolved by an administrator before the affected component will function properly.

On Cisco Unified Operations Manager, you can see a separate type of event—*IPCCSingleStateNotification*—corresponding to an IPCC single-state trap as shown in Figure 8. The value of the Component property is written as *ComponentId-ProcessName/MessageId*. If you do not clear this event within 30 minutes of receiving it, this single-state notification is automatically cleared by Cisco Unified Operations Manager.

Figure 8. Single-State Notification



For more information on Unified CCE device SNMP notifications, see http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_7_2/configuration/guide/serviceability.pdf.

See the following table containing events processed by Cisco Unified Operations Manager.

Table 6. CUCCE traps

Message ID (hex)	Type	Severity	Message Class	MessageText	Description	Action
102C001*	Raise	Error	NM REBOOT ON FAIL	Critical process %1 died. Rebooting node.	A critical process needed to run the ICM software on this node has died. The Node Manager is forcing a reboot of the node.	Contact the Support Center.
102C003*	Clear	Warning	NM REBOOT ON FAIL	Restarting process %1.	The Node Manager is restarting process %1 after the process died or was terminated.	No action is required.
102C009*	Raise	Warning	NM REBOOT ON FAIL	Process %4 exited after %1 seconds. Minimum required uptime for %4 process is %2 seconds. Delaying process restart for %3 seconds.	Process %4 exited after running for %1 seconds. Such processes must run for at least %2 seconds before the Node Manager will automatically restart them after they terminate. The Node Manager will restart the process after delaying %3 seconds for other environmental changes to complete.	No action is required.
102C00A*	Clear	Warning	NM REBOOT ON FAIL	Restarting process %2 after having delayed restart for %1 seconds.	The Node Manager is restarting process %2 after the requisite delay of %1 seconds.	No action is required.
102C00B*	Raise	Error	NM REBOOT ON FAIL	Terminating process %1.	The Node Manager is terminating process %1.	No action is required.

102C00C*	Raise	Error	NM REBOOT ON FAIL	Process %1 exited after having detected a software failure.	Process %1 exited (terminated itself) after it detected an internal software error.	If the process continues to terminate itself, call the Support Center.
102C00D*	Raise	Warning	NM REBOOT ON FAIL	Process %1 detected failure and requested that it be restarted by the Node Manager.	Process %1 has detected a situation that requires it to request that the Node Manager restart it. This often indicates a problem external to the process itself (for example, some other process may have failed).	If the process continues to terminate itself, call the Support Center.
102C00E*	Raise	Error	NM REBOOT ON FAIL	Process %1 exited with unexpected exit code %2.	Process %1 exited (terminated) with exit code %2. This termination is unexpected and the process died for an unknown reason.	Contact the Support Center.
102C00F*	Raise	Warning	NM REBOOT ON FAIL	Process %3 exited after %1 seconds. Process restart will be delayed for a minimum of %2 seconds.	Process %3 exited after running for %1 seconds. The Node Manager will restart the process after delaying %2 seconds for other environmental changes to complete.	If the process continues to terminate itself, call the Support Center.
102C010*	Clear	Warning	NM REBOOT ON FAIL	Process %1 successfully reinitialized after restart.	Process %1 was successfully restarted.	No action is required.
102C011*	Clear	Informational	NM REBOOT ON FAIL	Process %1 successfully started.	Process %1 was successfully started.	No action is required.
102C012*	Raise	Warning	NM REBOOT ON FAIL	Process %1 exited cleanly and requested that it be restarted by the Node Manager.	Process %1 terminated itself successfully and has requested that the Node Manager restart it.	No action is required.
102C013	Raise	Warning	NM REBOOT ON FAIL	Process %1 exited from Control-C or window close.	Process %1 exited as a result of a CTRL-C request or a request to close the process's active window.	No action is required.
102C014*	Raise	Error	NM INITIALIZING	Process %1 exited and requested that the Node Manager reboot the system.	Process %1 terminated itself successfully but, due to other conditions, has requested that the Node Manager reboot the machine.	No action is required.
102C101*	Raise	Error	NM REBOOT ON FAIL	%1 node critical process %2 died. Rebooting node.	A critical process needed to run the ICM software on this node has died. The Node Manager is forcing a reboot of the node.	Contact the Support Center.
102C103*	Clear	Warning	NM REBOOT ON FAIL	%1 node restarting process %2.	The Node Manager is restarting process %2 after the process died or was terminated.	No action is required.
102C107*	Clear	Informational	NM INITIALIZING	%1 Node Manager started. Last shutdown was for reboot after failure of critical process.	The Node Manager has started. The last shutdown was requested by the Node Manager since it recognized that a critical process for the node failed.	No action is required.
102C108*	Clear	Error	NM INITIALIZING	%1 Node Manager started. Last shutdown was for unknown reasons. Possible causes include a power failure, a system crash or a Node Manager crash.	The Node Manager has started. The Node Manager cannot determine why the system is restarting. Possible causes are: power failure, a system crash (Windows NT blue screen), a system hang (in which an operator forced a reboot), or the Node Manager itself crashed.	Contact the Support Center.
102C109*	Raise	Warning	NM REBOOT ON FAIL	%4 node process %5 exited after %1 seconds. Minimum required uptime for %5 process is %2 seconds. Delaying process restart for %3 seconds.	Process %5 exited after running for %1 seconds. Such processes must run for at least %2 seconds before the Node Manager will automatically restart them after they terminate. The Node Manager will restart the process after delaying %3 seconds for other environmental changes to complete.	No action is required.
102C10A*	Clear	Warning	NM REBOOT ON FAIL	%2 node restarting process %3 after having	The Node Manager is restarting process %3 after the requisite	No action is required.

				delayed restart for %1 seconds.	delay of %1 seconds.	
102C10B*	Raise	Error	NM REBOOT ON FAIL	Terminating process %2.	The %1 Node Manager is terminating process %2.	No action is required.
102C10C*	Raise	Error	NM REBOOT ON FAIL	%1 node process %2 exited after having detected a software failure.	Process %2 exited (terminated itself) after it detected an internal software error.	If the process continues to terminate itself, call the Support Center.
102C10D*	Raise	Warning	NM REBOOT ON FAIL	Process %2 on %1 has detected a failure. Node Manager is restarting the process.	The specified Process has detected a situation that requires it to request that the Node Manager restart it. This often indicates a problem external to the process itself (for example, some other process may have failed).	Node Manager on the ICM node will restart the process. The node should be checked to assure it is online using rttest. If the condition is common, the process logs must be examined for cause.
102C10E*	Raise	Error	NM REBOOT ON FAIL	Process %2 on %1 went down for unknown reason. Exit code %3. It will be automatically restarted.	The specified Process exited (terminated) with the indicated exit code. This termination is unexpected and the process died for an unknown reason. It will be automatically restarted.	Contact the Support Center.
102C10F*	Raise	Warning	NM REBOOT ON FAIL	Process %4 on %3 is down after running for %1 seconds. It will restart after delaying %2 seconds for related operations to complete.	Specified process is down after running for the indicated number of seconds. It will restart after delaying for the specified number of seconds for related operations to complete.	Determine if process has returned to service or has stayed offline. If process is offline or bouncing determine the cause from logs.
102C110*	Clear	Warning	NM REBOOT ON FAIL	%1 node process %2 successfully reinitialized after restart.	Process %2 was successfully restarted.	No action is required.
102C111*	Clear	Informational	NM REBOOT ON FAIL	%1 node process %2 successfully started.	Process %2 was successfully started.	No action is required.
102C112*	Raise	Warning	NM REBOOT ON FAIL	%1 node process %2 exited cleanly and requested that it be restarted by the Node Manager.	Process %2 terminated itself successfully and has requested that the Node Manager restart it.	No action is required.
102C113	Raise	Warning	NM REBOOT ON FAIL	%1 node process %2 exited from Control-C or window close.	Process %2 exited as a result of a CTRL-C request or a request to close the process's active window.	No action is required.
102C114*	Raise	Error	NM INITIALIZING	%1 node process %2 exited and requested that the Node Manager reboot the system.	Process %2 terminated itself successfully but, due to other conditions, has requested that the Node Manager reboot the machine.	No action is required.
102D001*	Raise	Error	NM INITIALIZING	Node Manager crashed after having been up for %1 seconds. Scheduling system reboot in %2 seconds.	The Node Manager has itself crashed after having run for %1 seconds. The machine will be rebooted after waiting %2 seconds.	Contact the Support Center.
102D002*	Raise	Error	NM INITIALIZING	Node Manager crashed after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.	The Node Manager has itself crashed after having run for %1 seconds. The machine cannot be rebooted since auto-reboot is disabled. The Node Manager Manager will attempt to restart the service.	Contact the Support Center.
102D003*	Raise	Error	NM INITIALIZING	Node Manager requested reboot after having been up for %1 seconds. Scheduling system reboot in %2 seconds.	The Node Manager has requested the machine be rebooted after having run for %1 seconds. The machine will be rebooted after waiting %2 seconds.	Contact the Support Center.

102D004*	Raise	Error	NM INITIALIZING	Node Manager requested reboot after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.	The Node Manager has requested the machine be rebooted after having run for %1 seconds. The machine cannot be rebooted since auto-reboot is disabled. The Node Manager Manager will attempt to restart the service.	Contact the Support Center.
102D101*	Raise	Error	NM INITIALIZING	%3 Node Manager crashed after having been up for %1 seconds. Scheduling system reboot in %2 seconds.	The Node Manager has itself crashed after having run for %1 seconds. The machine will be rebooted after waiting %2 seconds.	Contact the Support Center.
102D102*	Raise	Error	NM INITIALIZING	%2 Node Manager crashed after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.	The Node Manager has itself crashed after having run for %1 seconds. The machine cannot be rebooted since auto-reboot is disabled. The Node Manager Manager will attempt to restart the service.	Contact the Support Center.
102D103*	Raise	Error	NM INITIALIZING	%3 Node Manager requested reboot after having been up for %1 seconds. Scheduling system reboot in %2 seconds.	The Node Manager has requested the machine be rebooted after having run for %1 seconds. The machine will be rebooted after waiting %2 seconds.	Contact the Support Center.
102D104*	Raise	Error	NM INITIALIZING	%2 Node Manager requested reboot after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.	The Node Manager has requested the machine be rebooted after having run for %1 seconds. The machine cannot be rebooted since auto-reboot is disabled. The Node Manager Manager will attempt to restart the service.	Contact the Support Center.
102D105*	Raise	Error	NM INITIALIZING	%2 A Critical Process has requested a reboot after the service has been up for %1 seconds. Auto-reboot on Process Request is disabled. Will attempt service restart.	A Critical Process has requested a reboot after the service has been up for %1 seconds. The machine cannot be rebooted since Auto-reboot on Process Request is disabled. The Node Manager Manager will attempt to restart the service.	Contact the Support Center.
102D106*	Raise	Error	NM INITIALIZING	%3 A Critical Process has requested a reboot after having been up for %1 seconds. Scheduling system reboot in %2 seconds.	A Critical Process has requested the machine be rebooted after having run for %1 seconds. The machine will be rebooted after waiting %2 seconds.	Contact the Support Center.
1040010*	Raise	Warning	MDS SYNCH CONNECT TIMEOUT	Synchronizer timed out trying to establish connection to peer.	The MDS message synchronizer was unable to connect to its duplexed partner within the timeout period. Either the duplexed partner is down, or there is no connectivity to the duplexed partner on the private network.	Verify reliable network connectivity on the private network. Call the Cisco Systems, Inc. Customer Support Center in the event of a software failure on the duplexed partner.
1040022*	Raise	Error	MDS SYNCH CONNECT TIMEOUT	Connectivity with duplexed partner has been lost due a failure of the private network, or duplexed partner is out of service.	The MDS message synchronizer has lost connectivity to its duplexed partner. This indicates either a failure of the private network, or a failure of the duplexed partner.	Confirm services are running on peer machine. Check MDS process to determine if it is paired or isolated. Ping test between peers over the private network. Check PGAG and MDS for TOS (Test Other Side) messages indicating the private network has failed and MDS is testing the health of the peer over the public network.

1040023*	Clear	Informational	MDS SYNCH CONNECT TIMEOUT	Communication with peer Synchronizer established.	The MDS message synchronizer has established communication with its duplexed partner.	No action is required.
105007D*	Clear	Informational	RTR PERIPHERAL	Peripheral %2 (ID %1) is on-line.	The specified peripheral is on-line to the ICM. Call and agent state information is being received by the CallRouter for this site.	No action is required.
105007E*	Raise	Error	RTR PERIPHERAL	ACD/IVR %2 (ID %1) is off-line and not visible to the Peripheral Gateway. Routing to this site is impacted.	The specified ACD/IVR is not visible to the Peripheral Gateway. No call or agent state information is being received by the CallRouter from this site. Routing to this site is impacted.	ACD/IVR Vendor should be contacted for resolution. If Peripheral Gateway is also offline per messaging (message ID 10500D1) or rttest then proceed with troubleshooting for Peripheral Gateway off-line alarm first.
10500D0*	Clear	Informational	RTR PHYSICAL CONTROLLER	Physical controller %2 (ID %1) is on-line.	The Router is reporting that physical controller %2 is on-line.	No action is required.
10500D1*	Raise	Error	RTR PHYSICAL CONTROLLER	Peripheral Gateway %2 (ID %1) is not connected to the Central Controller or is out of service. Routing to this site is impacted.	The specified Peripheral Gateway is not connected to the Central Controller. It could be down. Possibly it has been taken out of service. Routing to this site is impacted.	Communication (network) between the Central Controller (Router) and the PG should be checked using 'ping' and 'tracert'. Must have visible and visible high priority connection from PG to Route. CCAG process on Router and PGAG process on PG should be checked. PG may have been taken out of service for maintenance.
10500D2*	Clear	Informational	RTR PERIPHERAL	PG has reported that peripheral %2 (ID %1) is operational.	PG has reported that peripheral %2 (ID %1) is operational.	No action is required.
10500D3*	Raise	Error	RTR PERIPHERAL	PG has reported that peripheral %2 (ID %1) is not operational.	This may indicate that the peripheral is off-line for maintenance or that the physical interface between the peripheral and the PG is not functioning.	Check that the peripheral is not itself off-line and that the connection from the peripheral to the PG is intact.
10500FF*	Clear	Informational	RTR PTOCESS OK	Side %1 %2 process is OK.	The Router is reporting that side %1 process %2 is OK.	No action is required.

1050100*	Raise	Error	RTR PROCESS OK	Process %2 at the Central Site side %1 is down.	The specified process at the central controller site is down. The central controller side is indicated. Attempts will be made to automatically restart the process.	This alarm only occurs for Central Controller (Router and Logger) processes. If the process for BOTH sides is down there is a total failure for that process. Critical processes include: - 'mds' - Router - Message Delivery Service coordinates messaging between duplexed Routers AND Loggers. When this process is down the Central Controller is down and no routing logic is occurring via ICM. - 'rtr' - Router - call routing intelligence. - 'clgr / hlgr' - Logger - configuration / historical data processing to configuration database. - 'rts' - Router - Real Time Server data feed from the router to the Admin Workstations of reporting. - 'rcv' - Logger Recovery - the process that keeps the redundant historical databases synchronized between duplexed loggers.
10501F1*	Clear	Informational	RTR NODE	ICM Node %2 (ID %1) is on-line.	The specified node is on-line to the ICM.	No action is required.
10501F2*	Raise	Error	RTR NODE	ICM Node %2 (ID %1) is off-line.	The specified node is not visible to the ICM. Distribution of real time data may be impacted.	No action is required.

Recommendations on Monitoring Important Cisco Unified Contact Center Device Components with Operations Manager

Recommendations on Performance Monitoring

We recommend that you generate daily graphs and seven-day reports for trend analysis. A seven-day report establishes a baseline for the system.

To generate a daily graph, go to the Service Level View and select the **Performance** right-click option on the device, then select the appropriate metric and time that you want to view. Operations Manager can give you a real-time graph over the past 72 hours.

You can generate a seven-day (or longer) report using Cisco Unified Service Statistics Manager.

As part of the Cisco Unified Communications Management Suite, Cisco Unified Service Statistics Manager extracts the data from Operations Manager and provides advanced statistics analysis and reporting capabilities for Cisco Unified Communications deployments.

The performance data is also stored as comma-separated value (CSV) files for a period of 72 hours, in the following location: C:\Program Files\CSCOpx\data\gsu_#GSUdata#_. If you want data for a period of more than 72 hours, you must manually copy the CSV files to another location.

CPU Usage

View the performance report or graphs for Total CPU Usage (Percentage) on a Cisco Unified Contact Center device by selecting the **Performance** right-click option on the device from the Service Level View. The Maximum and Average data provides trending information.

You can also view each processor's CPU utilization in 5-minute increments by selecting the **Detailed Device View** right-click option on the device from the Service Level View.

Memory Usage

View the performance report or graphs for Memory Usage (Percentage) on a Cisco Unified Contact Center device by selecting the **Performance** right-click option on the device from the Service Level View. Minimum and average values are used for establishing system growth needs. Maximum free memory values are used to detect memory leaks.

Calls Active

This value represents the number of streaming connections that are currently active (in use); in other words, the number of calls that actually have a voice path connected.

Calls in setup mode or in teardown mode are not reported by this count.

View the performance report or graphs for Active Calls (Number) on a Cisco Unified Contact Center Router by selecting the **Performance** right-click option from the Service Level View.

The minimum and maximum of this value can also be collected over time for capacity planning purposes.

Real-time graphing of this parameter, compared with expected values based on historical data, is useful in detecting subtle system performance degradation (generally by detecting that the real-time number of calls active is below expected values compared to the same time-of day/day-of-week baseline values).

To view related counters, go to **Detailed Device View > Cisco IPCC Router Usage**.

Inbound Calls per sec

This value represents the total number of calls received per second. Collection of this data over time can be used to analyze traffic load.

View the performance report or graphs for Inbound Calls per sec on a Cisco Unified Contact Center router by selecting the **Performance** right-click option from the Service Level View.

To view related counters, go to **Detailed Device View > Cisco IPCC Router Usage**.

Agents Logged On

This value represents the total number of agents logged on to the router. This counter, along with the previously mentioned performance counters, helps you analyze the system load.

View the performance report or graphs for Agents Logged On on a Cisco Unified Contact Center Router by selecting the **Performance** right-click option from the Service Level View.

To view related counters, go to **Detailed Device View > Cisco IPCC Router Usage**.

Recommendations on Events for Notification Services

The following are the most important Cisco Unified Contact Center Enterprise-related events, for which you can set up email, e-page, or SNMP trap notification. See Table 2 for the corresponding recommended actions.

Caution: The following recommendations for critical items to be monitored are deployment specific and should be customized for individual customers. Based on bandwidth availability, if you have especially slow-speed WAN links, you might need to adjust the polling intervals. Thresholds may need to be adjusted based on your baseline data.

Events Associated with CPU

HighUtilization

This event indicates that current utilization exceeds the utilization threshold configured for this network adapter or processor.

Events Associated with Memory

InsufficientFreeMemory

This event occurs when the percentage of available free memory resources is lower than the configured value. This event indicates that available free memory resources are running low.

Events Associated with High Temperature

TemperatureSensorDown

This event indicates that the server temperature is outside of the normal operating range, and the system will be shut down.

TemperatureHigh

This event is generated if a temperature sensor's current temperature is higher than the threshold.

Events Associated with Power Supply

PowerSupplyDown

This event is generated if the power supply is down.

Events Associated with Fan

FanDown

This event is generated if the primary fan is down.

Critical Service-Associated Events

ServiceDown

This event is generated when one of the critical services (any of the services in the Detailed Device View) is currently not running. This could be due to someone manually stopping the service. If you intend to stop a service for a long period of time, we highly recommend disabling monitoring for the service to avoid this alert.

Dual-State Notification

This event is generated when the Unified Contact Center logger detects and raises faults on Unified Contact Center components, such as the router and peripheral gateway, and their critical processes. The event description contains the details of the component and its associated process (if it is process related). Once the fault is rectified on the system (manually or automatically), the logger generates a Clear state event. Cisco Unified Operations Manager captures and automatically clears the event's associated Raise state events.

Single-State Notification

This event is generated when the Unified Contact Center logger detects and raises faults on Unified Contact Center components, such as the router and peripheral gateway, and their critical processes. The event description contains the details of the component and its associated process (if it is process related). The single-state Raise state indicates that a health-affecting error has occurred and that a subsequent Clear state notification will not be forthcoming. An example of a single-state Raise condition is an application configuration error that requires the system to be stopped and the problem resolved by an administrator before the affected component will function properly.

Reports

Events Report

We recommend that the administrator generate daily and weekly reports, described in this section, for trend analysis.

To store or receive reports from email, select **Reports > Alert and Event History > Export**, select **All events for the last 24 hours** and **All events for the last 24 hours**, select the file format, and enter the location or email address (or both). CSV file format allows you to quickly sort the events based on event name or device name, and to identify past outages and top issues in the network.

Device Inventory Report

The Device Inventory Report provides a detailed device inventory. To generate this report, select **Detailed Device View** from the list shown in Figure 3: List of Context-Sensitive Tools.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-543550-00 07/09