Cisco CallManager Serviceability System Guide

Release 5.0(1)

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7475-01

Cisco CallManager Serviceability System Guide

CONTENTS

Preface

This preface describes the purpose, audience, organization, and conventions of this guide, and provides information on how to obtain related documentation.

Note This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at this URL:

http://www.cisco.com/univercd/home/home.htm

The preface covers these topics:

Purpose

The *Cisco CallManager Serviceability System Guide* provides information about the Cisco CallManager Serviceability program, including the Real-Time Monitoring Tool (RTMT).

Use this book with the *Cisco CallManager System Guide*, the *Cisco CallManager Administration Guide,* the *Cisco CallManager Serviceability Administration Guide*, and the *CDR Analysis and Reporting Administration Guide*. All documents provide instructions for administering the Cisco CallManager program and include descriptions of procedural tasks that you complete using Cisco CallManager Administration.

Audience

The *Cisco CallManager Serviceability System Guide* provides information for network administrators responsible for managing and supporting the Cisco CallManager system. Network engineers, system administrators, or telecom engineers use this guide to learn about, and administer, remote serviceability features. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table shows how this guide is organized:

Chapter	Description
Chapter 1, "Introduction"	Provides an overview of the Cisco CallManager Serviceability program, remote serviceability programs, and reporting tools.
Chapter 2, "Service Management"	Provides a brief description of the Cisco CallManager services such as Cisco TFTP, Cisco CTIManager, and Cisco RIS Data Collector as well as an overview of the procedures for activating/deactivating and starting/stopping services.
Chapter 3, "Alarms"	Provides an overview of alarms and alarm definitions.
Chapter 4, "Trace"	Provides an overview and the procedures for configuring trace parameters and trace collection.
Chapter 5, "Real-Time Monitoring Tool"	Provides an overview of performance and device monitoring and alert notification.
Chapter 6, "Performance Objects and Counters"	Provides a complete list of performance objects and their associated counters. Provides tables with related information about Cisco CallManager perfmon counters, the Real-Time Monitoring Tool, and CCM_SNMP_MIB.
Chapter 7, "Alerts"	Provides an overview of alerts, including a description of preconfigured alerts. Describes fields that you use to configure alerts and alert actions. Provides a list of attributes of alert logs.
Chapter 8, "Log Partition Monitoring"	Provides information about Log Partition Monitoring to monitor the disk usage of the log partition on a server (or all servers in the cluster).
Chapter 9, "Serviceability Reports Archive"	Provides an overview on the reports generated by the Cisco Serviceability Reporter service
Chapter 10, "Simple Network Management Protocol"	Provides an overview of Cisco CallManager support of SNMP versions 1, 2c, and 3. Administrators use SNMP to troubleshoot and to perform diagnostics and network management tasks.

Related Documentation

Refer to the *Cisco CallManager Documentation Guide* for further information about related Cisco IP telephony applications and products. The following URL shows an example of the path to the documentation guide:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/<release #>/doc_gd/index.htm

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
——►	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means *the information contains useful tips.*

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

PART 1

Understanding Serviceability

Introduction

This chapter contains information on the following topics:

Cisco CallManager Serviceability Overview

Cisco CallManager Serviceability, a web-based troubleshooting tool for Cisco CallManager, provides the following functionality:

- Saves Cisco CallManager services alarms and events for troubleshooting and provides alarm message definitions.
- Saves Cisco CallManager services trace information to various log files for troubleshooting. Administrators can configure trace in Cisco CallManager Serviceability and collect and view trace information in the Cisco CallManager real-time monitoring tool.
- Provides feature services that you can activate and deactivate in the Service Activation window.
- Provides an interface for starting and stopping feature and network services.
- Provides an interface for viewing status for feature and network services.
- Generates reports for CDR Analysis and Reporting (CAR) and Real-Time Monitoring Tool (RTMT).
- Provides CDROnDemand, which allows you to retrieve the CDR/CMR files from Cisco CallManager.
- Allows Cisco CallManager to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a server (or all servers in the cluster)

Reporting Tools

Cisco CallManager Serviceability provides the following reporting tools:

- Cisco CDR Analysis and Reporting—Generates reports for Quality of Service, traffic, and billing information through Cisco CDR Analysis and Reporting. For more information, see the *CDR Analysis and Reporting Administration Guide*.
- Cisco CallManager Real-Time Monitoring Tool (RTMT)—Monitors real-time behavior of the components in a Cisco CallManager cluster through the real-time monitoring tool (RTMT); creates daily reports that you can access through the Serviceability Reports Archive.
- Serviceability Reports Archive—Archives reports that Cisco CallManager Serviceability generates.
- Cisco Dialed Number Analyzer—Allows you to test and diagnose a deployed Cisco CallManager dial plan configuration, analyze the test results and use the results to tune the dial plan. For more information on how to access and use the Dialed Number Analyzer, see the *Cisco Dialed Number Analyzer Guide*.

Remote Serviceability Tools

To supplement the management and administration of the Cisco CallManager system, you can use remote serviceability tools. Using these tools, you can gather system and debug information for diagnostic help or remote troubleshooting. The tools can process and report on a collection of local or remote Cisco CallManager configuration information.

With customer permission, technical support engineers log on to a Cisco CallManager server and get a desktop or shell that allows them to perform any function that could be done from a local logon session.

Cisco CallManager supports the following capabilities for remote serviceability:

- Simple Network Management Protocol (SNMP)—Provides remote management for managed devices such as Cisco CallManager
- Show Command Line Interface—Displays Cisco CallManager system data.
- CiscoWorks2000—Purchased separately from Cisco CallManager, supports maintenance of Cisco networks and devices. The following features, which serve as examples only, show how you can use CiscoWorks2000 to manage Cisco CallManager operations:

  Path Analysis defines Cisco CallManager system paths in the form of maps, trace logs, or discovery tables. Path Analysis, which traces connectivity between two specified points in your network, requires that you enable CDR logging in Cisco CallManager Administration.

  Syslog Analysis tools monitor and manage a wide range of events and error messages concurrently on each Cisco CallManager server and other Cisco devices at your site.

  Cisco Discovery Protocol (CDP) enables discovery of Cisco CallManager servers and management of those servers by CiscoWorks2000. After you use the CDP cache MIB of the direct neighboring device to discover the Cisco CallManager, you can use CiscoWorks2000 to query other Cisco CallManager-supported MIBs for provisions or statistics information about topology services, user tracking, path analysis, and other network management services. When you use CiscoWorks2000, you must keep the CDP driver enabled at all times to discover Cisco CallManager.

Browser Support

Cisco supports the following browsers with Cisco CallManager Serviceability:

- Internet Explorer 6.0 (or later)
- Netscape 7.1 (or later)

To access Cisco CallManager Serviceability, you must browse to the application from a machine that runs the supported browser.

Note Cisco CDR Analysis and Reporting (CAR) does not support Netscape 7.0 (or later). To access the application, use Internet Explorer 5.5 (or later).

Cisco CallManager Serviceability uses HTTPS to establish secure connections.

Where to Find More Information

Additional Cisco Documentation

- *CDR Analysis and Reporting Administration Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Dialed Number Analyzer Guide*
- CiscoWorks2000 user documentation

  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm

Service Management

Cisco CallManager Serviceability service management includes working with feature and network services and servlets, which are associated with the Tomcat Java Webserver. Feature services allow you to use Cisco CallManager-related features, while network services are required for your system to function.

If something is wrong with a service or servlet, an alarm gets written to an alarm monitor. After viewing the alarm information, you can run a trace on the service. Be aware that services and servlets display different trace levels in the Trace Configuration window.

This chapter, which provides a description of services/servlets, Service Activation, and Control Center, contains information on the following topics:

Feature Services

After a Cisco CallManager installation, the system does not automatically activate feature services, which are Cisco CallManager-related services that are required to use Cisco CallManager features. In Cisco CallManager Serviceability, you can activate, start, and stop feature services. After you activate feature services, you can modify associated service parameters in Cisco CallManager Administration. If you are upgrading Cisco CallManager, those services that you activated on the system prior to the upgrade automatically activate and start after the upgrade.

Activation turns on and starts the service. After you activate a service in the Service Activation window, you do not need to start it in the Control Center—Feature Services window. If the service does not start for any reason, you must start it in the Control Center—Features Services window.

In the Service Activation window, Cisco CallManager Serviceability categorizes feature services into the following groups:

- Database and Admin Services, page 2-5
- Performance and Monitoring Services, page 2-5
- Security Services, page 2-6
- Directory Services, page 2-6
- Backup and Restore Services, page 2-6

In the Control Center—Feature Services window, Cisco CallManager Serviceability categorizes services into the same groups that display in the Service Activation window.

Tip For service activation recommendations, see the "Service Activation" section on page 2-12 and the "Activating and Deactivating Feature Services" in the *Cisco CallManager Serviceability Administration Guide*.

CM Services

Cisco CallManager

The Cisco CallManager service provides software-only call processing as well as signaling and call control functionality.

Tip Before you activate this service, verify that the Cisco CallManager displays in the Cisco CallManager Find/List window in Cisco CallManager Administration. If the server does not display, add the Cisco CallManager before you activate this service. For information on how to add the Cisco CallManager, refer to the *Cisco CallManager Administration Guide*.

Tip If you deactivate the Cisco CallManager or CTIManager services in Service Activation, the Cisco CallManager where you deactivated the service no longer exists in the database. This means that you cannot choose the Cisco CallManager for configuration operations in Cisco CallManager Administration because it will not display in the graphical user interface (GUI). If you then reactivate the services on the same Cisco CallManager, the database creates the Cisco CallManager again and adds a "CM_" prefix to the server name or IP address; for example, if you reactivate the Cisco CallManager or CTIManager service on a server with an IP address of 172.19.140.180, then CM_172.19.140.180 displays in Cisco CallManager Administration. You can now choose the Cisco CallManager, with the new "CM_" prefix, in Cisco CallManager Administration.

The following services rely on Cisco CallManager service activation:

- Cisco CTIManager, page 2-3
- CDR Services, page 2-4

Cisco TFTP

Cisco Trivial File Transfer Protocol (TFTP) builds and serves files consistent with the trivial file transfer protocol, a simplified version of FTP. Cisco TFTP serves embedded component executable, ringer files, and device configuration files.

A configuration file includes a list of Cisco CallManagers to which devices (telephones and gateways) make connections. When a device boots, the component queries a Dynamic Host Configuration Protocol (DHCP) server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. The device requests a configuration file from the TFTP server. The configuration file contains a list of Cisco CallManagers and the TCP port through which the device connects to those Cisco CallManagers.

Cisco IP Voice Media Streaming App

The Cisco IP Voice Media Streaming Application service provides voice media streaming functionality for the Cisco CallManager for use with MTP, conferencing, music on hold (MOH), and annunciator. The Cisco IP Voice Media Streaming Application relays messages from the Cisco CallManager to the IP voice media streaming driver, which handles RTP streaming.

Cisco Messaging Interface

The Cisco Messaging Interface allows you to connect a simplified message desk interface (SMDI)-compliant external voice-messaging system with the Cisco CallManager. The CMI service provides the communication between the voice-messaging system and Cisco CallManager. The SMDI defines a way for a phone system to provide a voice-messaging system with the information that is needed to intelligently process incoming calls.

Cisco CTIManager

The CTI Manager contains the CTI components that interface with applications. With CTI Manager, applications can access resources and functionality of all Cisco CallManagers in the cluster and have improved failover capability. One or more CTI Managers can be active in a cluster, but only one CTI Manager can exist on an individual server. An application (JTAPI/TAPI) can have simultaneous connections to multiple CTI Managers; however, an application can only use one connection at a time to open a device with media termination.

Cisco CallManager Attendant Console Server

The Cisco CallManager Attendant Console Server service provides centralized services for Cisco WebAttendant and Attendant Console clients and pilot points. For Cisco WebAttendant and Attendant Console clients, this service provides call-control functionality, line state information for any accessible line within the Cisco CallManager domain, and caching of directory information. For pilot points, this service provides automatic redirection to directory numbers that are listed in hunt groups and failover during a Cisco CallManager failure.

Cisco Extended Functions

The Cisco Extended Functions service provides support for some Cisco CallManager features, including Quality Report Tool (QRT). For more information about individual features, refer to the *Cisco CallManager System Guide* and the *Cisco IP Phone Administration Guide for Cisco CallManager.*

Cisco CallManager Cisco IP Phone Services

When activated, the Cisco CallManager Cisco IP Phone Service initializes the service URLs for the Cisco IP Phone services that you configured in Cisco CallManager Administration.

Cisco Dialed Number Analyzer

The Cisco Dialed Number Analyzer service can be activated/deactivated from the serviceability web pages.

When activated, this tool will consume a lot of resources. Cisco does not recommend activating the service on all the nodes in a cluster. Cisco recommends that you activate this service only during off-peak hours or only on one of the nodes of a cluster where call processing activity is the least.

Cisco DHCP Monitor Service

Cisco DHCP Monitor Service monitors IP address changes for IP Phones in the database tables. When a change is detected, it modifies the /etc./dhcpd.conf file and restarts the DHCPD daemon.

CTI Services

Cisco IP Manager Assistant

When activated, Cisco IP Manager Assistant enables managers and their assistants to work together more effectively. Cisco IPMA supports two modes of operation: proxy line support and shared line support. The Cisco IPMA service supports both proxy line and shared line support in a cluster. Refer to the *Cisco CallManager Features and Services Guide*.

The feature comprises a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.

The service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets on the basis of preconfigured call filters. The manager can change the call routing dynamically; for example, by pressing a softkey on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Cisco CallManager users comprise managers and assistants. The routing service intercepts manager calls and routes them appropriately. An assistant user handles calls on behalf of a manager. Cisco IPMA comprises features for managers and features for assistants.

Cisco WebDialer Web Service

Cisco WebDialer provides click-to-dial functionality. It allows users in a Cisco CallManager cluster to initiate a call to other users inside or outside the cluster by using a web page or a desktop application. Cisco WebDialer provides a web page that enables users to call each other within a cluster. Cisco WebDialer comprises two components: WebDialer servlet and Redirector servlet.

The Redirector servlet provides the ability for third-party applications to use Cisco WebDialer. The Redirector servlet finds the appropriate Cisco CallManager cluster for the WebDialer user and redirects the request to the WebDialer in that cluster. The Redirector functionality only applies for HTTP/HTML-based WebDialer client applications because it is not available for Simple Object Access Protocol (SOAP)-based WebDialer applications.

CDR Services

Cisco CAR Scheduler

The Cisco CAR Scheduler service allows you to schedule CAR-related tasks; for example, you can schedule report generation or CDR file loading into the CAR database.

For this service to work, activate the Cisco CallManager service on the first node and ensure that it is running.

Cisco CAR Web Service

The Cisco CAR Web Service loads the user interface for CAR, a web-based reporting application that generates either csv or pdf reports by using CDR data.

For this service to work, activate the Cisco CallManager service on the first node and ensure that it is running.

Database and Admin Services

Cisco AXL Web Service

The Cisco AXL Web Service allows you to modify Cisco CallManager database entries and execute stored procedures from AVVID client-based applications that use AXL.

Cisco Bulk Provisioning Service

Cisco Bulk Provisioning Service can only be activated on the first node. If you use the Bulk Administration Tool (BAT) to administer phones and users, you must activate this service.

Performance and Monitoring Services

Cisco Serviceability Reporter

The Cisco Serviceability Reporter service generates the following daily reports:

- Device Statistics
- Server Statistics
- Service Statistics
- Call Activities
- Alert
- Performance Protection Report

This service gets installed on all the Cisco CallManager nodes in the cluster. Reporter generates reports once a day based on logged information. You can access the reports that Reporter generates in Cisco CallManager Serviceability from the Tools menu.

Each summary report comprises different charts that display the statistics for that particular report.

Cisco Serviceability Reporter comprises two service parameters:

- Report Generation Time—Number of minutes after midnight. Reports generate at this time for the last day.
- Report Deletion Age—Number of days that the report must be kept in the disk. The system deletes the reports that are older than the specified age.

.Cisco CCM SNMP Service

This service provides SNMP access to provisioning and statistics information that is available for Cisco CallManager.

Security Services

Cisco CTL Provider

The Cisco CTL Provider service, which runs with local system account privileges, works with the Cisco CTL Provider Utility, a client-side plug-in, to change the security mode for the cluster from nonsecure to mixed mode. When you install the plug-in, the Cisco CTL Provider service retrieves a list of all Cisco CallManager and Cisco TFTP servers in the cluster for the CTL file, which contains a list of security tokens and servers in the cluster.

After you activate the service, the Cisco CTL Provider service reverts to the default CTL port, which is 2444. If you want to change the port, refer to the Cisco CallManager security documentation for more information. You must install and configure the Cisco CTL Client and activate this service for the clusterwide security mode to change from nonsecure to secure.

Cisco Certificate Authority Proxy Function (CAPF)

Working in conjunction with the CAPF application, the Cisco Certificate Authority Proxy Function (CAPF) service can perform the following tasks, depending on your configuration:

- Issue locally significant certificates to supported Cisco IP Phone models.
- Using SCEP, request certificates from third-party certificate authorities on behalf of supported Cisco IP Phone models.
- Upgrade existing certificates on the phones.
- Retrieve phone certificates for troubleshooting.
- Delete locally significant certificates on the phone.

Note When you view real-time information in RTMT, the Cisco Certificate Authority Proxy Function (CAPF) service displays only for the first node.

Directory Services

Cisco DirSync

Unlike Windows versions of Cisco CallManager, Cisco CallManager 5.0 does not contain an embedded directory. Because of this change, the Cisco CallManager database stores all user information. If you use an integrated corporate directory, for example, Microsoft Active Directory or Netscape/iPlanet Directory, with Cisco CallManager, the Cisco DirSync service migrates the user data to the Cisco CallManager database. The Cisco DirSync service does not synchronize the passwords from the corporate directory.

Backup and Restore Services

Cisco DRF Master

The Cisco DRF Master Agent service supports the DRF Master Agent, which works with the graphical user interface (GUI) or command line interface (CLI) to schedule backups, perform restores, view dependencies, check status of jobs, and cancel jobs, if necessary. The Cisco DRF Master Agent also provides the storage medium for the backup and restoration process (tape drive in Cisco CallManager 5.0).

Network Services

Installed automatically with Cisco CallManager, network services include services that the Cisco CallManager system requires for the cluster to function; for example, database and platform services. Because these services are required for basic Cisco CallManager functionality, you cannot activate them in the Service Activation window. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a network service in the Call Control—Network Services window.

After the Cisco CallManager installation, network services start automatically, as noted in the Call Control—Network Services window.

In the Control Center—Network Services window, Cisco CallManager Serviceability categorizes services into the following groups:

Platform Services

A Cisco DB

A Cisco DB is the Progres database engine.

Cisco Tomcat

The Cisco Tomcat service supports the web server in Cisco CallManager 5.0.

SNMP Master Agent

This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.

MIB2 Agent

This service provides SNMP access to variables that are defined in RFC 1213, which read and write variables; for example, system, interfaces, IP, and so on.

Host Resources Agent

This service provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base.

Native Agent Adaptor

This service allows you to forward SNMP requests to another SNMP agent that runs on the system.

System Application Agent

This service provides SNMP access to the applications that are installed and executing on the system. This implements the SYSAPPL-MIB.

Cisco CDP Agent

This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco CallManager node.

Cisco Syslog Agent

This service supports gathering of syslog messages that various Cisco CallManager components generate.

Cisco Electronic Notification

This service works with the Cisco IPT Platform Administration, so you can send e-mails about software updates.

Cisco License Manager

Cisco License Manager keeps track of the licenses that are purchased and used by the customer. It controls licenses checkins and checkouts and it is responsible for issuing and reclaiming licenses. Cisco License Manager manages the Cisco CallManager application and the number of IP Phone unit licenses. When the number of phones exceeds the number of licenses, it issues alarms to notify the administrator. This service runs on all the nodes, but the service on the first node is responsible for issuing and reclaiming licenses.

Cisco Certificate Expiry Monitor

This service periodically checks the expiration status of certificates that are generated by Cisco CallManager and sends notification when a certificate is close to its expiration date.

DB Services

Cisco Database Layer Monitor

The Cisco Database Layer Monitor service monitors aspects of the database layer. This server is responsible for change notification and monitoring.

CM Services

Cisco CallManager Admin

The Cisco CallManager Admin service supports Cisco CallManager Administration, the web application/interface that you use to configure Cisco CallManager settings. After the Cisco CallManager installation, this service starts automatically and allows you access to the web pages. If you stop this service on a server, you cannot access the Cisco CallManager Administration graphical user interface when you browse into that server.

Cisco CallManager Serviceability

The Cisco CallManager Serviceability service supports Cisco CallManager Serviceability, the web application/interface that you use to troubleshoot Cisco CallManager issues. After the Cisco CallManager installation, this service starts automatically and allows you access to the web pages. If you stop this service on a server, you cannot access the Cisco CallManager Serviceability GUI when you browse into that server.

Cisco CallManager Personal Directory

The Cisco CallManager Personal Directory service supports Cisco Personal Directory.

Cisco Log Partition Monitoring Tool

The Cisco Log Partition Monitoring Tool service supports the Log Partition Monitoring feature, which monitors the disk usage of the log partition on a server (or all servers in the cluster) by using configured thresholds and a polling interval.

Cisco CDP

Cisco CDP advertises Cisco CallManager to other applications, so the application, for example, SNMP or CiscoWorks2000, can perform network management tasks for Cisco CallManager.

Cisco Trace Collection Servlet

The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using the RTMT client. After Cisco CallManager installation, this service starts automatically. If you stop this service on a server, you cannot collect or view traces on that server.

Cisco Trace Collection Service

The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client. After Cisco CallManager installation, this service starts automatically. If you stop this service on a server, you cannot collect or view traces on that server.

Tip If necessary, Cisco recommends that you restart the Cisco Trace Collection Service before restarting Cisco Trace Collection Servlet to reduce the initialization time.

Cisco RIS Data Collector

The Real-time Information Server (RIS) maintains real-time Cisco CallManager information such as device registration status, performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as Real-Time Monitoring Tool (RTMT), SOAP applications, Cisco CallManager Administration and AlertMgrCollector (AMC) to retrieve the information that is stored in all RIS nodes in the cluster.

Cisco AMC Service

Used for the real-time monitoring tool (RTMT), this service, Alert Manager and Collector service, existed as a component of the Cisco RIS Data Collector service in previous Windows releases of Cisco CallManager. This service allows RTMT to retrieve real-time information that exists on nodes in the cluster

Cisco Extension Mobility Application

The Cisco Extension Mobility service allows you to define login settings such as duration limits on phone configuration for the Cisco CallManager Extension Mobility feature. The Cisco CallManager Extension Mobility feature allows users within a Cisco CallManager cluster to temporarily configure any Cisco IP Phone 7960/7940 in the cluster as their own phone by logging in to that phone. After a user logs in, the phone adopts the user's personal phone number(s), speed dials, services links, and other user-specific properties. After logout, the phone adopts the original user profile.

Performance and Monitoring Services

Cisco CallManager Serviceability RTMT

The Cisco CallManager Serviceability RTMT service supports the Cisco CallManager Real-Time Monitoring Tool (RTMT), which allows you to collect and view traces, view performance monitoring objects, work with alerts, and monitor devices, system performance, CTI applications, and so on.

Cisco RTMT Reporter Servlet

The Cisco RTMT Reporter servlet allows you to publish reports for RTMT

Cisco Tomcat Stats Servlet.

The Cisco Tomcat Stats Servlet allows you to monitor the Tomcat perfmon counters by using RTMT or the Command Line Interface. Do not stop this service unless you suspect that this service is using too many resources, such as CPU time.

SOAP Services

Cisco SOAP-Real-Time Service APIs

The Cisco SOAP-Real-Time Service APIs allows you to collect real-time information for devices and CTI applications. This service also provides APIs for activating, starting, and stopping services.

Cisco SOAP Performance Monitoring APIs

The Cisco SOAP Performance Monitoring APIs service allows you to use performance monitoring counters for various applications through SOAP APIs; for example, you can monitor memory information per service, CPU usage, Cisco Callmanager counters, and so on.

Cisco SOAP-Log Collection APIs

The Cisco SOAP-Log Collection APIs service allows you to collect log files and to schedule collection of log files on a remote SFTP server. Examples of log files that you can collect include syslog, core dump files, Cisco application trace files, and so on.

Backup and Restore Services

Cisco DRF Local

The Cisco DRF Local service supports the Cisco DRF Local Agent, which acts as the workhorse for the DRF Master Agent. Components on a node register with the Cisco DRF Local Agent to use the disaster recovery framework. The Cisco DRF Local Agent executes commands that it receives from the Cisco DRF Master Agent. Cisco DRF Local Agent sends the status, logs, and command results to the Cisco DRF Master Agent.

CDR Services

Cisco CDR Repository Manager

You can activate the Cisco CDR Repository Manager service only on the first node, which contains the Cisco CallManager database. This service starts automatically.

Cisco CDR Agent

The Cisco CDR Agent service transfers CDR and CMR files that are generated by Cisco CallManager from the local host to the CDR repository node, where the CDR Repository Manager service runs over a SFTP connection.

For this service to work, activate the Cisco CallManager service on the first node and ensure that it is running.

Service Activation

You can activate or deactivate multiple feature services or choose default services to activate from the Service Activation window in Cisco CallManager Serviceability. Cisco CallManager Serviceability activates feature services in automatic mode and checks for service dependencies based on a single-server configuration. When you choose to activate a feature service, Cisco CallManager Serviceability prompts you to select all the other services, if any, that depend on that service to run based on a single-server configuration. When you click the Set Default button, the Cisco CallManager Serviceability chooses those services that are required to run Cisco CallManager based on a single-server configuration. Activating a service automatically starts the service. You start/stop services from Control Center.

Control Center

From Control Center in Cisco CallManager Serviceability, you can view status and start and stop one service at a time for a particular server in the cluster. To perform these tasks, Cisco CallManager Serviceability provides two Control Center windows. To start, stop, and restart network services, access the Control Center—Network Services window. To start, stop, and restart feature services, access the Control Center—Feature Services window.

Tip Use the Related Links drop-down list box and the Go button to navigate to Control Center and Service Activation windows.

Starting and stopping a Cisco CallManager (feature) service causes all Cisco IP Phones and gateways that are currently registered to that Cisco CallManager service to fail over to their secondary Cisco CallManager service. Devices and phones need to restart only if they cannot register with another Cisco CallManager service. Starting and stopping a Cisco CallManager service causes other installed applications (such as Conference Bridge or Cisco Messaging Interface) that are homed to that Cisco CallManager to start and stop as well.

Caution Stopping a Cisco CallManager service also stops call processing for all devices that the service controls. When a Cisco CallManager service is stopped, calls from an IP phone to another IP phone will stay up; calls in progress from an IP phone to a Media Gateway Control Protocol (MGCP) gateway also stay up, but other types of calls drop.

Services Configuration Checklist

Table 2-1 lists the steps for installing and configuring services.

Table 2-1 Services Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Activate the feature services that you want to run on your Cisco CallManager servers. **Note** If you are upgrading from a previous version of Cisco CallManager, Cisco CallManager Serviceability automatically activates and starts the services that were started before you began the upgrade.	• Feature Services, page 2-1 • Activating and Deactivating Feature Services, *Cisco CallManager Serviceability Administration Guide*
Step 2	Configure the appropriate service parameters.	• *Cisco CallManager Administration Guide* • i-button help in Service Parameter window in Cisco CallManager Administration
Step 3	Troubleshoot problems by using the Cisco CallManager Serviceability trace tools, if needed.	• Trace Configuration, *Cisco CallManager Serviceability Administration Guide* • Trace Collection and Log Central in RTMT, *Cisco CallManager Serviceability Administration Guide*

Where to Find More Information

Related Topics

- Control Center, page 2-12
- Feature Services, page 2-1
- Network Services, page 2-7

Additional Cisco Documentation

- *Cisco CallManager System Guide*
- *Cisco CallManager Administration Guide*
- Cisco CallManager Features and Services Guide
- Cisco CallManager Security Guide
- *Troubleshooting Guide for Cisco CallManager*

PART 2

Monitoring Tools

Alarms

This chapter provides information on Serviceability Alarms and contains the following topics:

Understanding Alarms

Cisco CallManager Serviceability Alarms allows you to configure alarms and events and provides alarm message definitions. Both functions assist the system administrator and support personnel in troubleshooting Cisco CallManager problems.

You use alarms to provide run-time status and state of the Cisco CallManager system and to take corrective action for problem resolution; for example, to determine whether phones are registered and working. Alarms contain information such as explanation and recommended action. Alarm information includes application name, machine name, and cluster name to help you perform troubleshooting, even for problems that are not on your local Cisco CallManager.

You configure the alarm interface to send alarm information to multiple destinations, and each destination can have its own alarm event level (from debug to emergency). You can direct alarms to the Syslog Viewer (local syslog), Syslog file (remote syslog), an SDI trace log file, an SDL trace log file (for Cisco CallManager and CTIManager only), or to all destinations. When a service issues an alarm, the alarm interface sends the alarm to the chosen monitors (for example, SDI trace). The monitor forwards the alarm or writes it to its final destination (such as a log file).

You use the trace and log central option in the Real-Time Monitoring Tool (RTMT) to collect alarms that are sent to an SDI or SDL trace log file. You use the SysLog Viewer in the real-time monitoring tool to view alarms that are sent to the local syslog.

The alarm definitions describe alarm messages: what they mean and how to recover from them. You search the Alarm Definitions window for alarm information. When you click on any service-specific alarm, a description of the alarm information (including any user-defined text that you have added) and a recommended action display.

Alarm Configuration

You configure alarm information that will be used for trace and troubleshooting. You can configure alarms for services, such as Cisco CallManager and Cisco CTIManager, on a particular server, or you configure alarms for a particular service on all servers in the cluster.

You choose an alarm event level, such as Error, and a destination(s), such as Syslog Viewer (local syslog), for the alarms for an individual service and the monitor destination. Choosing an event level accomplishes two tasks: helps the administrator narrow the types of alarms that Cisco CallManager collects and prevents the Syslog and trace files from becoming overloaded.

Alarm Definitions

Cisco CallManager stores alarm definitions and recommended actions in a standard query language (SQL) server database. The system administrator can search the database for definitions of all the alarms. The definitions include the alarm name, description, explanation, recommended action, severity, parameters, and monitors. This information aids the administrator in troubleshooting problems that Cisco CallManager encounters.

Serviceability Alarm Definitions allow administrators to add additional explanation or recommendations for an alarm. All administrators have access to the added information. Administrators directly enter information into the User Defined Text box that displays in the Alarm Details window. Standard horizontal and vertical scroll bars support scrolling. Cisco CallManager Serviceability adds the information to the database.

Viewing Alarm Information

You view alarm information to determine whether Cisco CallManager problems exist. The method that you use to view the alarm depends on the destination that you chose when configuring the alarm. You can view alarm information that is sent to the SDI or SDL trace log file by using the trace and log central option in RTMT or by using a text editor. You can view alarm information that is sent to local syslog by using the SysLog Viewer.

Tip You can also use CiscoWorks2000 report viewer to view remote syslog messages.

Alarm Configuration Checklist

Table 3-1 provides an overview of the steps for configuring alarms.

Table 3-1 Alarm Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Choose the server and service for which you want the alarm information.	Understanding Alarms, page 3-1 Configuring or Updating an Alarm for a Service, *Cisco CallManager Serviceability Administration Guide*
Step 2	Choose the destination of the alarm: • All services can go to the SDI log (but must be configured in Trace also). • All services can go to the SysLog Viewer. • If you are using CiscoWorks2000, check the Remote Syslog destination and specify a host name. • Only Cisco CallManager and Cisco CTIManager use the SDL log.	Configuring or Updating an Alarm for a Service, *Cisco CallManager Serviceability Administration Guide* Alarm Destination Settings, *Cisco CallManager Serviceability Administration Guide*
Step 3	Choose the alarm event level.	Configuring or Updating an Alarm for a Service, *Cisco CallManager Serviceability Administration Guide* Alarm Event Level Settings, *Cisco CallManager Serviceability Administration Guide*
Step 4	If desired, add a definition to an alarm.	Alarm Definitions, *Cisco CallManager Serviceability Administration Guide*
Step 5	If you chose an SDI or SDL trace file as the alarm destination, collect traces and view with the trace and log central option of RTMT.	Trace Collection and Log Central in RTMT, *Cisco CallManager Serviceability Administration Guide* Using Local Browse, *Cisco CallManager Serviceability Administration Guide* Using the Query Wizard, *Cisco CallManager Serviceability Administration Guide*
Step 6	If you chose local syslog as the alarm destination, view the alarms in the SysLog Viewer.	Using SysLog Viewer in RTMT, *Cisco CallManager Serviceability Administration Guide*
Step 7	See the corresponding alarm definition for the description and recommended action.	Viewing Alarm Definitions and Adding User-Defined Descriptions, *Cisco CallManager Serviceability Administration Guide*

Where to Find More Information

Related Topics

- Configuring or Updating an Alarm for a Service, page 3-1, *Cisco CallManager Serviceability Administration Guide*
- Viewing Alarm Definitions and Adding User-Defined Descriptions, page 4-1, *Cisco CallManager Serviceability Administration Guide*
- Alarm Definition Catalog Descriptions, page 4-2, *Cisco CallManager Serviceability Administration Guide*
- Trace Collection and Log Central in RTMT, page 10-1, *Cisco CallManager Serviceability Administration Guide*

Trace

This chapter provides information on the Cisco CallManager Serviceability trace tools and contains the following topics:

Understanding Trace

Cisco CallManager Serviceability provides trace tools to assist the system administrator and support personnel in troubleshooting Cisco CallManager problems. Cisco CallManager Serviceability supports SDI (System Diagnostic Interface) trace, SDL (Signaling Distribution Layer) trace, and Log4J trace (for Java applications).

You use the Trace Configuration window to specify the level of information that you want traced as well the type of information that you want to trace to be included in each trace file. If the service is a call-processing application such as Cisco CallManager or Cisco CTIManager, you can configure a trace on devices such as phones and gateway.

You use the Alarm Configuration window to direct various levels of alarms to destinations, including SDI or SDL trace log files.

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the trace and log central option in the Real-Time Monitoring Tool (RTMT).

Trace Configuration

You can configure trace parameters for any Cisco CallManager service that is available on any Cisco CallManager server in the cluster. Use the Trace Configuration window to specify the parameters that you want to trace for troubleshooting Cisco CallManager problems.

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the trace files.) You can configure trace for a single service or apply the trace settings for that service to all servers in the cluster.

If the service is a call-processing application such as Cisco CallManager or Cisco CTIManager, you can configure a trace on devices such as phones and gateways; for example, you can narrow the trace to all enabled phones with a directory number beginning with 555.

If you want to use predetermined troubleshooting trace settings rather than choosing your own trace fields, you can use the Troubleshooting Trace window. For more information on troubleshooting trace, see the "Troubleshooting Trace Setting" section on page 4-2.

After you have configured information that you want to include in the trace files for the various services, you can collect trace files by using the trace and log central option in RTMT. For more information regarding trace collection, see the "Trace Collection" section on page 4-3.

Troubleshooting Trace Setting

The Troubleshooting Trace Setting window allows you to choose the services in Cisco CallManager for which you want to set predetermined troubleshooting trace settings. Using this window, you can choose the required services on different Cisco CallManager nodes in the cluster, so the trace settings of the chosen services get changed to reflect the predetermined trace settings.

Note The predetermined troubleshooting trace settings for a service include SDL, SDI, and Log4j trace settings. The system backs up the trace settings that were originally set before Cisco CallManager applies the troubleshooting trace settings. The original trace settings get restored when you reset the troubleshooting trace settings.

After you apply troubleshooting trace settings to some services, subsequent requests to open the Troubleshooting Trace Setting window display the Troubleshooting Trace Setting window again and show the services that you have set for troubleshooting. You can reset the trace settings to the original settings by choosing the Reset Troubleshooting Traces button.

When you apply Troubleshooting Trace Setting to a service, the Serviceability Trace Configuration window displays a message that states that troubleshooting trace has been set for the given service(s). A link to the Troubleshooting Trace Setting window displays, so you can reset the settings for the service, if necessary.

The Trace Configuration window displays all the settings as read-only, except for some parameters of trace output settings; for example, Maximum No. of Files. You can modify these parameters even when you have applied troubleshooting trace settings.

Trace Collection

Use trace and log central, an option within the real-time monitoring client-side plug-in, to collect, view, and zip various Cisco CallManager service traces and/or other Cisco CallManager log files. With the trace and log central option, you can collect Cisco CallManager SDL/SDI traces, Cisco CallManager Application Logs (such as Bulk Administration Tool logs), System Logs (such as Event View Application, Security, and System logs), and crash dump files.

The trace and log central option provides several methods to collect and view trace files, as described in the following list:

- Remote Browse—After the system has generated trace files, you can view them on the server by using the viewers within the real-time monitoring tool. You can also use the remote browse feature to download the traces to your PC.
- Collect Files—Collects and downloads traces for services, applications, and system logs on one or more servers in the cluster for an absolute date and time range (such as between July 8, 2004 at 12:30 and August 8, 2004 at 12:30) or for a relative time (such as, within the last 30 minutes).
- Query Wizard—Collects trace files for services, applications, and system logs for an absolute or relative time range that contain text strings that you specify. You can view the collected trace file and/or download the trace files to your PC. You can also save the trace collection query criteria for later use. If you save the query as a regular query, you can only run the query on the node on which it was created. If you save the query as a generic query, you can run it on any node in any cluster.
- Schedule Collection—Schedules a recurring trace collection and allows users to perform a specified action, including: run another query, generate a syslog, or download the trace files on a SFTP server.
- Local Browse—After you have collected trace files and downloaded them to your PC, you can view them with a text editor that can handle UNIX variant line terminators such as WordPad on your PC, or you can view them by using the viewers within the real-time monitoring tool.
- Collect Crash Dump—Collects a crash dump file for one or more servers on your network.
- Real Time Trace—Comprises two options: view real-time data and monitor user events. The view real-time data option allows you to view the current trace file that is being written on the server for an application. The monitor user event option enables the system to monitor real-time trace files and perform a specified action when a search string displays in the trace file. Actions include generating an alert, generating local or remote syslogs, or downloading trace files via SFTP.
- Job Status—Allows you to view the status of the trace collection jobs that are running on the system as well as recently processed jobs.

After the system has generated trace files, you can view them on the server by using the remote browse option.

You can collect individual traces files or zip multiple traces into a single file. You can manually delete the collected trace files from the server, or you can set the trace and log central option to delete the trace files from the server after collection.

After you collect the files, you can view them in the Local Browse option. The file displays in the appropriate viewer, such as the QRT Viewer, Q931 Translator, Log Viewer, or Generic Viewer.

Note For devices that support encryption, the SRTP keying material does not display in the trace file.

Trace Configuration and Collection Checklist

Table 4-1 provides an overview of the steps for configuring and collecting trace for Cisco CallManager services.

Table 4-1 Trace Configuration and Collection Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Using Cisco CallManager Administration **System > Enterprise Parameters**, configure the maximum number of devices that are available for tracing. Enter a value in the Max Number of Device Level Trace field. The default specifies 12.	*Cisco CallManager Administration Guide*
Step 2	Configure the trace setting for the service for which you want to collect traces. You can configure trace for the service on one server or on all servers in the cluster. To configure trace settings, choose what information you want to include in the trace log by choosing the debug level and trace fields. You can also configure trace for specific devices if you are configuring trace for the Cisco CallManager service or the Cisco CTIManager service. If you want to run predetermined traces on services, set troubleshooting trace for those services.	Trace Configuration, *Cisco CallManager Serviceability Administration Guide* Troubleshooting Trace Setting Configuration, *Cisco CallManager Serviceability Administration Guide*
Step 3	Install the real-time monitoring tool on a local PC.	Real-Time Monitoring Configuration, *Cisco CallManager Serviceability Administration Guide*
Step 4	If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the TraceCollectionToolEvent alert.	Setting Alert Properties, *Cisco CallManager Serviceability Administration Guide*
Step 5	If you want to automatically capture traces for alerts such as CriticalServiceDownand CodeYellow, check the **Enable TCT Download** check box in Set Alert/Properties dialog box for the alerts.	Setting Alert Properties, *Cisco CallManager Serviceability Administration Guide*
Step 6	Collect Cisco CallManager traces, applications, and system traces within the Cisco CallManager cluster.	Trace Collection and Log Central in RTMT, *Cisco CallManager Serviceability Administration Guide*

Table 4-1 Trace Configuration and Collection Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 7	View the log file in the appropriate viewer.	Using Local Browse, *Cisco CallManager Serviceability Administration Guide* Using the Query Wizard, *Cisco CallManager Serviceability Administration Guide* Using Q931 Translator, *Cisco CallManager Serviceability Administration Guide* Displaying QRT Report Information, *Cisco CallManager Serviceability Administration Guide*
Step 8	If you enabled troubleshooting trace, reset the trace settings services on the Cisco CallManager nodes, so the original settings get restored. **Note** Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.	Troubleshooting Trace Setting Configuration, *Cisco CallManager Serviceability Administration Guide*

Where to Find More Information

Related Topics

- Alarm Configuration, page 3-2
- Alarm Configuration Checklist, page 3-3
- Alarm Configuration, *Cisco CallManager Serviceability Administration Guide*
- Trace Configuration, *Cisco CallManager Serviceability Administration Guide*
- Trace Collection and Log Central in RTMT, *Cisco CallManager Serviceability Administration Guide*
- Setting Alert Properties, *Cisco CallManager Serviceability Administration Guide*
- Using Q931 Translator, *Cisco CallManager Serviceability Administration Guide*
- Troubleshooting Trace Setting Configuration, *Cisco CallManager Serviceability Administration Guide*

Real-Time Monitoring Tool

This chapter contains information on the following topics:

Understanding the Real-Time Monitoring Tool

Real-Time Monitoring Tool, which runs as a client-side application, uses HTTPS and TCP to monitor device status, system performance, device discovery, and CTI applications in the Cisco CallManager cluster. The tool also connects directly to devices via HTTPS to troubleshoot system problems.

Note Even when RTMT does not run, tasks such as alarm and performance monitoring updates occur in the background.

RTMT allows you to perform the following tasks:

- Monitor a set of management objects that are preconfigured
- Generate various alerts, in the form of e-mails, for objects when values go over/below user-configured thresholds
- Collect and view traces in various default viewers that exist in RTMT
- Translate Q931 messages
- View syslog messages in SysLog Viewer
- Work with performance-monitoring counters

You can install RTMT, which works for resolutions 800*600 and above, on a Windows 98, Windows XP, Windows 2000, or Red Hat Linux with KDE and/or Gnome client. To avoid CPU spiking while you collect and zip files, do not install RTMT on a server where you installed Cisco CallManager. For information on how to install and launch RTMT, refer to the following sections in the *Cisco CallManager Serviceability Administration Guide*:

- Installing the Real-Time Monitoring Tool (RTMT), page 7-1
- Using RTMT, page 7-3

To connect to any node in the Cisco CallManager cluster, you must enter the CCMAdministrator application user authentication information in the User Name and Password fields when you launch the tool. Likewise, you must enter either the IP address or host name of the first node. If the authentication fails for any reason, the tool prompts you to reenter the server and authentication details. After the authentication succeeds, RTMT launches the monitoring module from local cache or from a remote node when the local cache does not contain a monitoring module that matches the backend version.

After you initially load RTMT, the load includes a default configuration that is called CM-Default. The first time that you use RTMT, it will use the CM-Default profile and display the summary page in the monitor pane. CM-Default dynamically monitors all registered phones for all Cisco CallManager nodes. If your cluster contains five configured Cisco CallManager nodes, CM-Default displays the registered phones for each node in a Cisco CallManager cluster, as well as calls in progress and active gateway ports and channels.

You can configure RTMT to display the information that interests you, such as different performance counters for different features, in the monitor pane of RTMT and save the framework of your configuration in a profile. You can then restore the profile at a later time during the same session or the next time that you log in to RTMT. By creating multiple profiles, so each profile displays unique information, you can quickly display different information by switching profiles.

You save, restore, and delete Cisco CallManager configuration information by using Profile in the System menu, as described in "Working with Configuration Profiles" section on page 7-5.

RTMT generates daily reports in PDF format for precanned objects, as described in the "RTMT Collector, Alert Manager, and RTMT Reporter" section on page 5-4.

RTMT arranges the preconfigured monitoring objects into the following major categories:

- Summary
- Server
- Call Process
- Service
- Device
- CTI
- Performance

RTMT Components

The RTMT window comprises the following main components:

- Menu Bar, which includes the following menu options:
  - System—Allows you to save, restore, and delete existing RTMT profiles, monitor Java Heap Memory Usage, go to the Serviceability Report Archive window in Cisco CallManager Serviceability, log off or exit RTMT.
  - Monitor—Allows you to monitor precanned objects.
  - Search—Allows you to search for devices, such as phones and H.323 devices, and for CTI applications, devices, and lines to monitor.
  - Edit—Allows you to configure categories (for table format view), set the polling rate for devices and performance monitoring counters, hide the quick launch channel, and edit the trace setting for RTMT.
  - Devices—Allows you to search for devices and to view phone information, port/channel status, and so on.
  - Performance—Allows you to work with performance monitoring counters.
  - Tools—Allows you to work with alerts, collect traces, and view syslog messages.
  - Window—Allows you to close a single RTMT window or all RTMT windows.
  - Application—Allows you to browse to Cisco CallManager Administration or Cisco CallManager Serviceability
  - Help—Allows you to access RTMT documentation online help or to view the RTMT version.
- Quick Launch Channel—Pane on the left side of RTMT window that displays icons that you can click to monitor various objects.
- View/Tool tabs—Allows you to display preconfigured categories in the Quick Launch Channel; Tool tab displays alert, trace, and syslog viewer categories.

  The View and Tools tabs differ in that anything related to the View tab gets saved as a profile that can be restored at any time that RTMT is invoked. The Tools tab relates only to the systemwide alert functionality. You cannot save the states.
- Monitor pane—Pane where monitoring results display.

RTMT Services, Servlets and Service Parameters

RTMT uses the following services/servlets:

- AMC service—This service starts up automatically after the installation and allows RTMT to retrieve real-time information that exists on nodes in the cluster.

  The following list comprises some AMC service parameters that are associated with RTMT. For the latest list of parameters, choose Server > Service Parameters in Cisco CallManager Administration. Then, choose the server and the AMC service.
  - Primary Collector
  - Failover Collector
  - Data Collection Enabled
  - Data Collection Polling Rate

  - Data Collection Reenumeration Interval
  - RIS Client Timeout
  - Server Synchronization Period
  - RMI Port Number
  - Alert Manager Enabled
  - Logger Enabled
  - Alarm Enabled
  - PerfMon Log Deletion Age

  For information on these service parameters, click the i button that displays in the Service Parameter window of Cisco CallManager Administration.

- Cisco CallManager Serviceability RTMT service (in the Control Center—Network Services window)— Supporting the Cisco CallManager Real-Time Monitoring Tool (RTMT), this service installs with Cisco CallManager and starts up automatically after the installation.
- Cisco RTMT Reporter servlet (in the Control Center—Network Services window)—This service, which installs with Cisco CallManager and starts up automatically after the installation, allows you to publish reports for RTMT.

RTMT Collector, Alert Manager, and RTMT Reporter

RTMT Collector, a component that automatically gets installed with Cisco CallManager, logs preconfigured monitoring objects information while Alert Manager, also automatically installed, logs alert histories into log files. Each preconfigured object belongs to one of several categories: devices, services, servers, call activities, and PPR. Each category has a separate log file, and alert details get logged in a separate file. Also, a separate log file exists to log important perfmon object values for Cisco CallManager-related services and processes.

Tip Although they require no configuration tasks to run, RTMT Collector and Alert Manager support redundancy. If the primary collector or manager fails for any reason, the secondary collector and manager perform the tasks until primary support becomes available. RTMT Collector, Alert Manager, and RTMT Reporter run on the first node to minimize call-processing interruptions.

The locally written log files appear in the primary collector server at /var/log/active/cm/log/amc. Because the primary collector changes because of failover and fallback scenarios, the log files can exist on more than one server in the Cisco CallManager cluster.

Log files exist in csv format. You can read log files, except an alert log file, by using native NT perfmon viewer. New log files get created every day at 00:00 hours on the local system. New logs for devices, services, servers, and calls get created when the time zone changes, when a new node is added to the cluster, or during failover/fallback scenarios. The first column of all these logs comprises the time zone information and the number of minutes from the Greenwich Meridian Time (GMT). RTMT Reporter uses these log files as a data source to generate daily summary reports. The report, which is based on the default monitoring objects, generates every 24 hours for the following information:

- Call Activity Status—Number of call attempted and number of calls completed for each Cisco CallManager, each gateway, trunk, and overall cluster. Number of channels available, in-service for each gateway.
- Device Status—Number of registered phones, gateways and trunks per each server and overall cluster.
- Server Status—% CPU load,% memory used,% disk space used per server.
- Service Status —For each CTI Manager, number of opened devices and lines. For each TFTP server, number attempted and failed requests.
- Alert Status—Number of alerts per server. Number of alert per severity level for the cluster, including the top 10 alerts in the cluster.
- Performance Protection Report—Trend analysis information on default monitoring objects that allows you to track overall system health. The report includes information for the for the last 7 days for each server.

Tip The RTMT reports display in English only.

The following service parameters apply to RTMT report generation: RTMT Reporter Designated Node, RTMT Report Generation Time, and RTMT Report Deletion Age. For information on these parameters, click the i button that displays in the Service Parameter window in Cisco CallManager Administration.

For more information on the Serviceability reports, see the "Serviceability Reports Archive" section on page 9-1.

Viewing a Summary

The Summary option in RTMT allows you to monitor important common information in a single monitoring pane. In a summary, you can monitor the following information:

- Virtual Memory usage
- CPU usage
- Registered phones
- Calls in progress
- Active gateway ports and channels

Monitoring Server Status

The Servers category monitors CPU and memory usage, processes, disk space usage, and critical services on each Cisco CallManager server.

The CPU and Memory monitor provide information about the CPU usage and Virtual memory usage on each Cisco CallManager server. For each CPU, the information includes the percentage of time each processor spends executing processes in different modes and operations (User, Nice, System, Idle, IRQ, SoftIRQ, and IOWait). The percentage of CPU is the total time spent executing in all the different modes and operations excluding the Idle time. For memory, the information includes the Total, Used, Free, Shared, Buffers, Cached, Total Swap, Used Swap, and Free Swap memory in Kbytes, and the percentage of Virtual Memory in Use.

The Processes monitor provide information about the processes that are running on the system. These processes include the process, process ID (PID), CPU percentage, Status, Shared Memory (KB), Nice (level), VmRSS (KB), VmSize (KB), VmData (KB), Thread Count, Page Fault Count, and Data Stack Size (KB).

The Critical Services monitoring category provides the name of the critical service, the status (whether the service is up, down, or activated), and the elapsed time during which the services have existed in a particular status for a particular Cisco CallManager node.

Table 5-1 provides information about the objects that RTMT monitors, the alert, thresholds, and defaults. For information on daily CPU, memory, and disk usage reports, see the "Server Statistics Report" section on page 9-5.

Table 5-1 Servers Category

Monitored Objects (displayed)	Alert/Threshold/Default
• CPU Usage (100% Idle) on each server. • Virtual Memory Usage (% memory in use out of total) on each server. • CPU and memory usage for all processes on each server	• Call Processing node - CPU usage pegged X% over X seconds. Default specifies 90%, 30 seconds. • Non-CallProcessing node - CPU Usage pegged X% over X seconds. Default specifies 99%, 120 seconds. • Available memory equals less than X%. Default specifies 10%. • When CPU peg or excessive memory usage alerts occur, the name of the top process displays in the alert message. In case of dllhost service, the real meaningful name displays instead of generic name dllhost.
Disk space usage for all logical drives on each server.	Available disk space on the largest logical drive equals less than X%. Default specifies 10%.
State of activated critical services on each server.	Service state changed from Up->Down.

Understanding Server Logs

Every 5 minutes, the server data gets logged into the file as a single record. The system logs the data every 5 minutes for the following counters, based on the following calculation:

- cpuUsage—Average of all the values that were collected in the last 5 minutes
- MemoryInUse—Average of all the values that were collected in the last 5 minutes
- DiskSpaceInUse—Average of all the values that were collected in the last 5 minutes for the active partition

The AMC service logs the server data in csv format. The header of the log comprises the time zone information and a set of columns with the previous counters for a Cisco CallManager node. These sets of columns repeat for every node.

The following file name format of the server log applies: ServerLog_MM_DD_YYYY_hh_mm.csv. The first line of each log file comprises the header.

To download the server logs for viewing on your local computer, refer to Trace Collection and Log Central in RTMT, page 10-1

Monitoring Call-Processing Activity

The Call Process monitoring category monitors the following items:

- Call Activity—You can monitor the number of calls that were attempted, calls that were completed, and call in progress for a particular Cisco CallManager node or the entire cluster.
- Gateway Activity—You can monitor gateway activity for each gateway type. Gateway activity monitoring includes the number of active ports, the number of ports in service, and the number of calls that were completed for each gateway type for a particular Cisco CallManager node or the entire cluster.
- Trunk Activity—The system monitors trunk activity by trunk type for a particular node or cluster. Trunk activity monitoring includes the number of calls in progress and the number of calls that were completed for a particular trunk type.
- SDL Queue—SDL Queue monitoring monitors the number of signals in the SDL queue and the number of signals that were processed for a particular signal distribution layer (SDL) queue type. The SDL queue types comprise high, normal, low, and lowest queue. You can monitor the SDL queue for a particular node or the entire cluster.
- SIP Activity—The system displays a summary of SIP requests, SIP responses, total number of failed incoming responses (4xx, 5xx, and 6xx), total number of failed outgoing responses (4xx, 5xx, and 6xx), number of retry requests, and number of retry responses.

Table 5-3 provides information about the objects that RTMT monitors, the alert, thresholds, and defaults. For information on Cisco CallManager call activity daily reports, see the "Call Activities Report" section on page 9-9.

Table 5-2 Call Activities Category

Monitored Objects (displayed)	Alert/Threshold/Default
CallsAttempted, CallsCompleted, and CallsInProgress for each Cisco CallManager node and cluster.	N/A
CallsAttempted, CallsCompleted, and CallsInProgress of each type of MGCP FXS/FXO/PRI/T1CAS/H.323 gateway, as well as SIP and H.323 Trunks for each Cisco CallManager node and cluster.	N/A
Channel/Port Status of each MGCP FXS/FXO/PRI/T1CAS gateway.	N/A
SDL Queue activity on each Cisco CallManager node.	N/A
MGCP FXS Gateway - Number of In-Service and Active ports for each Cisco CallManager node and cluster.	• Route-List exhausted
MGCP FXO Gateway - number of In-Service and Active ports for each Cisco CallManager node and cluster.	• Route-List exhausted

Table 5-2 Call Activities Category (continued)

Monitored Objects (displayed)	Alert/Threshold/Default
MGCP PRI Gateway - Number of In-Service and Active channels for each Cisco CallManager node and cluster.	• D-Channel out of service • Route List exhausted
MGCP T1CAS Gateway - number of In-Service and Active ports for each Cisco CallManager node and cluster.	• Route List exhausted

Understanding Call-Processing Logs

The system accumulates call-processing data in the memory whenever RTMT calls the LogCall API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every 5 minutes for the following counters on the basis of the following calculation:

- cmCallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsInProgress—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXO_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_PRI_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_T1_CAS_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsInProgress—Average of all the values that were collected in last 5 minutes
- gwH323_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkH323_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkH323_CallsInProgress—Average of all the values collected in last 5 minutes
- trunkH323_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsInProgress—Average of all the values that were collected in last 5 minutes
- trunkSIP_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)

- gwMGCP_FXS_PortsInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_PortsInService—Average of all the values that were collected in lasts 5 minutes
- gwMGCP_PRI_SpansInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_SpansInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_ActivePorts—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_ActivePorts—Average of all the values that were collected in last 5 minutes
- gwMGCP_PRI_ActiveChannels—Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_ActiveChannels—Average of all the values that were collected in last 5 minutes

The AMC service logs the call data in windows Performance tool-compatible csv format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for a node. These sets of columns repeat for every node.

The following file name format of the Call Log applies: CallLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log file comprises the header.

Monitoring Services

The Service monitoring category monitors the activities of Cisco TFTP requests, heartbeat of different nodes, and database activities.

The Cisco TFTP service builds and serves files that are consistent with the trivial file transfer protocol, which is a simplified version of the File Transfer Protocol (FTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files. You can view the total Cisco TFTP requests, requests not found, and requests that were aborted.

The tool (RTMT) monitors the heartbeat of Cisco CallManagers, Cisco TFTPs, and Cisco CallManager Attendant Console Server services for different nodes.The heartbeat acts as an indicator of the life of whatever it is monitoring. When the heartbeat is lost, a blinking icon appears in the lower, right corner of the RTMT window. To find when the heartbeat loss was detected, click the blinking icon. An e-mail can notify you of the heartbeat loss, if you configure the system to do so.

The database summary provides connection information for each node, such as the connection requests that are queued in the database, the connection requests that are queued in memory, the total number of active client connections, and the number of devices that are queued for a device reset.

Table 5-3 provides information about the objects that RTMT monitors, the alert, thresholds, and defaults. For information on daily reports for CTI and Cisco TFTP usage statistics, see the "Service Statistics Report" section on page 9-7.

Table 5-3 Services Category

Monitored Objects (displayed)	Alert/Threshold/Default
Number of open devices, lines, CTI connections, and active Cisco CallManager links for each CTI Manager.	N/A
TotalTftpRequests and TotalTftpRequestsAborted for each Cisco TFTP server.	N/A
Connection and replication status for each Directory server.	• Connection failed. • Replication failed.
Heartbeat rate for each Cisco CallManager, Cisco TFTP, and TCD services.	• Cisco CallManager heartbeat rate equals <0.x. Default equals 0.5. • Cisco TFTP heartbeat rate equals <0.x. Default specifies 0.5. • TCD heartbeat rate equals <0.x. Default specifies 0.5.

Understanding Service Logs

The service data accumulates in the memory whenever RTMT calls the LogService API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every 5 minutes for the following counters, based on the following calculation:

- ctiOpenDevices—Average of all the values that were collected in last 5 minutes
- ctiLines—Average of all the values that were collected in last 5 minutes
- ctiConnections—Average of all the values that were collected in last 5 minutes
- ctiActiveCMLinks—Average of all the values that were collected in last 5 minutes
- tftpRequests—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- tftpAbortedRequests—Cumulative (difference between last collected value and the first collected value in last 5 minutes)

The AMC service logs the service data in csv format. The header of the log comprises the time zone information and a set of columns with the counters that were previously listed for a Cisco CallManager node. These sets of columns repeat for every node.

The following file name format of the Service Log applies: ServiceLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log comprises the header.

Monitoring Devices

The Device monitoring category provides a summary of devices, device search capability, and a summary of phones.

The device summary provides information on the number of registered phones, gateways, and media resource devices on each Cisco CallManager. Table 5-4 provides information about the objects that RTMT monitors, the alert, thresholds, and defaults, and what kind of reports that RTMT generates for those devices. For information on daily reports on number of registered devices, see the "Device Statistics Report" section on page 9-2.

Table 5-4 Devices Category

Monitored Objects (displayed)	Alert/Threshold/Default
Number of registered phones for each Cisco CallManager and cluster.	• Total number of registered phones drops by X% in consecutive polls. Default specifies 10%.
Number of registered gateways on each Cisco CallManager and cluster.	• (Warning) Clusterwide total number of registered gateways decreased in consecutive polls. • (Informational) Clusterwide total number of registered gateways increased in consecutive polls.
Number of registered media devices on each Cisco CallManager and cluster.	• (Warning) Clusterwide total number of registered media devices decreased in consecutive polls. • (Informational) Clusterwide total number of registered media devices increased in consecutive polls. • Media List exhausted.

The Device Search menu comprises the following items on which you can search: phones, gateway devices, H.323 devices, CTI devices, voice-messaging devices, media resources, hunt lists, and SIP trunks.

You can search on any device in the Cisco CallManager cluster and choose the status of the devices, including registered, unregistered, rejected, any status, and devices that are only configured in the database. You can also search by any model, or a specific device model, and set up criteria that include several different attributes. For phones, you can also search on the basis of phone protocol.

Tip To find the matching item, RTMT requires that you activate the RIS service in the Service Activation window.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a time stamp of the device that has been opened/closed and the application that controls the device media.

The phone summary provides information on the number of Registered Phones, SIP phones, SCCP Phones, Partially Registered phones, and the number of failed registration attempts.

Understanding Device Logs

The device data accumulates in the memory whenever RTMT calls the LogDevice API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The data gets logged every 5 minutes for the following counters based on the following calculation:

- gatewayDevicesFXS—Average of all the values that were collected in last 5 minutes
- gatewayDevicesFXO—Average of all the values that were collected in last 5 minutes
- gatewayDevicesPRI—Average of all the values that were collected in last 5 minutes
- gatewayDevicesT1—Average of all the values that were collected in last 5 minutes
- gatewayDevicesH323—Average of all the values that were collected in last 5 minutes

The AMC service logs the device data in csv format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for a node. These sets of columns repeat for every node.

The following file name format of the Device Log applies: DeviceLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log file comprises the header.

Monitoring CTI Applications, Devices, and Lines

The CTI search menu allows you to search on the following CTI components:

- CTI Applications
- CTI Devices
- CTI Lines

The CTI category monitors CTI Manager activities and provides CTI search capability. With CTI Manager, you can monitor the number of open devices, lines, and CTI connections. You can specify criteria for the CTI applications, devices, and lines that include CTI status, device name, application pattern, and attributes.

Tip To find the matching item, RTMT requires that you activate the RIS service in the Service Activation window in Cisco CallManager Serviceability.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a time stamp of the device that has been opened/closed and the application that controls the device media.

Where to Find More Information

Related Topics

- Alert Configuration in RTMT, *Cisco CallManager Serviceability Administration Guide*
- Configuring and Using Performance Monitoring, *Cisco CallManager Serviceability Administration Guide*

- Trace Collection and Log Central in RTMT, *Cisco CallManager Serviceability Administration Guide*
- Alerts, page 7-1
- Performance Objects and Counters, page 6-1

Performance Objects and Counters

This chapter, which provides an overview of Cisco CallManager-related objects and counters, contains information on the following topics:

Working with Performance Objects and Counters

Cisco CallManager directly updates Performance counters (called PerfMon counters), which are call-processing-related counters. The counters contain simple, useful counts such as number of registered phones, number of active calls, and number of available conference bridge resources.

The Cisco CallManager object contains most of the performance counters, and these counters have only one instance. The instance-based counters that belong to the other objects can have zero or more instances. For example, if two phones are registered to Cisco CallManager, two instances of each counter that belong to the Cisco phones object exist.

For information on specific counters, click the blue text in the following list to go to the object:

Tip For the latest performance monitoring counters, objects, and counter descriptions that are available for Cisco CallManager, access the performance monitoring counters in the Real-Time Monitoring Tool. In RTMT, you can review a counter description, as described in the "Displaying a Counter Description" section on page 9-9.

Cisco Analog Access

The Cisco Analog Access object provides information about registered Cisco Analog Access gateways. Table 6-1 contains information about Cisco Analog Access counters.

Table 6-1 Cisco Analog Access

Counters	Counter Descriptions
OutboundBusyAttempts	This counter represents the total number of times that Cisco CallManager attempts a call through the Analog Access gateway when all ports were busy.
PortsActive	This counter represents the number of ports that are currently in use (active). A port appears active when a call is in progress on that port.
PortsOutOfService	This counter represents the number of ports that are currently out of service. Counter applies only to loop-start and ground-start trunks.

Cisco Annunciator Device

The Cisco Annunciator Device object provides information about registered Cisco annunciator devices. Table 6-2 contains information about Cisco Annunciator counters.

Table 6-2 Cisco Annunciator Device

Counters	Counter Descriptions
OutOfResources	This counter represents the total number of times that Cisco CallManager attempted to allocate an annunciator resource from an annunciator device and failed; for example, because all resources were already in use.
ResourceActive	This counter represents the total number of annunciator resources that are currently active (in use) for an annunciator device.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used at the current time for the annunciator device.
ResourceTotal	This counter represents the total number of annunciator resources that are configured for an annunciator device.

Cisco CallManager

The Cisco CallManager object provides information about calls, applications, and devices that are registered with the Cisco CallManager. Table 6-3 contains information about Cisco CallManager counters.

Table 6-3 Cisco CallManager

Counters	Counter Descriptions
AnnunciatorOutOfResources	This counter represents the total number of times that Cisco CallManager attempted to allocate an annunciator resource from those that are registered to a Cisco CallManager when none were available.
AnnunciatorResourceActive	This counter represents the total number of annunciator resources that are currently in use on all annunciator devices that are registered with a Cisco CallManager.
AnnunciatorResourceAvailable	This counter represents the total number of annunciator resources that are not active and are currently available.
AnnunciatorResourceTotal	This counter represents the total number of annunciator resources that are provided by all annunciator devices that are currently registered with Cisco CallManager.
AuthenticatedCallsActive	This counter represents the number of authenticated calls that are currently active (in use) on Cisco CallManager. An authenticated call designates one in which all the endpoints that are participating in the call are authenticated. An authenticated phone uses the Transport Layer Security (TLS) authenticated Skinny protocol signaling with Cisco CallManager.

Table 6-3 Cisco CallManager (continued)

Counters	Counter Descriptions
AuthenticatedCallsCompleted	This counter represents the number of authenticated calls that connected and subsequently disconnected through Cisco CallManager. An authenticated call designates one in which all the endpoints that are participating in the call are authenticated. An authenticated phone uses the TLS authenticated Skinny protocol signaling with Cisco CallManager.
AuthenticatedPartiallyRegisteredPhone	This counter represents the number of partially registered, authenticated SIP phones.
AuthenticatedRegisteredPhones	This counter represents the total number of authenticated phones that are registered to Cisco CallManager. An authenticated phone uses the TLS authenticated Skinny protocol signaling with Cisco CallManager.
BRIChannelsActive	This counter represents the number of BRI voice channels that are currently in an active call on this Cisco CallManager.
BRISpansInService	This counter represents the number of BRI spans that are currently available for use.
CallManagerHeartBeat	This counter represents the heartbeat of Cisco CallManager. This incremental count indicates that Cisco CallManager is up and running. If the count does not increment, that indicates that Cisco CallManager is down.
CallsActive	This counter represents the number of voice or video streaming connections that are currently in use (active); in other words, the number of calls that actually have a voice path that is connected on Cisco CallManager.
CallsAttempted	This counter represents the total number of attempted calls. An attempted call occurs any time that a phone goes off hook and back on hook, regardless of whether any digits were dialed, or whether it connected to a destination. The system considers some call attempts during feature operations (such as transfer and conference) to be attempted calls.
CallsCompleted	This counter represents the number of calls that were actually connected (a voice path or video stream was established) through Cisco CallManager. This number increases when the call terminates.
CallsInProgress	This counter represents the number of voice or video calls that are currently in progress on Cisco CallManager, including all active calls. When a phone goes off hook, this action creates a call in progress until it goes back on hook. When all voice or video calls that are in progress are connected, the number of CallsInProgress represents the number of CallsActive.
EncryptedCallsActive	This counter represents the number of encrypted calls that are currently active (in use) on this Cisco CallManager. An encrypted call represents one in which all the endpoints that are participating in the call are encrypted.

Table 6-3 Cisco CallManager (continued)

Counters	Counter Descriptions
EncryptedCallsCompleted	This counter represents the number of encrypted calls that were connected and subsequently disconnected through this Cisco CallManager. An encrypted call represents one in which all the endpoints that are participating in the call are encrypted.
EncryptedPartiallyRegisteredPhones	This counter represents the number of partially registered, encrypted SIP phones.
EncryptedRegisteredPhones	This counter represents the total number of encrypted phones that are registered on this Cisco CallManager.
FXOPortsActive	This counter represents the number of FXO ports that are currently in use (active) on a Cisco CallManager.
FXOPortsInService	This counter represents the number of FXO ports that are currently available for use in the system.
FXSPortsActive	This counter represents the number of FXS ports that are currently in use (active) on a Cisco CallManager.
FXSPortsInService	This counter represents the number of FXS ports that are currently available for use in the system.
HuntListsInService	This counter represents the number of hunt lists that are currently in service on Cisco CallManager.
HWConferenceActive	This counter represents the total number of hardware conference resources that are provided by all hardware conference bridge devices that are currently registered with Cisco CallManager.
HWConferenceCompleted	This counter represents the total number of conferences that used a hardware conference bridge (hardware-based conference devices such as Cisco Catalyst 6000, Cisco Catalyst 4000, Cisco VG200, Cisco series 26xx and 36xx) that is allocated from Cisco CallManager and that have completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
HWConferenceOutOfResources	This counter represents the total number of times that Cisco CallManager attempted to allocate a hardware conference resource from those that are registered to a Cisco CallManager when none was available.
HWConferenceResourceActive	This counter represents the total number of conference resources that are in use on all hardware conference devices (such as Cisco Catalyst 6000, Catalyst 4000, Cisco VG200, Cisco series 26xx and 36xx) that are registered with Cisco CallManager. System considers conference to be active when one or more calls are connected to a bridge.

Table 6-3 Cisco CallManager (continued)

Counters	Counter Descriptions
HWConferenceResourceAvailable	This counter represents the number of hardware conference resources that are not in use and that are available to be allocated on all hardware conference devices (such as Cisco Catalyst 6000, Cisco Catalyst 4000, Cisco VG200, Cisco series 26xx and 36xx) that are allocated from Cisco CallManager and that have been completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
HWConferenceResourceTotal	This counter represents the number of active conferences on all hardware conference devices that are registered with Cisco CallManager.
InitializationState	This counter represents the current initialization state of Cisco CallManager. Cisco CallManager includes the following initialization state values: 1-Database; 2-Regions; 3-Locations; 4-Calling Search Space; 5-Time Of Day; 6-AAR Neighborhoods; 7-Digit Analysis; 8-Route Plan; 9-Call Control; 10-Supplementary Services; 11-Directory; 12-SDL Link; 13-Device; 100-Initialization Complete. Not all states displays when this counter is used. This does not indicate that an error occurred; it simply indicates that the state(s) initialized and completed within the refresh period of the performance monitor.
LocationOutOfResources	This counter represents the total number of times that a call through Locations failed due to the lack of bandwidth.
MOHMulticastResourceActive	This counter represents the total number of multicast MOH resources that are currently in use (active) on all MOH servers that are registered with a Cisco CallManager.
MOHMulticastResourceAvailable	This counter represents the total number of active multicast MOH connections that are not being used on all MOH servers that are registered with a Cisco CallManager.
MOHOutOfResources	This counter represents the total number of times that the Media Resource Manager attempted to allocate an MOH resource when all available resources on all MOH servers that are registered with a Cisco CallManager were already active.
MOHTotalMulticastResources	This counter represents the total number of multicast MOH resources or connections that are provided by all MOH servers that are currently registered with a Cisco CallManager.
MOHTotalUnicastResources	This counter represents the total number of unicast MOH resources or streams that are provided by all MOH servers that are currently registered with Cisco CallManager. Each MOH unicast resource uses one stream.

Table 6-3 Cisco CallManager (continued)

Counters	Counter Descriptions
MOHUnicastResourceActive	This counter represents the total number of unicast MOH resources that are currently in use (active) on all MOH servers that are registered with Cisco CallManager. Each MOH unicast resource uses one stream.
MOHUnicastResourceAvailable	This counter represents the total number of unicast MOH resources that are currently available on all MOH servers that are registered with Cisco CallManager. Each MOH unicast resource uses one stream.
MTPOutOfResources	This counter represents the total number of times Cisco CallManager attempted but failed to allocate an MTP resource from one MTP device that is registered with Cisco CallManager. This also means that no transcoders were available to act as MTPs.
MTPResourceActive	This counter represents the total number of MTP resources that are currently in use (active) on all MTP devices that are registered with a Cisco CallManager. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
MTPResourceAvailable	This counter represents the total number of MTP resources that are not in use and are available to be allocated on all MTP devices that are registered with Cisco CallManager. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
MTPResourceTotal	This counter represents the total number of media termination point (MTP) resources that are provided by all MTP devices that are currently registered with Cisco CallManager.
PartiallyRegisteredPhone	This counter represents the number of partially registered SIP phones.
PRIChannelsActive	This counter represents the number of PRI voice channels that are in an active call on a Cisco CallManager.
PRISpansInService	This counter represents the number of PRI spans that are currently available for use.
RegisteredAnalogAccess	This counter represents the number of registered Cisco analog access gateways that are registered with system. The count does not include the number of Cisco analog access ports.
RegisteredHardwarePhones	This counter represents the number of Cisco hardware IP phones (for example, Cisco IP Phone models 7960, 7940, 7910, and so on.) that are currently registered in the system.
RegisteredMGCPGateway	This counter represents the number of MGCP gateways that are currently registered in the system.
RegisteredOtherStationDevices	This counter represents the number of station devices other than Cisco hardware IP phones that are currently registered in the system (for example, Cisco IP SoftPhone, CTI port, CTI route point, Cisco voice-mail port).

Table 6-3 Cisco CallManager (continued)

Counters	Counter Descriptions
SIPLineServerAuthorizationChallenges	This counter represents the number of authentication challenges for incoming SIP requests that the Cisco CallManager server issued to SIP phones. An authentication challenge occurs when a SIP phone with Digest Authentication enabled sends a SIP line request to Cisco CallManager.
SIPLineServerAuthorizationFailures	This counter represents the number of authentication challenge failures for incoming SIP requests from SIP phones to the Cisco CallManager server. An authentication failure occurs when a SIP phone with Digest Authentication enabled sends a SIP line request with bad credentials to Cisco CallManager.
SIPTrunkApplicationAuthorization	This counter represents the number of application-level authorization checks for incoming SIP requests that the Cisco CallManager server issued to SIP trunks. An application-level authorization check occurs when the Cisco CallManager system compares an incoming SIP request to the application-level settings on the SIP Trunk Security Profile window in Cisco CallManager Administration.
SIPTrunkApplicationAuthorizationFailures	This counter represents the number of application-level authorization failures for incoming SIP requests that occurred on Cisco CallManager SIP trunks. An application-level authorization failure occurs when Cisco CallManager compares an incoming SIP request to the application-level settings on the SIP Trunk Security Profile window in Cisco CallManager Administration and finds that application-level authorization for one or more of the features on that window is not allowed.
SIPTrunkServerAuthorizationChallenges	This counter represents the number of authentication challenges for incoming SIP requests that Cisco CallManager issued to SIP trunks. An authentication challenge occurs when a SIP trunk with Digest Authentication enabled sends a SIP request to Cisco CallManager.
SIPTrunkServerAuthorizationFailures	This counter represents the number of authentication challenge failures that occurred for incoming SIP requests from SIP trunks to Cisco CallManager. An authentication failure occurs when a SIP trunk with Digest Authentication enabled sends a SIP request with bad credentials to Cisco CallManager.
SWConferenceActive	This counter represents the number of active conferences on all software conference devices that are registered with Cisco CallManager.
SWConferenceCompleted	This counter represents the total number of conferences that used a software conference bridge that was allocated from a Cisco CallManager and that have been completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.

Table 6-3 Cisco CallManager (continued)

Counters	Counter Descriptions
SWConferenceOutOfResources	This counter represents the total number of times that Cisco CallManager attempted to allocate a software conference resource from those that are registered to Cisco CallManager when none were available. Counter includes failed attempts to add a new participant to an existing conference.
SWConferenceResourceActive	This counter represents the total number of conference resources that are in use on all software conference devices that are registered with Cisco CallManager. The system considers a conference to be active when one or more calls connect to a bridge. One resource is equal to one stream.
SWConferenceResourceAvailable	This counter represents the number of new software-based conferences that can be started at the same time, for Cisco CallManager. You must have a minimum of three streams available for each new conference.One resource is equal to one stream
SWConferenceResourceTotal	This counter represents the total number of software conference resources that are provided by all software conference bridge devices that are currently registered with Cisco CallManager.
SystemCallsAttempted	This counter represents the total number of server originated calls and attempted calls to the Unity Message waiting indicator (MWI).
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are in an active call on a Cisco CallManager.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently available for use.
TLSConnectedSIPTrunks	This counter represents the number of SIP trunks that are configured and connected via Transport Layer Security (TLS).
TLSConnectedWSM	This counter represents the number of WSM Connectors that is configured and connected to Motorola WSM via Transport Layer Security (TLS).
TranscoderOutOfResources	This counter represents the total number of times that Cisco CallManager attempted to allocate a transcoder resource from a transcoder device that is registered to a Cisco CallManager when none was available.
TranscoderResourceActive	This counter represents the total number of transcoders that are in use on all transcoder devices that are registered with Cisco CallManager. A transcoder in use represents one transcoder resource that has been allocated for use in a call. Each transcoder resource uses two streams.
TranscoderResourceAvailable	This counter represents the total number of transcoders that are not in use and that are available to be allocated on all transcoder devices that are registered with Cisco CallManager. Each transcoder resource uses two streams.
TranscoderResourceTotal	This counter represents the total number of transcoder resources that are provided by all transcoder devices that are currently registered with Cisco CallManager.

Table 6-3 Cisco CallManager (continued)

Counters	Counter Descriptions
VCBConferenceActive	This counter represents the total number of active video conferences on all video conference bridge devices that are registered with Cisco CallManager.
VCBConferenceAvailable	This counter represents the total number of new video conferences on all video conference bridge devices that are registered with Cisco CallManager.
VCBConferenceCompleted	This counter represents the total number of video conferences that used a video conference bridge that are allocated from Cisco CallManager and that have been completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
VCBConferenceTotal	This counter represents the total number of video conferences that are supported on all video conference bridge devices that are registered with Cisco CallManager.
VCBOutOfConferences	This counter represents the total number of times that Cisco CallManager attempted to allocate a video conference resource from those that are registered to Cisco CallManager when none was available.
VCBOutOfResources	This counter represents the total number of failed new video conference requests. A conference request can fail because, for example, the configured number of conferences is already in use.
VCBResourceActive	This counter represents the total number of video conference resources that are currently in use on all video conference devices that are registered with Cisco CallManager.
VCBResourceAvailable	This counter represents the total number of video conference resources that are not active and are currently available.
VCBResourceTotal	This counter represents the total number of video conference resources that are provided by all video conference bridge devices that are currently registered with Cisco CallManager.
VideoCallsActive	This counter represents the number of active video calls with active video streaming connections on all video conference bridge devices that are registered with Cisco CallManager.
VideoCallsCompleted	This counter represents the number of video calls that were actually connected with video streams and then released.
VideoOutOfResources	This counter represents the total number of times that Cisco CallManager attempted to allocate a video-streaming resource from one of the video conference bridge devices that is registered to Cisco CallManager when none was available.

Cisco CallManager Attendant Console

The Cisco CallManager Attendant Console (Cisco CallManager Attendant Console Server service) object provides information about the Cisco CallManager Attendant Console. Table 6-4 contains information about Cisco CallManager Attendant Console counters.

Table 6-4 Cisco CallManager Attendant Console

Counters	Counter Descriptions
CallsActive	Do not use this counter. Information in this counter may not accurately reflect the total number of active calls.
CallsRedirected	This counter represents the total number of redirected calls for a Cisco CallManager Attendant Console Server service. This number increases every time that a pilot point receives a call and redirects the call to a member of its hunt group.
CallsTotal	This counter represents the total number of all calls that have been made since the Cisco CallManager Attendant Console Server service started.
CcmLineLinkState	This counter represents the line state. Values include 0, 1, 10, or 11. A value of 0 indicates that the Cisco CallManager Attendant Console Server service has not registered or has not received line link state information from Cisco CallManager; 1 indicates that the Cisco CallManager Attendant Console Server service has registered and is receiving line link state information from Cisco CallManager; 10 indicates that the Cisco CallManager Attendant Console Server service has logged into CTI but has not registered or has not received line link state information from Cisco CallManager; 11 indicates that the Cisco CallManager Attendant Console Server service has logged into CTI and has registered and is receiving line link state information.
ClientsOnline	This counter represents the total number of Cisco CallManager attendant console clients that are currently online. Attendant Console clients include all users that are configured in the attendant console User Configuration window in Cisco CallManager Administration that are currently online. This number increases by one for each client that goes online and decreases by one for each client that goes offline.
ClientsRegistered	This counter represents the total number of registered clients for a Cisco CallManager Attendant Console Server service. This number increases by one for each new registration of a Cisco CallManager attendant console client when the client application logs in.
ClientsTotal	This counter represents the total number of Cisco CallManager Attendant Console clients that are currently registered with the Cisco CallManager Attendant Console Server service. Attendant console clients represent all users that are configured in the Attendant Console User Configuration window in Cisco CallManager Administration.

Table 6-4 Cisco CallManager Attendant Console (continued)

Counters	Counter Descriptions
HeartBeat	This counter represents the heartbeat of the Cisco CallManager Attendant Console Server service. This incremental count indicates that Cisco CallManager Attendant Console Server service is up and running. If the count does not increase, this means that the service is down.
LinesActive	Do not use this counter. Information in this counter may not accurately reflect the total number of active lines.
LinesIdle	Do not use this counter. Information in this counter may not accurately reflect the total number of idle lines.
LinesTotal	Do not use this counter. Information in this counter may not accurately reflect the total number of lines.
PilotPointsTotal	This counter represents the total number of pilot points that are configured in Cisco CallManager.
StartTime	This counter represents the time in milliseconds since the Cisco CallManager Attendant Console Server service started. The real-time clock in the computer, which is simply a reference point that indicates the current time and the time that has elapsed, in milliseconds, since the service started provides the basis for this time. The reference point specifies midnight, January 1, 1970.
Version	This counter represents the version of the Cisco CallManager Attendant Console Server service.

Cisco CallManager System Performance

The Cisco CallManager System Performance object provides system performance information about Cisco CallManager. Table 6-5 contains information about Cisco CallManager system performance counters.

Table 6-5 Cisco CallManager System Performance

Counters	Counter Descriptions
AverageExpectedDelay	This counter represents the current average expected delay before any incoming message gets handled.
CallsRejectedDueToCallThrottling	This counter represents the total number of calls that were rejected since the start of service due to call throttling.
CallThrottlingGenericCounter3	This counter represents a generic counter that is used for call-throttling purpose.
CodeRedEntryExit	This counter indicates whether Cisco CallManager has entered or exited a Code Red state (call-throttling mode). Valid values include 0 (Exit) and 1 (Entry).
CodeYellowEntryExit	This counter indicates whether Cisco CallManager has entered or exited a Code Yellow state (call-throttling mode). Valid values include 0 (Exit) and 1 (Entry).

Table 6-5 Cisco CallManager System Performance (continued)

Counters	Counter Descriptions
EngineeringCounter1	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter2	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter3	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter4	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter5	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter6	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter7	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter8	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
QueueSignalsPresent 1-High	This counter indicates the number of high-priority signals in the Cisco CallManager queue. High-priority signals include timeout events, internal Cisco CallManager keepalives, certain gatekeeper events, and internal process creation, among other events. A large number of high-priority events will cause degraded performance on Cisco CallManager and result in slow call connection or loss of dial tone. Use this counter in conjunction with the QueueSignalsProcessed 1-High counter to determine the processing delay on Cisco CallManager.
QueueSignalsPresent 2-Normal	This counter indicates the number of normal-priority signals in the Cisco CallManager queue. Normal-priority signals include call-processing functions, key presses, on-hook and off-hook notifications, among other events. A large number of normal-priority events will cause degraded performance on Cisco CallManager, sometimes resulting in delayed dial tone, slow call connection, or loss of dial tone. Use this counter in conjunction with the QueueSignalsProcessed 2-Normal counter to determine the call-processing delay on Cisco CallManager. Remember that high-priority signals must complete before normal-priority signals begin to process, so check the high-priority counters as well to get an accurate picture of the potential delay.

Table 6-5 Cisco CallManager System Performance (continued)

Counters	Counter Descriptions
QueueSignalsPresent 3-Low	This counter indicates the number of low-priority signals in the Cisco CallManager queue. Low-priority signals include station device registration (except the initial station registration request message), among other events. A large number of signals in this queue could result in delayed device registration, among other events.
QueueSignalsPresent 4-Lowest	This counter indicates the number of lowest priority signals in the Cisco CallManager queue. Lowest priority signals include the initial station registration request message during device registration, among other events. A large number of signals in this queue could result in delayed device registration, among other events.
QueueSignalsProcessed 1-High	This counter indicates the number of high-priority signals that Cisco CallManager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 1-High counter to determine the processing delay on this queue.
QueueSignalsProcessed 2-Normal	This counter indicates the number of normal-priority signals that Cisco CallManager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 2-Normal counter to determine the processing delay on this queue. Remember that high-priority signals get processed before normal-priority signals.
QueueSignalsProcessed 3-Low	This counter indicates the number of low-priority signals that Cisco CallManager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 3-Low counter to determine the processing delay on this queue. The number of signals processed gives an indication of how much device registration activity is being processed in this time interval.
QueueSignalsProcessed 4-Lowest	This counter indicates the number of lowest priority signals that Cisco CallManager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 4-Lowest counter to determine the processing delay on this queue. The number of signals that are processed gives an indication of how many devices began the Cisco CallManager registration process in this time interval.
QueueSignalsProcessed Total	This counter provides a sum total of all queue signals that Cisco CallManager processes for each 1-second period for all queue levels: high, normal, low, and lowest.
SkinnyDevicesThrottled	This counter represents the total number of Skinny devices that are being throttled. A Skinny device gets throttled (asked to shut down and reregister) when the total number of events that the Skinny device generated exceeds the configured maximum threshold value (default value specifies 2000 events) within a 5-second interval.

Table 6-5 Cisco CallManager System Performance (continued)

Counters	Counter Descriptions
ThrottlingSampleActivity	This counter indicates how many samples, out of the configured sample size, have non-zero averageExpectedDelay values. This counter gets reset when any sample has an averageExpectedDelay value of zero. This process repeats for each batch of samples. A batch represents the configured sample size.
TotalCodeYellowEntry	This counter indicates the number of times that Cisco CallManager call processing enters the code yellow state. This counter remains cumulative from the start of the Cisco CallManager process.

Cisco CTIManager

The Cisco CTI Manager object provides information about Cisco CTI Manager. Table 6-6 contains information about Cisco CTIManager counters.

Table 6-6 Cisco CTI Manager

Counters	Counter Descriptions
CcmLinkActive	This counter represents the total number of active Cisco CallManager links. CTI Manager maintains links to all active Cisco CallManagers in the cluster.
CTIConnectionActive	This counter represents the total number of CTI clients that are currently connected to the CTIManager. This counter increases by one when new connection is established and decreases by one when a connection is released. The CTIManager service parameter MaxCTIConnections determines the maximum number of active connections.
DevicesOpen	This counter represents the total number of devices that are configured in Cisco CallManager that CTI applications control and/or monitor. Devices include hardware IP phones, CTI ports, CTI route points, and so on.
LinesOpen	This counter represents the total number of lines that are configured in Cisco CallManager that control and/or monitor CTI applications.
QbeVersion	This counter represents the version number of the Quick Buffer Encoding (QBE) interface that the CTIManager uses.

Cisco Dual-Mode Mobility

The Cisco Dual-Mode Mobility object provides information about the dual-mode mobility application on Cisco CallManager. Table 6-7 contains information about Cisco Dual-Mode Mobility counters.

Table 6-7 Cisco Dual-Mode Mobility

Counters	Counter Descriptions
CallsAnchored	This counter represents the number of calls that are placed or received on dual-mode phones that are anchored in Cisco CallManager. The counter increments when a call is received from or placed to a dual-mode phone. The counter increments twice if a dual-mode phone calls another dual-mode phone.
DMMSRegistered	This counter represents the number of Dual-mode Mobile Station (DMMS) subscribers that are registered in the wireless LAN (WLAN).
FollowMeAborted	This counter represents the number of failed follow-me operations.
FollowMeAttempted	This counter represents the number of follow-me operations that Cisco CallManager attempted. The counter increments when a SIP 302 - Moved Temporarily message is received from the Wireless Service Manager (WSM) and Cisco CallManager redirects the call to the DMMS in WLAN.
FollowMeCompleted	This counter represents the number of follow-me operations that were successfully completed. The counter increments when the DMMS in WLAN answers the call and the media (voice path) is successfully established with the calling device.
FollowMeInProgress	This counter represents the number of follow-me operations that are currently in progress. The counter increments when a follow-me is attempted and it decrements when the follow-me operation is aborted or completed.
H1HandOutAttempted	This counter represents the number of H1 hand-out operations that dual-mode phones attempt. The counter increments when Cisco CallManager processes a call to the H1 number from a DMMS.
H1HandOutCompleted	This counter represents the number of successfully completed H1 hand-out operations The counter increments when the DMMS in WLAN successfully establishes a media (voice path).
H2HandOutCompleted	This counter represents the number of successfully completed H2 hand-out operations. The counter increments when the DMMS in WLAN successfully establishes a media (voice path).
H2HandOutsAttempted	This counter represents the number of H2 hand-out operations that dual-mode phones attempt. The counter increments when Cisco CallManager receives a call to the H2 number from a DMMS.
HandInAborted	This counter represents the number of hand-in operations that failed.
HandInAttempted	This counter represents the number of hand-in operations that dual-mode phones attempt.

Table 6-7 Cisco Dual-Mode Mobility (continued)

Counters	Counter Descriptions
HandInCompleted	This counter represents the number of successfully completed hand-in operations. The counter increments when the DMMS in WLAN successfully establishes a media (voice path).
HandInInProgress	This counter represents the number of hand-in operations that are currently in progress. The counter increments when a hand-in is attempted, and the counter decrements when the hand-in is aborted or completed.
Hand Out Aborted	This counter represents the number of hand-out operations that failed.
Hand Out In Progress	This counter represents the number of H1 and H2 hand-out operations that are currently in progress. The counter increments when a H1 or H2 hand-out is attempted, and it decrements when the hand-out is aborted or completed.

Cisco Extension Mobility

The Cisco Extension Mobility object provides information about the extension mobility application. Table 6-8 contains information about Cisco CallManager Extension Mobility counters.

Table 6-8 Cisco Extension Mobility Application

Counters	Counter Descriptions
RequestsHandled	This counter represents the total number of HTTP requests that the extension mobility application handled since the last restart of the Cisco CallManager service. A typical login would constitute two HTTP requests: one to query the initial login state of the device, and another to log in the user on a device. Similarly, a typical logout also results in two HTTP requests.
RequestsInProgress	This counter represents the number of HTTP requests that the extension mobility application currently is handling. A typical login would constitute two HTTP requests: one to query the initial login state of the device and another to log in the user on a device. Similarly, a typical logout also results in two HTTP requests.
Requests Throttled	This counter represents the total number of Login/Logout Requests that failed due to throttling.
Successful Logins	This counter represents the total number of successful login requests that were completed through EM Service.
Successful Logouts	This counter represents the total number of successful logout requests that were completed through EM Service
Total Attempted Login/Logout Requests	This counter represents the total number of Login and Logout requests that were attempted through this EM Service. This number includes both successful and unsuccessful attempts.

Cisco Gatekeeper

The Cisco Gatekeeper object provides information about registered Cisco gatekeeper devices. Table 6-9 contains information about Cisco gatekeeper device counters.

Table 6-9 Cisco Gatekeeper

Counters	Counter Descriptions
ACFsReceived	This counter represents the total number of RAS Admission Confirm messages that are received from the configured gatekeeper and its alternate gatekeepers.
ARQsAttempted	This counter represents the total number of RAS Admission Request messages that are attempted by using the configured gatekeeper and its alternate gatekeepers.
RasRetries	This counter represents the number of retries due to loss or delay of all RAS acknowledgement messages on the configured gatekeeper and its alternate gatekeepers.
VideoOutOfResources	This counter represents the total number of video-stream requests to the configured gatekeeper or its alternate gatekeepers that failed, most likely due to lack of bandwidth.

Cisco H.323

The Cisco H.323 object provides information about registered Cisco H.323 devices. Table 6-10 contains information about Cisco H.323 device counters.

Table 6-10 Cisco H.323

Counters	Counter Descriptions
CallsActive	This counter represents the number of streaming connections that are currently active (in use) on the configured H.323 device; in other words, the number of calls that actually have a voice path that is connected.
CallsAttempted	This counter represents the total number of calls that have been attempted on a device, including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the total number of successful calls that were made from a device.
CallsInProgress	This counter represents the number of calls that are currently in progress on a device.

Table 6-10 Cisco H.323 (continued)

Counters	Counter Descriptions
VideoCallsActive	This counter represents the number of video calls with video streaming connections that are currently active (in use) on all H.323 trunks that are registered with a Cisco CallManager; in other words, the number of calls that actually have video-streaming connections on a Cisco CallManager.
VideoCallsCompleted	This counter represents the number of video calls that were actually connected with video streams for all H.323 trunks that were registered with a Cisco CallManager. This number increases when the call terminates.

Cisco Hunt Lists

The Cisco Hunt Lists object provides information about the hunt lists that are defined in Cisco CallManager administration. Table 6-11 contains information about Cisco hunt list counters.

Table 6-11 Cisco Hunt Lists

Counters	Counter Descriptions
CallsAbandoned	This counter represents the number of abandoned calls that occurred through a hunt list. An abandoned call represents one in which a caller hangs up before the call is answered.
CallsActive	This counter represents the number of calls that are currently active (in use) that occurred through a hunt list. An active call represents one that gets distributed and answered, and to which a voice path connects.
CallsBusyAttempts	This counter represents the number of times that calls through a hunt list were attempted when all members of the line and/or route groups were busy.
CallsInProgress	This counter represents the number of calls that are currently in progress through a hunt list. A call in progress represents one that the Call Distributor is attempting to extend to a member of a line or route group and that has not yet been answered. Examples of a hunt list member include a line, a station device, a trunk device, or a port/channel of a trunk device.
CallsRingNoAnswer	This counter represents the total number of calls through a hunt list that rang but that called parties did not answer.

Table 6-11 Cisco Hunt Lists (continued)

Counters	Counter Descriptions
HuntListInService	This counter specifies whether the particular hunt list is currently in service. A value of 0 indicates that the hunt list is out of service; a value of 1 indicates that the hunt list is in service. A hunt list could be out of service because the hunt list is not running on a primary Cisco CallManager based on its Cisco CallManager Group or because the hunt list has been disabled in Cisco CallManager Administration.
MembersAvailable	This counter represents the total number of available or idle members of line and route groups that belong to an in-service hunt list. An available member currently handles a call and will accept a new call. An idle member does not handle any call and will accept a new call. A hunt list member can be a route group, line group, or a combination. A member of a line group represents a directory number of a line on an IP phone or a voice-mail port. A member of a route group represents a station gateway, a trunk gateway, or port/channel of a trunk gateway.

Cisco HW Conference Bridge Device

The Cisco HW Conference Bridge Device object provides information about registered Cisco hardware conference bridge devices. Table 6-12 contains information about Cisco hardware conference bridge device counters.

Table 6-12 Cisco HW Conference Bridge Device

Counters	Counter Descriptions
HWConferenceActive	This counter represents the number of conferences that are currently active (in use) on a HW conference bridge device. One resource represents one stream.
HWConferenceCompleted	This counter represents the total number of conferences that have been allocated and released on a HW conference device. A conference starts when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a conference resource from a HW conference device and failed, for example, because all resources were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (active) for this HW conference device.One resource represents one stream.

Table 6-12 Cisco HW Conference Bridge Device (continued)

Counters	Counter Descriptions
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used now for a HW conference device. One resource represents one stream.
ResourceTotal	This counter represents the total number of resources for a HW conference bridge device. This counter equals the sum of the counters ResourceAvailable and ResourceActive. One resource represents one stream.

Cisco IP Manager Assistant

The Cisco IP Manager Assistant (IPMA) Service object provides information about the Cisco IP Manager Assistant application. Table 6-13 contains information on Cisco IPMA counters.

Table 6-13 Cisco IP Manager Assistant Service

Counters	Counter Descriptions
AssistantsActive	This counter represents the number of assistant consoles that are currently active. An active assistant console exists when an assistant is logged in from his or her assistant console desktop application.
LinesOpen	This counter represents the number of phone lines that the Cisco IPMA application opened. An open phone line exists when the IPMA application assumes line control from CTI.
ManagersActive	This counter represents the current number of managers that the Cisco IPMA is servicing.
SessionsCurrent	This counter represents the total number of managers assistants that are currently using the Cisco IPMA application. Each manager and each assistant constitutes an active session, so for one manager/assistant pair, this counter would reflect two sessions.

Cisco Lines

The Cisco Lines object represents the number of Cisco lines (directory numbers) that can dial and connect to a device. Lines represent all directory numbers that terminate on an endpoint. The directory number that is assigned to it identifies the line. The Cisco Lines object does not include directory numbers that include wildcards such as a pattern for a Digital or Analog Access gateway.

The Active counter represents the state of the line, either active or not active. A zero indicates the line is not in use. When the number is greater than zero, this indicates that the line is active, and the number represents the number of calls that are currently in progress on that line. If more than one call is active, this indicates the call is on hold either because of being placed on hold specifically (user hold) or because of a network hold operation (for example, a transfer is in progress, and it is on transfer hold). This applies to all directory numbers that are assigned to any device.

Cisco Locations

The Cisco Location object provides information about locations that are defined in Cisco CallManager. Table 6-14 contains information on Cisco location counters.

Table 6-14 Cisco Locations

Counters	Counter Descriptions
BandwidthAvailable	This counter represents the current bandwidth in a given location. A value of 0 indicates that no bandwidth is available.
BandwidthMaximum	This counter represents the maximum bandwidth that is available in a given location. A value of 0 indicates that infinite bandwidth is available.
CallsInProgress	This counter represents the number of calls that are currently in progress on a particular Cisco CallManager.
OutOfResources	This counter represents the total number of times that a call on a particular Cisco CallManager through the location failed due to lack of bandwidth.
RSVP AudioReservationErrorCounts	This counter represents the number of RSVP reservation errors in the audio stream.
RSVP MandatoryConnectionsInProgress	This counter represents the number of connections with mandatory RSVP that are in progress.
RSVP OptionalConnectionsInProgress	This counter represents the number of connections with optional RSVP that are in progress.
RSVP TotalCallsFailed	This counter represents the number of total calls that failed due to a RSVP reservation failure.
RSVP VideoCallsFailed	This counter represents the number of video calls that failed due to a RSVP reservation failure.
RSVP VideoReservationErrorCounts	This counter represents the number of RSVP reservation errors in the video stream
VideoBandwidthAvailable	This counter represents the bandwidth that is currently available for video in the location where the person who initiated the video conference resides. A value of 0 indicates that no bandwidth is available.
VideoBandwidthMaximum	This counter represents the maximum bandwidth that is available for video in the location where the person who initiated the video conference resides. A value of 0 indicates that no bandwidth is allocated for video.
VideoOutOfResources	This counter represents the total number of failed video-stream requests (most likely due to lack of bandwidth) in the location where the person who initiated the video conference resides.

Cisco Media Streaming Application

The Cisco IP Voice Media Streaming Application object provides information about the registered MTPs, MOH servers, conference bridge servers, and annunciators. Table 6-15 contains information on Cisco IP Voice Media Streaming Application counters.

Note One object exists for each Cisco CallManager in the Cisco CallManager group that is associated with the device pool that the annunciator device is configured to use.

Table 6-15 Cisco Media Streaming Application

Counter	Counter Descriptions
ANNConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Media Streaming Application that a Cisco CallManager connection was lost.
ANNConnectionState	For each Cisco CallManager that is associated with an annunciator, this counter represents the current registration state to Cisco CallManager; 0 indicates no registration to Cisco CallManager; 1 indicates registration to the primary Cisco CallManager; 2 indicates connection to the secondary Cisco CallManager (connected to Cisco CallManager but not registered until the primary Cisco CallManager connection fails).
ANNConnectionsTotal	This counter represents the total number of annunciator instances that have been started since the Cisco IP Voice Media Streaming Application service started.
ANNInstancesActive	This counter represents the number of actively playing (currently in use) announcements.
ANNStreamsActive	This counter represents the total number of currently active simplex (one direction) streams for all connections. Each stream direction counts as one stream. One internal stream provides the audio input and another output stream to the endpoint device.
ANNStreamsAvailable	This counter represents the remaining number of streams that are allocated for the annunciator device that are available for use. This counter starts as 2 multiplied by the number of configured connections (defined in the Cisco IP Voice Media Streaming App service parameter for the Annunciator, Call Count) and is reduced by one for each active stream that started.
ANNStreamsTotal	This counter represents the total number of simplex (one direction) streams that connected to the annunciator device since the Cisco IP Voice Media Streaming Application service started.
CFBConferencesActive	This counter represents the number of active (currently in use) conferences.
CFBConferencesTotal	This counter represents the total number of conferences that started since the Cisco IP Voice Media Streaming Application service started.

Table 6-15 Cisco Media Streaming Application (continued)

Counter	Counter Descriptions
CFBConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Media Streaming Application that a Cisco CallManager connection was lost.
CFBConnectionState	For each Cisco CallManager that is associated with a SW Conference Bridge, this counter represents the current registration state to Cisco CallManager; 0 indicates no registration to Cisco CallManager; 1 indicates registration to the primary Cisco CallManager; 2 indicates connection to the secondary Cisco CallManager (connected to Cisco CallManager but not registered until the primary Cisco CallManager connection fails).
CFBStreamsActive	This counter represents the total number of currently active simplex (one direction) streams for all conferences. Each stream direction counts as one stream. In a three-party conference, the number of active streams equals 6.
CFBStreamsAvailable	This counter represents the remaining number of streams that are allocated for the conference bridge that are available for use. This counter starts as 2 multiplied by the number of configured connections (defined in the Cisco IP Voice Media Streaming App service parameter for Conference Bridge, Call Count) and is reduced by one for each active stream started.
CFBStreamsTotal	This counter represents the total number of simplex (one direction) streams that connected to the conference bridge since the Cisco IP Voice Media Streaming Application service started.
MOHAudioSourcesActive	This counter represents the number of active (currently in use) audio sources for this MOH server. Some of these audio sources may not be actively streaming audio data if no devices are listening. The exception exists for multicast audio sources, which will always be streaming audio. When an audio source is in use, even after the listener has disconnected, this counter will always have one input stream for each configured MOH codec. For unicast streams, the stream may exist in a suspended state where no audio data is received until a device connects to listen to the stream. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, then two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Media Streaming Application that a Cisco CallManager connection was lost.

Table 6-15 Cisco Media Streaming Application (continued)

Counter	Counter Descriptions
MOHConnectionState	For each Cisco CallManager that is associated with an MOH, this counter represents the current registration state to Cisco CallManager; 0 indicates no registration to Cisco CallManager; 1 indicates registration to the primary Cisco CallManager; 2 indicates connection to the secondary Cisco CallManager (connected to Cisco CallManager but not registered until the primary Cisco CallManager connection fails).
MOHStreamsActive	This counter represents the total number of active (currently in use) simplex (one direction) streams for all connections. One output stream exists for each device that is listening to a unicast audio source, and one input stream exists for each active audio source, multiplied by the number of MOH codecs. When an audio source has been used once, it will always have one input stream for each configured MOH codec. For unicast streams, the stream may exist in a suspended state where no audio data is received until a device connects to listen to the stream. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, then two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHStreamsAvailable	This counter represents the remaining number of streams that are allocated for the MOH device that are available for use. This counter starts as 408 plus the number of configured half-duplex unicast connections and is reduced by 1 for each active stream that started. The counter gets reduced by 2 for each multicast audio source, multiplied by the number of MOH codecs that are configured. The counter gets reduced by 1 for each unicast audio source, multiplied by the number of MOH codecs configured.
MOHStreamsTotal	This counter represents the total number of simplex (one direction) streams that have connected to the MOH server since the Cisco IP Voice Media Streaming Application service started.
MTPConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Streaming Application that a Cisco CallManager connection was lost.
MTPConnectionState	For each Cisco CallManager that is associated with an MTP, this counter represents the current registration state to Cisco CallManager; 0 indicates no registration to Cisco CallManager; 1 indicates registration to the primary Cisco CallManager; 2 indicates connection to the secondary Cisco CallManager (connected to Cisco CallManager but not registered until the primary Cisco CallManager connection fails).
MTPConnectionsTotal	This counter represents the total number of MTP instances that have been started since the Cisco IP Voice Media Streaming Application service started.

Table 6-15 Cisco Media Streaming Application (continued)

Counter	Counter Descriptions
MTPInstancesActive	This counter represents the number of active (currently in use) instances of MTP.
MTPStreamsActive	This counter represents the total number of currently active simplex (one direction) streams for all connections. Each stream direction counts as one stream.
MTPStreamsAvailable	This counter represents the remaining number of streams that are allocated for the MTP device that are available for use. This counter starts as 2 multiplied by the number of configured connections (defined in the Cisco IP Voice Media Streaming App service parameter for MTP, Call Count) and is reduced by one for each active stream started.
MTPStreamsTotal	This counter represents the total number of simplex (one direction) streams that connected to the MTP device since the Cisco IP Voice Media Streaming Application service started.

Cisco Messaging Interface

The Cisco Messaging Interface object provides information about the Cisco Messaging Interface (CMI) service. Table 6-16 contains information on Cisco Messaging Interface (CMI) counters.

Table 6-16 Cisco Messaging Interface

Counters	Counter Descriptions
HeartBeat	This counter represents the heartbeat of the CMI service. This incremental count indicates that the CMI service is up and running. If the count does not increase (increment), the CMI service is down.
SMDIMessageCountInbound	This counter represents the running count of inbound SMDI messages since the last restart of the CMI service.
SMDIMessageCountInbound24 Hour	This counter represents the rolling count of inbound SMDI messages in the last 24 hours.
SMDIMessageCountOutbound	This counter represents the running count of outbound SMDI messages since the last restart of the CMI service.
SMDIMessageCountOutbound24Hour	This counter represents the rolling count of outbound SMDI messages in the last 24 hours.
StartTime	This counter represents the time in milliseconds when the CMI service started. The real-time clock in the computer, which simply acts as a reference point that indicates the current time and the time that has elapsed, in milliseconds, since the service started, provides the basis for this time. The reference point specifies midnight, January 1, 1970.

Cisco MGCP FXO Device

The Cisco Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) Device object provides information about registered Cisco MGCP FXO devices. Table 6-17 contains information on Cisco MGCP FXO device counters.

Table 6-17 Cisco MGCP FXO Device

Counters	Counter Descriptions
CallsCompleted	This counter represents the total number of successful calls that were made from the port on an MGCP FXO device.
OutboundBusyAttempts	This counter represents the total number of times that a call through the port on this MGCP FXO device was attempted when no voice channels were available.
PortStatus	This counter represents the status of the FXO port associated with this MGCP FXO device.

Cisco MGCP FXS Device

The Cisco MGCP Foreign Exchange Station (FXS) Device object provides information about registered Cisco MGCP FXS devices. One instance of this object gets created for each port on a Cisco Catalyst 6000 24 port FXS Analog Interface Module gateway. For example, a fully configured Catalyst 6000 Analog Interface Module would represent 24 separate instances of this object. Table 6-18 contains information on Cisco MGCP FXS device counters.

Table 6-18 Cisco MGCP FXS Device

Counters	Counter Descriptions
CallsCompleted	This counter represents the total number of successful calls that were made from this port on the MGCP FXS device.
OutboundBusyAttempts	This counter represents the total number of times that a call through this port on the MGCP FXS device was attempted when no voice channels were available.
PortStatus	This counter represents the status of the FXS port that is associated with a MGCP FXS device.

Cisco MGCP Gateways

The Cisco MGCP Gateways object provides information about registered MGCP gateways. Table 6-19 contains information on Cisco MGCP gateway counters.

Table 6-19 Cisco MGCP Gateways

Counters	Counter Descriptions
BRIChannelsActive	This counter represents the number of BRI voice channels that are currently active in a call in the gateway
BRISpansInService	This counter represents the number of BRI spans that are currently available for use in the gateway.
FXOPortsActive	This counter represents the number of FXO ports that are currently active in a call in the gateway.
FXOPortsInService	This counter represents the number of FXO ports that are currently available for use in the gateway.
FXSPortsActive	This counter represents the number of FXS ports that are currently active in a call in the gateway.
FXSPortsInService	This counter represents the number of FXS ports that are currently available for use in the gateway.
PRIChannelsActive	This counter represents the number of PRI voice channels that are currently active in a call in the gateway.
PRISpansInService	This counter represents the number of PRI spans that are currently available for use in the gateway.
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are currently active in a call in the gateway.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently available for use in the gateway.

Cisco MGCP PRI Device

The Cisco MGCP Primary Rate Interface (PRI) Device object provides information about registered Cisco MGCP PRI devices. Table 6-20 contains information on Cisco MGCP PRI device counters.

Table 6-20 Cisco MGCP PRI Device

Counters	Counter Descriptions
CallsActive	This counter represents the number of calls that are currently active (in use) on this MGCP PRI device.
CallsCompleted	This counter represents the total number of successful calls that were made from this MGCP PRI device.

Table 6-20 Cisco MGCP PRI Device (continued)

Counters	Counter Descriptions
Channel 1 Status through Channel 15 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associated with a MGCP PRI device. Possible values: 0 (Unknown) indicates that the status of the channel could not be determined; 1 (Out of service) indicates that this channel is not available for use; 2 (Idle) indicates that this channel has no active call and is ready for use; 3 (Busy) indicates that an active call exists on this channel; 4 (Reserved) indicates that this channel has been reserved for use as a D-Channel or for use as a Synch-Channel for E-1.
Channel 16 Status	This counter represents the status of the indicated B-Channel that is associated with a MGCP PRI Device. Possible values: 0-Unknown, 1-Out of service, 2-Idle, 3-Busy, 4-Reserved, for an E1 PRI Interface, this channel is reserved for use as a D-Channel.
Channel 17 Status through Channel 31 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associated with the MGCP PRI Device. 0-Unknown, 1-Out of service, 2-Idle, 3-Busy, 4-Reserved.
DatalinkInService	This counter represents the state of the Data Link (D-Channel) on the corresponding digital access gateway. This value will be set to 1 (one) if the Data Link is up (in service) or 0 (zero) if the Data Link is down (out of service).
OutboundBusyAttempts	This counter represents the total number of times that a call through an MGCP PRI device was attempted when no voice channels were available.

Cisco MGCP T1 CAS Device

The Cisco MGCP T1 Channel Associated Signaling (CAS) Device object provides information about registered Cisco MGCP T1 CAS devices. Table 6-21 contains information on Cisco MGCP TI CAS device counters.

Table 6-21 Cisco MGCP T1 CAS Device

Counters	Counter Descriptions
CallsActive	This counter represents the number of calls that are currently active (in use) on this MGCP T1 CAS device.
CallsCompleted	This counter represents the total number of successful calls that were made from this MGCP T1 CAS device.

Table 6-21 Cisco MGCP T1 CAS Device (continued)

Counters	Counter Descriptions
Channel 1 Status through Channel 24 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associated with an MGCP T1 CAS device. Possible values: 0 (Unknown) indicates the status of the channel could not be determined; 1 (Out of service) indicates that this channel is not available for use; 2 (Idle) indicates that this channel has no active call and is ready for use; 3 (Busy) indicates that an active call exists on this channel; 4 (Reserved) indicates that this channel has been reserved for use as a D-Channel or for use as a Synch-Channel for E-1.
OutboundBusyAttempts	This counter represents the total number of times that a call through the MGCP T1 CAS device was attempted when no voice channels were available.

Cisco Music On Hold (MOH) Device

The Cisco Music On Hold (MOH) Device object provides information about registered Cisco MOH devices. Table 6-22 contains information on Cisco MOH device counters.

Table 6-22 Cisco MOH Device

Counters	Counter Descriptions
MOHHighestActiveResources	This counter represents the largest number of simultaneously active MOH connections for an MOH server. This number includes both multicast and unicast connections.
MOHMulticastResourceActive	This counter represents the number of currently active multicast connections to multicast addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHMulticastResourceAvailable	This counter represents the number of multicast MOH connections to multicast addresses that are served by an MOH server that are not active and are still available to be used now for the MOH server. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHOutOfResources	This counter represents the total number of times that the Media Resource Manager attempted to allocate an MOH resource when all available resources on all MOH servers that are registered with a Cisco CallManager were already active.

Table 6-22 Cisco MOH Device (continued)

Counters	Counter Descriptions
MOHTotalMulticastResources	This counter represents the total number of multicast MOH connections that are allowed to multicast addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHTotalUnicastResources	This counter represents the total number of unicast MOH connections that are allowed by an MOH server. Each MOH unicast resource uses one stream.
MOHUnicastResourceActive	This counter represents the number of active unicast MOH connections to an MOH server. Each MOH unicast resource uses one stream.
MOHUnicastResourceAvailable	This counter represents the number of unicast MOH connections that are not active and are still available to be used now for an MOH server. Each MOH unicast resource uses one stream.

Cisco MTP Device

The Cisco Media Termination Point (MTP) Device object provides information about registered Cisco MTP devices. Table 6-23 contains information on Cisco MTP device counters.

Table 6-23 Cisco MTP Device

Counters	Counter Descriptions
OutOfResources	This counter represents the total number of times that an attempt was made to allocate an MTP resource from an MTP device and failed; for example, because all resources were already in use.
ResourceActive	This counter represents the number of MTP resources that are currently in use (active) for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
ResourceAvailable	This counter represents the total number of MTP resources that are not active and are still available to be used now for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
ResourceTotal	This counter represents the total number of MTP resources that an MTP device provides. This counter equals the sum of the counters ResourceAvailable and ResourceActive.

Cisco Phones

The Cisco Phones object provides information about the number of registered Cisco IP Phones, including both hardware-based and other station devices.

The CallsAttempted counter represents the number of calls that have been attempted from this phone. This number increases each time that the phone goes off hook and on hook.

Cisco Presence Feature

The Cisco Presence object provides information about presence subscriptions, such as statistics that are related to the speed dial or call list Busy Lamp Field (BLF) subscriptions. Table 6-24 contains information on Cisco Presence feature.

Table 6-24 Cisco Presence

Counters	Counter Descriptions
ActiveCallListAndTrunkSubscriptions	This counter represents the active presence subscriptions for the call list feature as well as presence subscriptions through SIP trunk.
ActiveSubscriptions	This counter represents all active incoming and outgoing presence subscriptions.
CallListAndTrunkSubscriptionsThrottled	This counter represents the cumulative number of rejected call list and trunk side presence subscriptions due to throttling for the call list feature.
IncomingLineSideSubscriptions	This counter represents the cumulative number of presence subscriptions that were received on the line side.
IncomingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptions that were received on the trunk side.
OutgoingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptions that were sent on the trunk side.

Cisco QSIG Features

The Cisco QSIG Feature object provides information regarding the operation of various QSIG features, such as call diversion and path replacement. Table 6-25 contains information on the Cisco QSIG feature counters.

Table 6-25 Cisco QSIG

Counters	Counter Descriptions
CallForwardByRerouteCompleted	This counter represents the number of successful calls that has been forwarded by rerouting. Call forward by rerouting enables the path for a forwarded call to be optimized (minimizes the number of B-Channels in use) from the originator's perspective. This counter gets reset when the Cisco CallManager service parameter Call Forward by Reroute Enabled is enabled or disabled, or when the Cisco CallManager service restarts.
PathReplacementCompleted	This counter represents the number of successful path replacements that have occurred. Path replacement in a QSIG network optimizes the path between two edge PINX (PBXs) that are involved in a call. This counter resets when the Cisco CallManager service parameter Path Replacement Enabled is enabled or disabled, or when the Cisco CallManager service restarts.

Cisco SIP

The Cisco Session Initiation Protocol (SIP) object provides information about configured SIP devices. Table 6-26 contains information on the Cisco SIP counters.

Table 6-26 Cisco SIP

Counters	Counter Descriptions
CallsActive	This counter represents the number of calls that are currently active (in use) on this SIP device.
CallsAttempted	This counter represents the number of calls that have been attempted on this SIP device, including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the number of calls that were actually connected (a voice path was established) from a SIP device. This number increases when the call terminates.
CallsInProgress	This counter represents the number of calls that are currently in progress on a SIP device, including all active calls. When all calls that are in progress are connected, the number of CallsInProgress equals the number of CallsActive.

Table 6-26 Cisco SIP (continued)

Counters	Counter Descriptions
VideoCallsActive	This counter represents the number of video calls with streaming video connections that are currently active (in use) on this SIP device.
VideoCallsCompleted	This counter represents the number of video calls that were actually connected with video streams for this SIP device. This number increments when the call terminates.

Cisco SIP Stack

The Cisco SIP Stack object provides information about Session Initiation Protocol (SIP) stack statistics that are generated or used by SIP devices such as SIP Proxy, SIP Redirect Server, SIP Registrar, and SIP User Agent. Table 6-27 contains information on Cisco SIP Stack counters.

Table 6-27 Cisco SIP Stack

Counters	Counter Descriptions
AckIns	This counter represents the total number of ACK requests that the SIP device received.
AckOuts	This counter represents the total number of ACK requests that the SIP device sent.
ByeIns	This counter represents the total number of BYE requests that the SIP device received. This number includes retransmission.
ByeOuts	This counter represents the total number of BYE requests that the SIP device sent. This number includes retransmission.
CancelIns	This counter represents the total number of CANCEL requests that the SIP device received. This number includes retransmission.
CancelOuts	This counter represents the total number of CANCEL requests that the SIP device sent. This number includes retransmission.
GlobalFailedClassIns	This counter represents the total number of 6xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses indicates that a SIP device, which is providing a client function, received a failure response message. Generally, the responses indicate that a server had definitive information on a particular called party and not just the particular instance in the Request-URI.
GlobalFailedClassOuts	This counter represents the total number of 6xx class SIP responses that the SIP device sent. This number includes retransmission. This class of responses indicates that a SIP device, which is providing a client function, received a failure response message. Generally, the responses indicate that a server had definitive information on a particular called party and not just the particular instance in the Request-URI.

Table 6-27 Cisco SIP Stack (continued)

Counters	Counter Descriptions
InfoClassIns	This counter represents the total number of 1xx class SIP responses that the SIP device received. This includes retransmission. This class of responses provides information on the progress of a SIP request.
InfoClassOuts	This counter represents the total number of 1xx class SIP responses that the SIP device sent. This includes retransmission. This class of responses provides information on the progress of processing a SIP request.
InfoIns	This counter represents the total number of INFO requests that the SIP device has received. This number includes retransmission.
InfoOuts	This counter represents the total number of INFO requests that the SIP device has sent. This number includes retransmission.
InviteIns	This counter represents the total number of INVITE requests that the SIP device received. This number includes retransmission.
InviteOuts	This counter represents the total number of INVITE requests that the SIP device has sent. This number includes retransmission.
NotifyIns	This counter represents the total number of NOTIFY requests that the SIP device has received. This number includes retransmission.
NotifyOuts	This counter represents the total number of NOTIFY requests that the SIP device has sent. This number includes retransmission.
OptionsIns	This counter represents the total number of OPTIONS requests that the SIP device received. This number includes retransmission.
OptionsOuts	This counter represents the total number of OPTIONS requests that the SIP device has sent. This number includes retransmission.
PRAckIns	This counter represents the total number of PRACK requests that the SIP device has received. This number includes retransmission.
PRAckOuts	This counter represents the total number of PRACK requests that the SIP device has sent. This number includes retransmission.
RedirClassIns	This counter represents the total number of 3xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses provides information about redirections to addresses where the callee may be reachable.
RedirClassOuts	This counter represents the total number of 3xx class SIP responses that the SIP device has sent. This number includes retransmission. This class of responses provides information about redirections to addresses where the callee may be reachable.
ReferIns	This counter represents the total number of REFER requests that the SIP device has received. This number includes retransmission.
ReferOuts	This counter represents the total number of REFER requests that the SIP device has sent. This number includes retransmission.
RegisterIns	This counter represents the total number of REGISTER requests that the SIP device has received. This number includes retransmission.

Table 6-27 Cisco SIP Stack (continued)

Counters	Counter Descriptions
RegisterOuts	This counter represents the total number of REGISTER requests that the SIP device has sent. This number includes retransmission.
RequestsFailedClassIns	This counter represents the total number of 4xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses indicates a request failure by a SIP device that is providing a client function.
RequestsFailedClassOuts	This counter represents the total number of 4xx class SIP responses that the SIP device has sent. This number includes retransmission. This class of responses indicates a request failure by a SIP device that is providing a client function.
RetryByes	This counter represents the total number of BYE retries that the SIP device has sent. To determine the number of first BYE attempts, subtract the value of this counter from the value of the sipStatsByeOuts counter.
RetryCancels	This counter represents the total number of CANCEL retries that the SIP device has sent. To determine the number of first CANCEL attempts, subtract the value of this counter from the value of the sipStatsCancelOuts counter.
RetryInfo	This counter represents the total number of INFO retries that the SIP device has sent. To determine the number of first INFO attempts, subtract the value of this counter from the value of the sipStatsInfoOuts counter.
RetryInvites	This counter represents the total number of INVITE retries that the SIP device has sent. To determine the number of first INVITE attempts, subtract the value of this counter from the value of the sipStatsInviteOuts counter.
RetryNotify	This counter represents the total number of NOTIFY retries that the SIP device has sent. To determine the number of first NOTIFY attempts, subtract the value of this counter from the value of the sipStatsNotifyOuts counter.
RetryPRAck	This counter represents the total number of PRACK retries that the SIP device has sent. To determine the number of first PRACK attempts, subtract the value of this counter from the value of the sipStatsPRAckOuts counter.
RetryRefer	This counter represents the total number of REFER retries that the SIP device has sent. To determine the number of first REFER attempts, subtract the value of this counter from the value of the sipStatsReferOuts counter.
RetryRegisters	This counter represents the total number of REGISTER retries that the SIP device has sent. To determine the number of first REGISTER attempts, subtract the value of this counter from the value of the sipStatsRegisterOuts counter.
RetryRel1xx	This counter represents the total number of Reliable 1xx retries that the SIP device has sent.

Table 6-27 Cisco SIP Stack (continued)

Counters	Counter Descriptions
RetryResponsesFinal	This counter represents the total number of Final Response retries that the SIP device has sent.
RetryResponsesNonFinal	This counter represents the total number of non-Final Response retries the SIP device has sent.
RetrySubscribe	This counter represents the total number of SUBSCRIBE retries that the SIP device has sent. To determine the number of first SUBSCRIBE attempts, subtract the value of this counter from the value of the sipStatsSubscribeOuts counter.
RetryUpdate	This counter represents the total number of UPDATE retries that the SIP device has sent. To determine the number of first UPDATE attempts, subtract the value of this counter from the value of the sipStatsUpdateOuts counter.
ServerFailedClassIns	This counter represents the total number of 5xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses indicates that failure responses were received by a SIP device that is providing a client function.
ServerFailedClassOuts	This counter represents the total number of 5xx class SIP responses that the SIP device has sent. This number includes retransmission. This class of responses indicates that failure responses were received by a SIP device that is providing a client function.
StatusCode1xxIns	This counter represents the total number of 1xx response messages, including retransmission, that the SIP device has received. This count includes the following 1xx responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress
StatusCode1xxOuts	This counter represents the total number of 1xx response messages, including retransmission, that the SIP device has sent. This count includes the following 1xx responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress

Table 6-27 Cisco SIP Stack (continued)

Counters	Counter Descriptions
StatusCode2xxIns	This counter represents the total number of 2xx response messages, including retransmission, that the SIP device has received. This count includes the following 2xx responses: • 200 OK • 202 Success Accepted
StatusCode2xxOuts	This counter represents the total number of 2xx response messages, including retransmission, that the SIP device has sent. This count includes the following 2xx responses: • 200 OK • 202 Success Accepted
StatusCode3xxins	This counter represents the total number of 3xx response messages, including retransmission, that the SIP device has received. This count includes the following 3xx responses: • 300 Multiple Choices • 301 Moved Permanently • 302 Moved Temporarily • 303 Incompatible Bandwidth Units • 305 Use Proxy • 380 Alternative Service
StatusCode302Outs	This counter represents the total number of 302 Moved Temporarily response messages, including retransmission, that the SIP device has sent.

Table 6-27 Cisco SIP Stack (continued)

Counters	Counter Descriptions
StatusCode4xxIns	This counter represents the total number of 4xx response messages, including retransmission, that the SIP device has received. This count includes the following 4xx responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending

Table 6-27 Cisco SIP Stack (continued)

Counters	Counter Descriptions
StatusCode4xxOuts	This counter represents the total number of 4xx response messages, including retransmission, that the SIP device has sent. This count includes the following 4xx responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending

Table 6-27 Cisco SIP Stack (continued)

Counters	Counter Descriptions
StatusCode5xxIns	This counter represents the total number of 5xx response messages, including retransmission, that the SIP device has received. This count includes the following 5xx responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed
StatusCode5xxOuts	This counter represents the total number of 5xx response messages, including retransmission, that the SIP device has sent. This count includes the following 5xx responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed
StatusCode6xxIns	This counter represents the total number of 6xx response messages, including retransmission, that the SIP device has received. This count includes the following 6xx responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
StatusCode6xxOuts	This counter represents the total number of 6xx response messages, including retransmission, that the SIP device has sent. This count includes the following 6xx responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
SubscribeIns	This counter represents the total number of SUBSCRIBE requests that the SIP device has received. This number includes retransmission.

Table 6-27 Cisco SIP Stack (continued)

Counters	Counter Descriptions
SubscribeOuts	This counter represents the total number of SUBSCRIBE requests that the SIP device has sent. This number includes retransmission.
SuccessClassIns	This counter represents the total number of 2xx class SIP responses that the SIP device has received. This includes retransmission. This class of responses provides information on the successful completion of a SIP request.
SuccessClassOuts	This counter represents the total number of 2xx class SIP responses that the SIP device has sent. This includes retransmission. This class of responses provides information on the successful completion of a SIP request.
SummaryRequestsIn	This counter represents the total number of SIP request messages that have been received by the SIP device. This number includes retransmissions.
SummaryRequestsOut	This counter represents the total number of SIP request messages that the device sent. This number includes messages that originate on the device and messages that are being relayed by the device. When a particular message gets sent more than once, each transmission gets counted separately; for example, a message that is re-sent as a retransmission or as a result of forking.
SummaryResponsesIn	This counter represents the total number of SIP response messages that the SIP device received. This number includes retransmission.
SummaryResponsesOut	This counter represents the total number of SIP response messages that the SIP device sent (originated and relayed). This number includes retransmission.
UpdateIns	This counter represents the total number of UPDATE requests that the SIP device has received. This number includes retransmission.
UpdateOuts	This counter represents the total number of UPDATE requests that the SIP device has sent. This number includes retransmission.

Cisco SW Conf Bridge Device

The Cisco SW Conference Bridge Device object provides information about registered Cisco software conference bridge devices. Table 6-28 contains information on the Cisco software conference bridge device counters.

Table 6-28 Cisco SW Conf Bridge Device

Counters	Counter Descriptions
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a conference resource from a SW conference device and failed because all resources were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (active) for a SW conference device. One resource represents one stream.

Table 6-28 Cisco SW Conf Bridge Device (continued)

Counters	Counter Descriptions
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used now for a SW conference device. One resource represents one stream.
ResourceTotal	This counter represents the total number of conference resources that a SW conference device provides. One resource represents one stream.This counter equals the sum of the ResourceAvailable and ResourceActive counters.
SWConferenceActive	This counter represents the number of software-based conferences that are currently active (in use) on a SW conference device.
SWConferenceCompleted	This counter represents the total number of conferences that have been allocated and released on a SW conference device. A conference starts when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.

Cisco TFTP Server

The Cisco Trivial File Transfer Protocol (TFTP) Server object provides information about the Cisco TFTP server. Table 6-29 contains information on Cisco TFTP server counters.

Table 6-29 Cisco TFTP Server

Counters	Counter Descriptions
BuildAbortCount	This counter represents the number of times that the build process aborted when it received a Build all request. This counter increases when building of device/unit/softkey/dialrules gets aborted as a result of group level change notifications.
BuildCount	This counter represents the number of times since the TFTP service started that the TFTP server has built all the configuration files in response to a database change notification that affects all devices. This counter increases by one every time the TFTP server performs a new build of all the configuration files.
BuildDeviceCount	This counter represents the number of devices that were processed in the last build of all the configuration files. This counter also updates while processing device change notifications. The counter increases when a new device is added and decreases when an existing device is deleted.
BuildDialruleCount	This counter represents the number of dial rules that were processed in the last build of the configuration files. This counter also updates while processing dial rule change notifications. The counter increases when a new dial rule is added and decreases when an existing dial rule is deleted.
BuildDuration	This counter represents the time in seconds that it took to build the last of all the configuration files.

Table 6-29 Cisco TFTP Server (continued)

Counters	Counter Descriptions
BuildSignCount	This counter represents the number of security-enabled phone devices for which the configuration file was digitally signed with the Cisco CallManager server key in the last build of all the configuration files. This counter also updates while processing security-enabled phone device change notifications.
BuildSoftKeyCount	This counter represents the number of softkeys that were processed in the last build of the configuration files. This counter increments when a new softkey is added and decrements when an existing softkey is deleted.
BuildUnitCount	This counter represents the number of gateways that were processed in the last build of all the configuration files. This counter also updates while processing unit change notifications. The counter increases when a new gateway is added and decreases when an existing gateway is deleted.
ChangeNotifications	This counter represents the total number of all the Cisco CallManager database change notifications that the TFTP server received. Each time that a device configuration is updated in Cisco CallManager Administration, the TFTP server gets sent a database change notification to rebuild the XML file for the updated device.
DeviceChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete configuration files for devices.
DialruleChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete configuration files for dial rules.
EncryptCount	This counter represents the number of configuration files that were encrypted. This counter gets updated each time a configuration file is successfully encrypted
GKFoundCount	This counter represents the number of GK files that were found in the cache. This counter gets updated each time a GK file is found in the cache
GKNotFoundCount	This counter represents the number of GK files that were not found in the cache. This counter gets updated each time a request to get a GK file results in the cache not finding it
HeartBeat	This counter represents the heartbeat of the TFTP server. This incremental count indicates that the TFTP server is up and running. If the count does not increase, this means that the TFTP server is down.
HttpConnectRequests	This counter represents the number of clients that are currently requesting the HTTP GET file request.

Table 6-29 Cisco TFTP Server (continued)

Counters	Counter Descriptions
HttpRequests	This counter represents the total number of file requests (such as requests for XML configuration files, phone firmware files, audio files, and so on.) that the HTTP server handled. This counter represents the sum total of the following counters since the HTTP service started: RequestsProcessed, RequestsNotFound, RequestsOverflow, RequestsAborted, and RequestsInProgress.
HttpRequestsAborted	This counter represents the total number of HTTP requests that the HTTP server. canceled (aborted) unexpectedly. Requests could get aborted if the requesting device cannot be reached (for instance, the device lost power) or if the file transfer was interrupted due to network connectivity problems.
HttpRequestsNotFound	This counter represents the total number of HTTP requests where the requested file was not found. When the HTTP server does not find the requested file, a message gets sent to the requesting device.
HttpRequestsOverflow	This counter represents the total number of HTTP requests that were rejected when the maximum number of allowable client connections was reached. The requests may have arrived while the TFTP server was building the configuration files or because of some other resource limitation. The Cisco TFTP advanced service parameter, Maximum Serving Count, sets the maximum number of allowable connections.
HttpRequestsProcessed	This counter represents the total number of HTTP requests that the HTTP server. successfully processed.
HttpServedFromDisk	This counters represents the number of requests that the HTTP server completed with the files that are on disk and not cached in memory.
LDFoundCount	This counter represents the number of LD files that were found in the cache. This counter gets updated each time a LD file is found in cache memory.
LDNotFoundCount	This counter represents the number of LD files that were not found in cache memory. This counter gets updated each time a request to get an LD file results in the cache not finding it.
MaxServingCount	This counter represents the maximum number of client connections that the TFTP can serve simultaneously. The Cisco TFTP advanced service parameter, Maximum Serving Count, sets this value.
Requests	This counter represents the total number of file requests (such as requests for XML configuration files, phone firmware files, audio files, and so on.) that the TFTP server handles. This counter represents the sum total of the following counters since the TFTP service started: RequestsProcessed, RequestsNotFound, RequestsOverflow, RequestsAborted, and RequestsInProgress.
RequestsAborted	This counter represents the total number of TFTP requests that the TFTP server canceled (aborted) unexpectedly. Requests could be aborted if the requesting device cannot be reached (for instance, the device lost power) or if the file transfer was interrupted due to network connectivity problems.

Table 6-29 Cisco TFTP Server (continued)

Counters	Counter Descriptions
RequestsInProgress	This counter represents the number of file requests that the TFTP server currently is processing. This counter increases for each new file request and decreases for each file request that is completed. This counter indicates the current load of the TFTP server.
RequestsNotFound	This counter represents the total number of TFTP requests where the requested file was not found. When the TFTP server does not find the requested file, a message gets sent to the requesting device.
RequestsOverflow	This counter represents the total number of TFTP requests that were rejected because the maximum number of allowable client connections was exceeded, because requests arrived while the TFTP server was building the configuration files, or because of some other resource limitation. The Cisco TFTP advanced service parameter, Maximum Serving Count, sets the maximum number of allowable connections.
RequestsProcessed	This counter represents the total number of TFTP requests that the TFTP server successfully processed.
SegmentsAcknowledged	This counter represents the total number of data segments that the client devices acknowledged. Files get sent to the requesting device in data segments of 512 bytes, and for each 512-byte segment, the device sends the TFTP server an acknowledgment message. Each additional data segment gets sent upon receipt of the acknowledgment for the previous data segment until the complete file is successfully transmitted to the requesting device.
SegmentsFromDisk	This counter represents the number of data segments that the TFTP server reads from the files on disk, while serving files.
SegmentSent	This counter represents the total number of data segments that the TFTP server sent. Files get sent to the requesting device in data segments of 512 bytes.
SEPFoundCount	This counter represents the number of SEP files that were successfully found in the cache. This counter gets updated each time a SEP file is found in the cache.
SEPNotFoundCount	This counter represents the number of SEP files that were not found in the cache. This counter gets updated each time a request to get a SEP file produces a not found in cache memory result.
SIPFoundCount	This counter represents the number of SIP files that were successfully found in the cache. This counter gets updated each time a SIP file is found in the cache
SIPNotFoundCount	This counter represents the number of SIP files that were not found in the cache. This counter gets updated each time a request to get a SIP file produces a not found in cache memory result.

Table 6-29 Cisco TFTP Server (continued)

Counters	Counter Descriptions
SoftkeyChangeNotifications	This counter represents the number of times that the TFTP server has received database change notification to create, update, or delete configuration files for softkeys.
UnitChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete gateway-related configuration files.

Cisco Tomcat Connector

The Tomcat Hypertext Transport Protocol (HTTP)/HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco CallManager related web pages are accessed. The Secure Socket Layer (SSL) status of the URLs for web applications provides the basis for the instance name for each Tomcat HTTP Connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL. Table 6-30 contains information on the Tomcat HTTP connector counters.

Table 6-30 Cisco Tomcat Connector

Counters	Counter Description
Errors	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that the connector encountered. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
MBytesReceived	This counter represents the amount of data that the connector received. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector.For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

Table 6-30 Cisco Tomcat Connector (continued)

Counters	Counter Description
MBytesSent	This counter represents the amount of data that the connector sent. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
Requests	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that the connector encountered. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco CallManager related windows s are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
Threads Total	This counter represents the connectors current total number of request processing threads, including available and in-use threads. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
Threads Max	This counter represents the connector's maximum number of request processing threads. Each incoming request on a Cisco CallManager related window requires a thread for the duration of that request. If more simultaneous requests are received than the currently available request processing threads can handle, additional threads will be created up to the configured maximum shown in this counter. If still more simultaneous requests are received, they accumulate within the server socket that the connector created, up to an internally specified maximum number. Any further simultaneous requests will receive connection refused messages until resources are available to process them. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The Connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

Cisco Tomcat JVM

The Cisco Tomcat Java Virtual Machine (JVM) object provides information about the Tomcat JVM, which represents, among other things, a pool of common resource memory that Cisco CallManager related web applications such as Cisco CallManager Administration, Cisco CallManager Serviceability, and more use. Table 6-31 contains information on the Tomcat JVM counters.

Table 6-31 Tomcat JVM

Counters	Counter Description
KBytes Memory Free	This counter represents the amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco CallManager Administration and Cisco CallManager Serviceability create. When the amount of free dynamic memory is low, more memory gets automatically allocated, and total memory size (represented by the KbytesMemoryTotal counter) increases but only up to the maximum (represented by the KbytesMemoryMax counter). You can determine the amount of memory in use by subtracting KBytesMemoryFree from KbytesMemoryTotal.
KBytes Memory Max	This counter represents the amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco CallManager Administration and Cisco CallManager Serviceability create. When the amount of free dynamic memory is low, more memory gets automatically allocated, and total memory size (represented by the KbytesMemoryTotal counter) increases but only up to the maximum (represented by the KbytesMemoryMax counter). You can determine the amount of memory in use by subtracting KBytesMemoryFree from KbytesMemoryTotal.
KBytes Memory Total	This counter represents the Tomcat Java Virtual Machine's current total dynamic memory block size including free and in-use memory.

Cisco Tomcat Web Application

The Cisco Tomcat Web Application object provides information about how to running Cisco CallManager web applications. The URLs for the web application provide basis for the instance name for each Tomcat Web Application. For example, Cisco CallManager Administration (https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco CallManager Serviceability gets identified by ccmservice, Cisco CallManager User Options gets identified by ccmuser, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root. Table 6-32 contains information on the Tomcat Web Application counters.

Table 6-32 Tomcat Web Application

Counters	Counter Description
Errors	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that a Cisco CallManager related web application encountered. The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Cisco CallManager Administration (https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco CallManager Serviceability gets identified by ccmservice, Cisco CallManager User Options gets identified by ccmuser, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root.
Requests	This counter represents the total number of requests that the web application handles. Each time that a web application is accessed, its Requests counter increments accordingly. The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Cisco CallManager Administration (https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco CallManager Serviceability gets identified by ccmservice, Cisco CallManager User Options gets identified by ccmuser, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root.
Sessions Active	This counter represents the number of sessions that the web application currently has active (in use). The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Cisco CallManager Administration (https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco CallManager Serviceability gets identified by ccmservice, Cisco CallManager User Options gets identified by ccmuser, and URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), get identified by _root.

Cisco Transcode Device

The Cisco Transcode Device object provides information about registered Cisco transcoding devices. Table 6-33 contains information on Cisco transcoder device counters.

Table 6-33 Cisco Transcode Device

Counters	Counter Descriptions
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a transcoder resource from a transcoder device and failed; for example, because all resources were already in use.
ResourceActive	This counter represents the number of transcoder resources that are currently in use (active) for a transcoder device. Each transcoder resource uses two streams.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used now for a transcoder device. Each transcoder resource uses two streams.
ResourceTotal	This counter represents the total number of transcoder resources that a transcoder device provided. This counter equals the sum of the counters ResourceActive and ResourceAvailable.

Cisco Video Conference Bridge

The Cisco Video Conference Bridge object provides information about registered Cisco video conference bridge devices. Table 6-34 contains information on Cisco video conference bridge device counters.

Table 6-34 Cisco Video Conference Bridge

Counters	Counter Descriptions
ConferenceActive	This counter represents the total number of video conferences that are currently active (in use) on a video conference bridge device. The system specifies a conference as active when the first call connects to the bridge.
ConferenceAvailable	This counter represents the number of video conferences that are not active and are still available on a video conference device.
ConferenceCompleted	This counter represents the total number of video conferences that have been allocated and released on a video conference device. A conference starts when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
ConferenceTotal	This counter represents the total number of video conferences that are configured for a video conference device.

Table 6-34 Cisco Video Conference Bridge (continued)

Counters	Counter Descriptions
OutOfConferences	This counter represents the total number of times an attempt was made to initiate a video conference from a video conference device and failed because the device already had the maximum number of active conferences allowed (as specified by the TotalConferences counter).
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a conference resource from a video conference device and failed, for example, because all resources were already in use.
ResourceActive	This counter represents the total number of resources that are currently active (in use) on a video conference bridge device. One resource gets used per participant.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available on a device to handle additional participants for a video conference bridge device.
ResourceTotal	This counter represents the total number of resources that are configured on a video conference bridge device. One resource gets used per participant.

Cisco WebDialer

The Cisco WebDialer object provides information about the Cisco WebDialer application and the Redirector servlet. Table 6-35 contains information on the Cisco WebDialer counters.

Table 6-35 Cisco WebDialer

Counters	Counter Descriptions
CallsCompleted	This counter represents the number of Make Call and End Call requests that the Cisco WebDialer application successfully completed.
CallsFailed	This counter represents the number of Make Call and End Call requests that were unsuccessful.
RedirectorSessionsHandled	This counter represents the total number of HTTP sessions that the Redirector servlet handled since the last service startup.
RedirectorSessionsInProgress	This counter represents the number of HTTP sessions that are currently being serviced by the Redirector servlet.
RequestsCompleted	This counter represents the number of Make Call and End Call requests that the WebDialer servlet has successfully completed.
RequestsFailed	This counter represents the number of Make Call and End Call requests that failed.
SessionsHandled	This counter represents the total number of CTI sessions that the Cisco WebDialer servlet handled since the last service startup.
SessionsInProgress	This counter represents the number of CTI sessions that the Cisco WebDialer servlet is currently servicing.

Cisco WSM Connector

The WSM object provides information on WSMConnectors that are configured on Cisco CallManager. . Each WSMConnector represents a physical Motrola WSM device. Table 6-36 contains information on the Cisco WSM Connector counters.

Table 6-36 Cisco WSM Connector

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use) on the WSMConnector device.
CallsAttempted	This counter represents the number of calls that have been attempted on the WSMConnector device, including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the number of calls that are connected (a voice path was established) through the WSMConnector device. The counter increments when the call terminates.
CallsInProgress	This counter represents the number of calls that are currently in progress on the WSMConnector device. This includes all active calls. When the number of CallsInProgress equals the number of CallsActive, this indicates that all calls are connected.
DMMSRegistered	This counter represents the number of DMMS subscribers that are registered to the WSM.

Database Change Notification Client

The Database Change Notification Client object provides information on change notification clients. Table 6-37 contains information on the Database Change Notification Client counters.

Table 6-37 Database Change Notification Client

Counters	Counter Descriptions
MessagesProcessed	This counter represents the number of database change notifications that have been processed.
MessagesProcessing	This counter represents the number of change notification messages that are currently being processed or are waiting to be processed in the change notification queue for this client.
QueueHeadPointer	This counter represents the head pointer to the change notification queue. The head pointer acts as the starting point in the change notification queue. To determine the number of notifications in the queue, subtract the tail pointer value from the head pointer value. By default, this counter refreshes every 15 seconds.
QueueMax	This counter represents the largest number of change notification messages that will be processed for this client.

Table 6-37 Database Change Notification Client (continued)

Counters	Counter Descriptions
QueueTailPointer	This counter represents the tail pointer to the change notification queue. The tail pointer represents the ending point in the change notification queue. To determine the number of notifications in the queue, subtract the tail pointer value from the head pointer value. By default, this counter refreshes every 15 seconds
TablesSubscribed	This counter represents the number of tables in which this client has subscribed.

Database Change Notification Server

The Database Change Notification Server object provides information on different change-notification-related statistics. Table 6-37 contains information on the Database Change Notification Server counters.

Table 6-38 Database Change Notification Server

Counter	Counter Descriptions
Clients	This counter represents the number of change notification clients (services/servlets) that have subscribed for change notification.
QueuedRequestsInDB	This counter represents the number of change notification records that are in the DBCNQueue (Database Change Notification Queue) table via direct TCP/IP connection (not queued in shared memory). This counter refreshes every 15 seconds.
QueuedRequestsInMemory	This counter represents the number of change notification requests that are queued in the DBCNQueue (Database Change Notification Queue) table in shared memory (rather than via direct TCP/IP connection).

Database Change Notification Subscription

The Database Change Notification Subscription object displays the names of tables where the client will receive Change Notifications.

The SubscribedTable object displays the database table with the service or servlet that will receive change notifications. Because the counter does not increment, this display occurs for informational purposes only

Database Layer Monitor

The Database Layer object collects information on the Cisco CallManager database as the Cisco Database Layer Monitor collects it.

The Cisco Database Layer Monitor service has responsibility for device resets. The ResetsQueued counter represents the number of records with devices that are currently resetting or queued to be reset. The counter only includes the resets that administrators invoke when they click on the Reset button on the device configuration window.

Database Local DSN

The Database Local Data Source Name (DSN) object and LocalDSN counter provide the DSN information for the local machine. Table 6-39 contains information on the Database local DSN.

Table 6-39 Database Local Data Source Name

Counters	Counter Descriptions
CcmDbSpace_Used	This counter represents the amount of CcmDbSpace that is being consumed
CcmtempDbSpace_Used	This counter represents the amount of CcmtempDbSpace that is being consumed.
LocalDSN	This counter represents the DSN that is being referenced from the local machine.
RootDbSpace_Used	This counter represents the amount of RootDbSpace that is being consumed.

DB User Host Information Counters

The DB User Host Information object provides information on DB User Host.

The DB:User:Host Instance object displays the number of connections that are present for each instance of DB:User:Host.

Enterprise Replication DBSpace Monitors

The enterprise replication DBSpace monitors object displays the usage of various ER DbSpaces. Table 6-40 contains information on the enterprise replication DB monitors.

Table 6-40 Enterprise Replication DBSpace Monitors

Counters	Counter Descriptions
ERDbSpace_Used	This counter represents the amount of ERDbSpace that was consumed.
ERSBDbSpace_Used	This counter represents the amount of ERSBDbSpace that was consumed.

Enterprise Replication Perfmon Counters

The Enterprise Replication Perfmon Counter object provides information on the various replication counters.

The ServerName:ReplicationQueueDepth counter displays information on the Q parameter.

IP

The IP object provides information on the IP statistics on your system. Table 6-41 contains information on the IP counters.

Table 6-41 IP

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated.
Frag Fails	This counter represents the number of IP datagrams that were discarded at this entity because the datagrams could not be fragmented, such as datagrams where the Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that were successfully fragmented at this entity.
In Delivers	This counter represents the number of input datagrams that were delivered to IP user protocols (including ICMP).
In Discards	This counter represents the number of input datagrams without errors that were discarded. This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	This counter represents the number of input datagrams with header errors that were discarded. This includes bad checksums, version number mismatch, other format errors, time-to-live exceeded, and other errors that were discovered in processing their IP options.
In Receives	This counter represents the number of input datagrams that were received. This counter includes datagrams that were received with errors
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	This counter represents the number of incoming IP datagrams that were received and the number of outgoing IP datagrams that were requested.
Out Discards	This counter represents the number of output IP datagrams that were not transmitted and were discarded. Lack of buffer space provides one possible reason.
Out Requests	This counter represents the number of IP datagrams that were requested by local IP user protocols (including ICMP) to IP requesting transmission.
Reasm Fails	This counter represents the number of IP reassembly failures that the IP reassembly algorithm detected.
Reasm OKs	This counter represents the number of IP datagrams that were successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments that were received that required reassembly.

Memory

The memory object provides information about the usage of physical memory and swap memory on the server. Table 6-42 contains information on memory counters.

Table 6-42 Memory

Counters	Counter Descriptions
% Mem Used	This counter displays the system physical memory utilization as a percentage.
% Page Usage	This counter represents the percentage of active pages.
% VM Used	This counter displays the system virtual memory utilization as a percentage.
Buffered KBytes	This counter represents the capacity of buffers in your system in kilobytes.
Cached KBytes	This counter represents the amount of cached memory in kilobytes.
Free KBytes	This counter represents the total amount of memory that is available in your system in kilobytes.
Free Swap KBytes	This counter represents the amount of free swap space that is available in your system in kilobytes.
Pages	This counter represents the number of pages that the system paged in from the disk plus the number of pages that the system paged out to the disk.
Pages Input	This counter represents the number of pages that the system paged in from the disk.
Pages Output	This counter represents the number of pages that the system paged out to the disk.
Shared KBytes	This counter represents the amount of shared memory in your system in kilobytes.
Total KBytes	This counter represents the total amount of memory in your system in kilobytes.
Total Swap KBytes	This counter represents the total amount of swap space in your system in kilobytes.
Used KBytes	This counter represents the amount of memory that is in use on the system in kilobytes.
Used Swap KBytes	This counter represents the amount of swap space that is in use on your system in kilobytes.

Network Interface

The network interface object provides information about the network interfaces on the system. Table 6-43 contains information on network interface counters.

Table 6-43 Network Interface

Counters	Counter Descriptions
Rx Bytes	This counter represents the number of bytes, including framing characters, that were received on the interface.
Rx Dropped	This counter represents the number of inbound packets that were chosen to be discarded even though no errors had been detected. This prevents the packet from being delivered to a higher layer protocol. Discarding packets to free up buffer space provides one reason.
Rx Errors	This counter represents the number of inbound packets (packet-oriented interfaces) and the number of inbound transmission units (character-oriented or fixed-length interfaces) that contained errors that prevented them from being deliverable to a higher layer protocol.
Rx Multicast	This counter represents the number of multicast packets that werereceived on this interface.
Rx Packets	This counter represents the number of packets that this sublayer delivered to a higher sublayer. This does not include the packets that were addressed to a multicast or broadcast address at this sublayer.
Total Bytes	This counter represents the total number of Rx bytes and Tx bytes.
Total Packets	This counter represents the total number of Rx packets and Tx packets.
Tx Bytes	This counter represents the total number of octets, including framing characters, that were transmitted out from the interface.
Tx Dropped	This counter represents the number of outbound packets that were chosen to be discarded even though no errors were detected. This action prevents the packet from being delivered to a higher layer protocol. Discarding a packet to free up buffer space. represents one reason.
Tx Errors	This counter represents the number of outbound packets (packet-oriented interfaces) and the number of outbound transmission units (character-oriented or fixed-length interfaces) that could not be transmitted because of errors.
Tx Packets	This counter represents the total number of packets that the higher level protocols requested for transmission, including those that were discarded or not sent. This does not include packets that were addressed to a multicast or broadcast address at this sublayer.
Tx QueueLen	This counter represents the length of the output packet queue (in packets).

Number of Replicates Created and State of Replication

The Number of Replicates Created and State of Replication object provides information about the replication state on the system. Table 6-44 contains information on replication counters.

Table 6-44 Number of Replicates Created and State of Replication

Counters	Counter Descriptions
Number of Replicates Created	This counter represents the number of replicates that have been created.
Replicate_State	This counter represents the state of replication. Possible values: 0-Not Started;1-Started; 2-Finished;3-Broken.

Partition

The partition object provides information about the file system and its usage in the system. Table 6-45 contains information on partition counters.

Table 6-45 Partition

Counters	Counter Descriptions
% CPU Time	This counter represents the percentage of CPU time that is dedicated to handling IO requests that were issued to the disk.
% Used	This counter represents the percentage of disk space that is in use on this file system.
% Wait in Read	This counter represents the percentage of CPU time that is spent waiting to read from the disk.
% Wait in Write	This counter represents the percentage of CPU time that is waiting to write to the disk.
Queue Length	This counter represents the average queue length for the requests that were issued to the disk.
Read Bytes Per Sec	This counter represents the amount of data that was read from the disk in kilobytes per second.
Total Mbytes	This counter represents the amount of total disk space that is on this file system in megabytes.
Used Mbytes	This counter represents the amount of disk space that is in use on this file system in megabytes.
Write Bytes Per Sec	This counter represents the amount of data that was written to the disk in kilobytes per second.

Process

The process object provides information about the processes that are running on the system. Table 6-46 contains information on process counters.

Table 6-46 Process

Counters	Counter Descriptions
% CPU Time	This counter, which is expressed as a percentage of total CPU time, represents the tasks share of the elapsed CPU time since the last update.
% MemoryUsage	This counter represents the percentage of physical memory that a task is currently using.
Data Stack Size	This counter represents the stack size for task memory status.
Nice	This counter represents the nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining the dispatchability of a task.
Page Fault Count	This counter represents the number of major page faults that a task encountered that required the data to be loaded into memory.
PID	This counter displays the task-unique process ID. The ID periodically wraps, but the value will never equal zero.
Process Status	This counter displays the process status: • 0 - Running • 1 - Sleeping • 2 - Uninterruptible disk sleep • 3 - Zombie • 4 - Traced • 5 - Paging • 6 - Unknown
Shared Memory Size	This counter displays the amount of shared memory (KB) that a task is using. Other processes could potentially share the same memory.
STime	This counter displays the number of jiffies that this process has scheduled in kernel mode. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement.
Thread Count	This counter displays the number of threads that are currently grouped with a task.
Total CPU Time Used	This counter displays the total CPU time in jiffies that the task used in user mode and kernel mode since the start of the task.
UTime	This counter displays the number of jiffies that this process has scheduled in user mode.

Table 6-46 Process (continued)

Counters	Counter Descriptions
Virtual Image	This counter displays the total amount of virtual memory (KB) that the task is using. It includes all code, data, shared libraries, and pages that have been swapped out: VirtualImage = SwappedSize + ResidentSize.
VmData	This counter displays the virtual memory usage of the heap for the task in kilobytes (KB).
VmRSS	This counter displays the resident set that is currently in physical memory in kilobytes (KB) This includes the code, data, and stack.
VmSize	This counter displays the total virtual memory usage for an entire task in kilobytes (KB).

Processor

The processor object provides information on different processor time usage in percentages. Table 6-47 contains information on processor counters.

Table 6-47 Processor

Counters	Counter Descriptions
% CPU Time	This counter displays the processors share of the elapsed CPU time since the last update. This share gets expressed as a percentage of total CPU time.
Idle Percentage	This counter displays the percentage of time that the processor is in idle state.
IOwait Percentage	This counter represents the percentage of time that the processor spends executing read or write operations.
Irq Percentage	This counter represents the percentage of time that the processor spends executing the interrupt request that is assigned to devices, including the time that the processor spends sending a signal to the computer.
Nice Percentage	This counter displays the percentage of time that the processor is executing nice processes in user mode.
Softirq Percentage	This counter represents the percentage of time that the processor spends executing the soft IRQ and deferring task switching to get better CPU performance.
System Percentage	This counter displays the percentage of time that the processor is executing processes in kernel mode.
User Percentage	This counter displays the percentage of time that the processor is executing normal processes in user mode.

System

The System object provides information on file descriptors on your system. Table 6-48 contains information on system counters

Table 6-48 System

Counters	Counter Descriptions
Allocated FDs	This counter represents the total number of allocated file descriptors.
Being Used FDs	This counter represents the number of file descriptors that are currently in use in the system.
Freed FDs	This counter represents the total number of allocated file descriptors on the system that are freed.
Max FDs	This counter represents the maximum number of file descriptors that are allowed on the system.
Total CPU Time	This counter represents the total time in jiffies that the system has been up and running.
Total Processes	This counter represents the total number of processes on the system.
Total Threads	This counter represents the total number of threads on the system.

TCP

The TCP object provides information on the TCP statistics on your system. Table 6-49 contains information on the TCP counters.

Table 6-49 TCP

Counters	Counter Description
Active Opens	This counter displays the number of times that the TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
Attempt Fails	This counter displays the number of times that the TCP connections made a direct transition to the SYN-RCVD state from the LISTEN state.
Curr Estab	This counter displays the number of TCP connections where the current state is either ESTABLISHED or CLOSE- WAIT.
Estab Resets	This counter displays the number of times that the TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
In Segs	This counter displays the total number of segments that were received, including those received in error. This count only includes segments that are received on currently established connections.

Table 6-49 TCP (continued)

Counters	Counter Description
InOut Segs	This counter displays the total number of In Segs and Out Segs.
Out Segs	This counter displays the total number of segments that were received, including those received in error. This count only includes segments that are received on currently established connections.
Passive Opens	This counter displays the number of times that TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
RetransSegs	This counter displays the total number of segments that were retransmitted because the segment contains one or more previously transmitted octets.

Thread

The Thread object provides a list of running threads on your system. Table 6-50 contains information on the Thread counters.

Table 6-50 Thread

Counters	Counter Description
% CPU Time	This counter displays the threads share of the elapsed CPU time since the last update. This counter expresses the share as a percentage of the total CPU time.
PID	This counter displays the threads leader process ID.

Using RTMT for Performance Monitoring

RTMT displays performance information of all Cisco CallManager components in a cluster. The tool integrates with Cisco CallManager administration and serviceability software. RTMT provides alert notification for troubleshooting performance. It also monitors various aspects of Cisco CallManager performance by periodically polling performance counter values. Refer to "Displaying a Counter Description" section on page 9-9 for examples on displaying perfmon counters in a chart or table format.

Perfmon monitoring allows you to perform the following tasks:

- From the Cisco CallManager cluster, monitor performance counters including Cisco CallManager nodes, TFTP servers, and database servers.
- Continuously monitor a set of preconfigured objects and receive notification in the form of an e-mail message.
- Associate counter threshold settings to alert notification. An e-mail or popup message provides notification to the administrator.

- Save and restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Display up to six perfmon counters in one chart for performance comparisons.

RTMT displays performance counters in chart or table format. Chart format looks like a miniature window of information. Up to six charts display in the RTMT performance monitoring pane for each category tab that you create. You can display a particular counter by double clicking the counter in the perfmon monitoring pane. Because chart view represents the default, you configure the performance counters to display in table format when you create a category.

You can remove a counter chart (table entry) with the Remove Chart/TableEntry menu item in the Perfmon menu in the menu bar.

Tip The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate of the AMC (Alert Manager and Collector) changes for Cisco CallManager Administration service parameters, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application and not the backend server time, provides the basis for the time stamp in each chart.

See the following sections for configuration options in the RTMT perfmon monitoring pane:

- Category Tabs, page 6-65
- Sample Rate, page 6-65
- Adding Counters to Monitor, page 6-66
- Alert Notification for Counters, page 6-66

Category Tabs

A category comprises monitored performance counters. A tab in the RTMT monitoring pane contains the category name. All performance counters that are monitored in this tab belong to a category. The system polls the performance counters in the tab at the same rate, with each category configured to have its own polling rate.

You can create custom categories in the RTMT monitoring pane to view information that helps you troubleshoot specific performance or device problems. If your Cisco CallManager system is experiencing performance problems with specific objects, create custom categories to monitor the performance of the counters within the object. If the system is experiencing problems with specific devices, create custom categories to monitor the devices within the cluster. In addition, you can create alert notifications for counters and gateways in these custom categories.

To create custom categories, you add a new category tab. When the tab is created, you specify the specific performance counters, devices, and alerts within that tab and then save your custom category by using Profile.

Sample Rate

The Cisco CallManager software polls counters, devices, and gateway ports to gather status information. In the RTMT monitoring pane, you configure the polling intervals for the performance counters, devices, and gateway ports for each category tab that you create.

Note High-frequency polling rate affects Cisco CallManager performance. The minimum polling rate for monitoring a performance counter in chart view equals 5 seconds; the minimum rate for monitoring a performance counter in table view equals 1 second. The default for both specifies 10 seconds.

Adding Counters to Monitor

To troubleshoot system performance problems, you add the counter that is associated with the perfmon object to the RTMT performance monitoring pane, which displays a chart for the counter. Before you add counters, see the "Category Tabs" section on page 6-65.

Category tabs contain up to six perfmon counter charts.

Alert Notification for Counters

Using the alert notification feature, Cisco CallManager notifies you of system problems. Perform the following configuration setup to activate alert notifications for a system counter:

- From the RTMT Perfmon Monitoring pane, choose the system perfmon counter.
- Set up an e-mail or a message popup window for alert notification.
- Determine the threshold for the alert (for example, an alert activates when calls in progress exceed the threshold of over 100 calls or under 50 calls).
- Determine the frequency of the alert notification (for example, the alert occurs once or every hour).
- Determine the schedule for when the alert activates (for example, on a daily basis or at certain times of the day).

Zoom Counter

To get a closer look at performance monitors, zoom the monitor counter in the RTMT perfmon monitoring pane by highlighting the counter chart and choosing Zoom Chart in the Perfmon menu.

Counter Properties

Counter properties allow you to display a description of the counter and configure data-sampling parameters.

The Counter Property window contains the option to configure data samples for a counter. The performance counters that display in the RTMT performance monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option to view all the data that a perfmon counter collected.

Understanding Perfmon Logs

The system logs the perfmon data whenever RTMT calls the LogPerfMon API. You can open the file log, which is compatible with the Windows Performance tool csv format, by using the Performance tool for analysis.

When you add new counters, RTMT changes the header to accommodate the new counters and logs the values correspondingly. When data is unavailable for an already existing counter (already added to header), RTMT inserts blank values in the file. If the character length of the new counters that are added is greater than 2000, the new file gets generated with all the counters.

The following file name format for the PerfMon Log applies:
PerfMonLog_<NodeName>_MM_DD_YYYY_hh_mm.csv.

The following lists comprises the perfmon counters that RTMT logs:

At System level

- Cisco CallManager System Performance\QueueSignalsPresent 1-High
- Cisco CallManager System Performance\QueueSignalsPresent 2-Normal
- Cisco CallManager System Performance\QueueSignalsPresent 3-Low
- Cisco CallManager System Performance\QueueSignalsPresent 4-Lowest
- Cisco CallManager System Performance\QueueSignalsProcessed 1-High
- Cisco CallManager System Performance\QueueSignalsProcessed 2-Normal
- Cisco CallManager System Performance\QueueSignalsProcessed 3-Low
- Cisco CallManager System Performance\QueueSignalsProcessed 4-Lowest

For each process that is running on the system

- Process\% Processor Time
- Process\ID Process
- Process\Private Bytes
- Process\Virtual Bytes

Additional Cisco Documentation

Troubleshooting Guide for Cisco CallManager

Where to Find More Information

Related Topics

- Real-Time Monitoring Tool, page 5-1
- Real-Time Monitoring Configuration *Cisco CallManager Serviceability Administration Guide*
- Trace Collection and Log Central in RTMT, *Cisco CallManager Serviceability Administration Guide*

Alerts

This chapter contains information on the following topics:

Understanding Alerts

RTMT, which supports alert defining, setting, and viewing, contains preconfigured and user-defined alerts. Although you can perform configuration tasks for both types, you cannot delete preconfigured alerts (whereas you can add and delete user-defined alerts). The Alert menu comprises the following menu options:

- Alert Central—This option comprises the current status and history of every alert in the Cisco CallManager cluster.

Note You can also access Alert Central by using the Alert tab in the left controlling center in the RTMT monitoring pane.

- Alert/Properties—This menu option allows you to set alerts and alert properties.
- Remove Alert—This menu category allows you to remove an alert.
- Enable Alert—With this menu category, you can enable alerts.
- Disable Alert—You can disable an alert with this category.
- Suspend cluster/node Alerts—This menu category allows you to temporarily suspend alerts on a particular Cisco CallManager node or on the entire cluster.
- Clear Alerts—This menu category allows you to reset an alert (change the color of an alert item from red to black) to signal that an alert has been taken care of. After an alert has been raised, its color will automatically change to red in RTMT and will stay that way until you manually clear the alert.
- Clear All—This menu category allows you to clear all alerts.
- Alert Events Detail—This menu category provides detailed information on alert events.

- Config Email Server—In this category, you can configure your e-mail server to enable alerts.
- Config Alert Action—This category allows you to set actions to take for specific alerts; you can configure the actions to send the alerts to desired e-mail recipients.

In RTMT you can configure alert notification for perfmon counter value thresholds, for schedule for alert checking, and for status change of device (for example, port is out of service).

The Tools tab below the Quick Launch Channel includes the Alert Central category. Alert Central provides both the current status and the history of all the alerts in the Cisco CallManager cluster. To monitor Cisco CallManager alerts, use the Tools tab in conjunction with the Alert menu option under the Tools menu.

Preconfigured Alerts

RTMT comprises a set of preconfigured alerts. You cannot delete these alerts; however, you can enable or disable them in Alert Central.

The following list comprises the preconfigured alerts in RTMT:

- BeginThrottlingCallListBLFSubscriptions
- CallProcessingNodeCpuPegging
- CDRAgentSendFileFailed
- CDRFileDeliveryFailed
- CDRHighWaterMarkExceeded
- CDRMaximumDiskSpaceExceeded
- CodeYellow
- CriticalServiceDown
- DBReplicationFailure
- ExcessiveVoiceQualityReports
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAttendantConsoleServerHeartbeatRate
- LowAvailableVirtualMemory
- LowCallManagerHeartbeatRate
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- LowTFTPServerHeartbeatRate
- MaliciousCallTrace
- MediaListExhausted
- MgcpDChannelOutOfService
- NonCallProcessingNodeCpuPegging

- NumberOfRegisteredGatewaysDecreased
- NumberOfRegisteredGatewaysIncreased
- NumberOfRegisteredMediaDevicesDecreased
- NumberOfRegisteredMediaDevicesIncreased
- NumberOfRegisteredPhonesDropped
- RouteListExhausted
- ThreadCounterUpdateStopped

Alert Customization

You can configure both preconfigured and user-defined alerts in RTMT; however, you cannot delete preconfigured alerts. You can also disable both preconfigured and user-defined alerts in RTMT. You can add and delete user-defined alerts in the performance-monitoring window.

Table 7-1 provides a list of fields that you will use to configure each alert; users can configure preconfigured fields, unless otherwise noted.

Table 7-1 Alert Customization

Field	Description	Comment
Alert Name	High-level name of the monitoring item with which RTMT associates an alert	Descriptive name. For preconfigured alerts, you cannot change this field. See the "Enabling Trace Download" section on page 7-6.
Description	Description of the alert	You cannot edit this field for preconfigured alerts. See the "Enabling Trace Download" section on page 7-6.
Perfmon Counters	List of source perfmon counters	For preconfigured alerts, you cannot change this field.
Value Threshold	Condition to raise alert (value is...)	Specify up < - > down, less than #, %, rate greater than #, %, rate.
Evaluation Method	Method used to check the threshold condition	Specify value to be evaluated as absolute, delta (present - previous), or % delta.
Duration Threshold	Condition to raise alert (how long value threshold has to persist before raising alert)	Options include right away and specify at least X minutes.
Number of Events Threshold	Raise alert only when a configurable number of events exceed a configurable time interval (in minutes).	For ExcessiveVoiceQualityReports, the default thresholds equal 10 to 60 minutes. For RouteListExhausted and MediaListExhausted, the defaults equal 0 to 60 minutes.

Table 7-1 Alert Customization (continued)

Field	Description	Comment
Node IDs	Cluster or list of nodes to monitor	Cisco CallManager nodes, Cisco TFTP node, or first node. **Note** When you deactivate both Cisco CallManager and Cisco TFTP services of a node, the system considers that node as removed from the currently monitored node list. When you reactivate both Cisco CallManager and Cisco TFTP services, that node gets added back, and its settings get restored to default values.
Alert Action ID	ID of alert action to take (System always logs alerts no matter what the alert action.)	Alert action gets defined first (see the "Alert Action Configuration" section on page 7-5). If this field is blank, that indicates that e-mail is disabled.
Disabled	Alert disabled	Options include enabled or disabled.
Clear Alert	Resets alert (change the color of an alert item from red to black) to signal that the alert has been resolved	After an alert has been raised, its color will automatically change to red and stay that way until you manually clear the alert. Use Clear All to clear all alerts.
In Safe Range	Indicates whether an alert threshold condition has been met (not configurable)	This field does not apply to MaliciousCall and Registered YYY types of alerts. For DChannel OOS alert, this field remains YES only when you no longer have any outstanding OOS devices. The Code Yellow alert will be back in safe range only when you receive a CodeYellowExit event from Cisco CallManager.
Alert Details	Displays the detail of an alert (not configurable)	For VoiceQualityReports, RouteListExhausted, and MediaListExhausted, up to 30 current event details display in the current monitoring interval if an alert has been raised in the current interval. Otherwise, the previous 30 event details in the previous interval displays. For DChannel OOS alert, the list of outstanding OOS devices at the time the alert was raised displays.

Table 7-1 Alert Customization (continued)

Field	Description	Comment
Alert Generation Rate	How often to generate alert when alert condition persists	Specify every X minutes. (Raise alert once every X minutes if condition persists.) Specify every X minutes up to Y times. (Raise alert Y times every X minutes if condition persists.)
User Provide Text	Administrator to append text on top of predefined alert text	N/A
Severity	For viewing purposes (for example, show only Sev. 1 alerts)	Specify defaults that are provided for predefined (for example, Error, Warning, Information) alerts.
Collection Polling Rate	Same rate for both preconfigured and user-defined alerts	Although not configurable through RTMT Alert Central, you can customize this through Cisco CallManager Administration in Service Parameters.

Alert Action Configuration

In RTMT, you can configure alert actions for every alert that is generated and have the alert action sent to e-mail recipients that you specify in the alert action list.

Table 7-2 provides a list of fields that you will use to configure alert actions. Users can configure all fields, unless otherwise marked.

Table 7-2 Alert Action Configuration

Field	Description	Comment
Alert Action ID	ID of alert action to take	Specify descriptive name.
Mail Recipients	List of e-mail addresses. You can selectively enable/disable an individual e-mail in the list.	N/A
Global Alert Action Flag	Flag to effectively disable all e-mails	If you disable this flag, no e-mails get sent out, even though alerts occur.

Enabling Trace Download

Some preconfigured alerts will allow you to initiate a trace download based on the occurrence of an event. You can automatically capture traces when a particular event occurs by checking the Enable TCT Download check box in Set Alert/Properties for the following alerts:

- CriticalServiceDown
- CodeYellow

Caution Enabling TCT Download may affect services on the server. Configuring a high number of downloads will adversely impact the quality of services on the server.

Understanding Alert Logs

The alert log stores the alert, which is also stored in memory. The memory gets cleared at a constant interval, leaving the last 30 minutes of data in the memory. When the service starts/restarts, the last 30 minutes of the alert data load into the memory by the system reading from the alert logs that exist in all servers in the cluster. The alert data in the memory gets sent to the RTMT clients on request.

Upon RTMT startup, RTMT shows all logs that occurred in the last 30 minutes in the Alert Central log history. Alert log periodically gets updated, and new logs get inserted into the log history window. After the number of logs reaches 100, RTMT removes the oldest 40 logs.

The following file name format for the alert log applies: AlertLog_MM_DD_YYYY_hh_mm.csv.

The alert log includes the following attributes:

- Time Stamp—Time when RTMT logs the data
- Alert Name—Descriptive name of the alert
- Node ID—Node name for where RTMT raised the alert
- Alert Message—Detailed description about the alert
- Monitored Object Name—Name of the object monitored
- Severity—Severity of the alert
- PollValue—Value of the monitored object where the alert condition occurred
- Action—Alert action taken

The first line of each log file comprises the header. Details of each alert gets written in a single line, separated by a comma.

Where to Find More Information

Related Topics

- Real-Time Monitoring Configuration, *Cisco CallManager Serviceability Administration Guide*
- Alert Configuration in RTMT, *Cisco CallManager Serviceability Administration Guide*

Log Partition Monitoring

This chapter contains information on the following topics:

Understanding Log Partition Monitoring

Log Partition Monitoring, which is installed automatically with Cisco CallManager, uses configurable thresholds to monitor the disk usage of the log partition on a server (or all servers in the cluster). You configure Log Partition Monitoring in Alert Central in RTMT.

Note Log Partition Monitoring relies on the Cisco Log Partition Monitoring Tool service, which is a network service that you can start and stop in the Control Center—Network Services window. When you install Cisco CallManager, this service starts automatically. Stopping the service causes a loss of feature functionality.

You can configure he following information parameters in Alert Central in RTMT:

- LogPartitionLowWaterMarkExceeded —Disk space utilization level at which log partition monitoring stops purging log files; level ranges exist from 10-90 percent; default equals 80 percent; configuration must be lower than high watermark.
- LogPartitionHighWaterMarkExceeded—Disk space utilization level at which log partition monitoring starts purging log files; level ranges exist from 15-95 percent; default equals 90 percent.

When log partition monitoring starts at system startup, the system checks the current disk space utilization. If the percentage of disk usage is above the low water mark, but less than the high water mark, the system sends a alarm message to syslog and generates a corresponding alert in RTMT Alert central.

To offload the log files and regain disk space on the server, you should collect the traces that you are interested in saving by using the Real-Time Monitoring tool.

If the percentage of disk usage is above the high water mark that you configured, the system sends an alarm message to syslog, generates a corresponding alert in RTMT Alert Central, and automatically purges log files until the value reaches the low water mark.

Note Log Partition Monitoring automatically identifies the active partition; if any log files exist in the inactive partition log partition directory, the system deletes those files first. If necessary, the system deletes log files in the active partition log partition directory, starting with the oldest log file for every application until the disk space percentage drops below the configured low watermark. The system does not send an e-mail when log partition monitoring purges the log files.

After the system determines the disk usage and performs the necessary tasks (sending alarms, generating alerts, or purging logs), log partition monitoring occurs at regular 5 minute intervals.

Where to Find More Information

Related Topics

- Log Partition Monitoring Configuration, *Cisco CallManager Serviceability Administration Guide*
- Trace Collection and Log Central in RTMT, *Cisco CallManager Serviceability Administration Guide*

PART 3

Reporting Tools

Serviceability Reports Archive

The Cisco Serviceability Reporter service generates daily reports in Cisco Serviceability Administration. Each report provides a summary that comprises different charts that display the statistics for that particular report. Reporter generates reports once a day on the basis of logged information.

See the following sections for detailed information about each report that Serviceability Reporter generates:

Note Because the Cisco Serviceability Reporter is only active on the Cisco CallManager on the first node, at any time, Reporter generates reports only on the first node, not the other nodes.

You can view reports from **Cisco CallManager Serviceability > Tools > Serviceability Reports Archive**.

The reports contain 24-hour data for the previous day. A suffix that is added to the report names shows the date for which Reporter generated them; for example, AlertRep_mm_dd_yyyy.pdf. The Serviceability Reports Archive window uses this date to display the reports for the relevant date only. The reports generate from the data that is present in the log files, with the timestamp for the previous day. The system considers log files for the current date and the previous two days for collecting data to take into account the time zone differences between the server locations.

Note Log files can be picked up from all the Cisco CallManager nodes in the cluster while generating reports.

The time that is shown in the report reflects the first node “System Time.” If the first node and subsequent node(s) are in different time zones, the first node “System Time” shows in the report.

Serviceability Reporter Service Parameters

Cisco Serviceability Reporter uses the following three service parameters:

- RTMT Reporter Designated Node—Specifies the designated node on which RTMT Reporter runs. Because the Serviceability Reporter service is CPU intensive, Cisco recommends that you specify a non-callprocessing node. This default equals the IP address of the server on which the RTMT Reporter service is first activated.
- Report Generation Time—The number of minutes after midnight. Reports generate at this time for the most recent day. The minimum value is 0 and the maximum value is 1439.
- Report Deletion Age—The number of days that the report must be kept in the disk. The system deletes reports that are older than the specified age. The minimum value is 0 and the maximum value is 30.

For more information about service parameter configuration, refer to the *Cisco CallManager Administration Guide*.

Note If a server gets removed completely from the network (the server should be removed from the network and also from the list of servers in Cisco CallManager Administration), Reporter does not consider this server while generating reports, even if the log file contains the data for that server.

Device Statistics Report

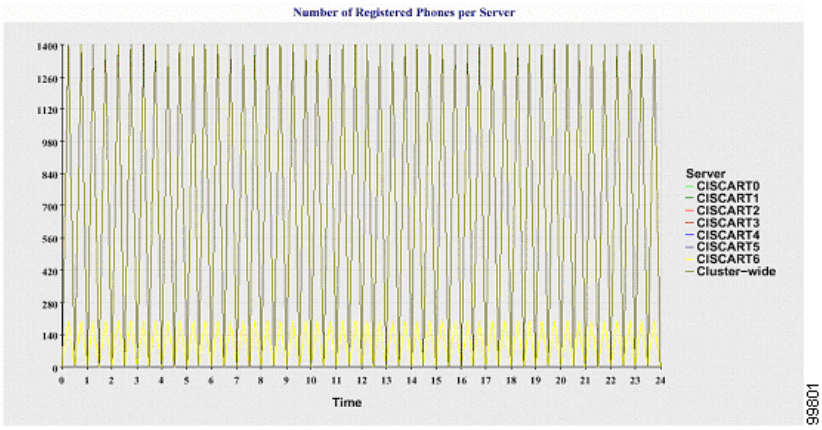
The Device Statistics Report provides the following line charts:

- Number of Registered Phones per Server—A line chart displays the number of registered phones for each Cisco CallManager server and cluster. Each line in the chart represents the data for each server in the cluster (for which data is available), and one extra line displays the clusterwide data. Each data value in the chart represents the average number of phones that are registered for a 15-minute duration. In any server shows no data, Reporter does not generate the line representing that server. If no data exists for all servers, for registered phones, Reporter does not generate the chart. The message “No data for Device Statistics report available” displays.

Note You can disable reports by setting the service parameter Report Deletion Time to a value of 0.

Figure 9-1 shows an example of a line chart that represents the number of registered phones per Cisco CallManager server.

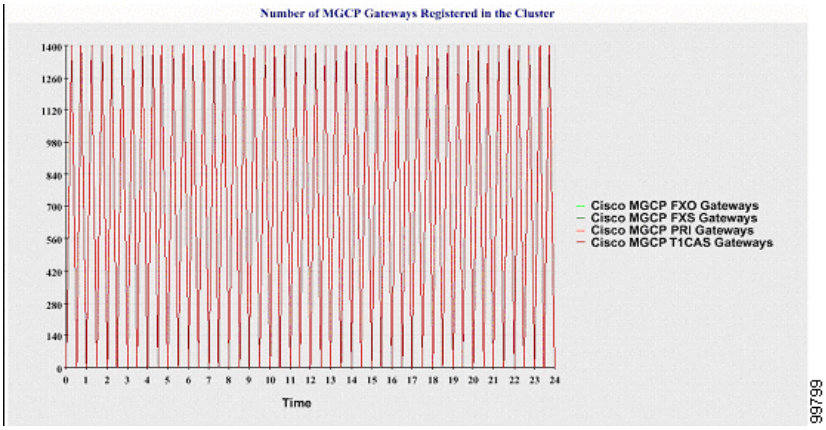
Figure 9-1 Line Chart Depicting Number of Registered Phones per Server



- Number of MGCP Gateways Registered in the Cluster—A line chart displays the number of registered MGCP FXO, FXS, PRI, and T1CAS gateways. Each line represents data only for the Cisco CallManager cluster; so, there are four lines showing clusterwide details for each gateway type. Each data value in the chart represents the average number of MGCP gateways that are registered for a 15-minute duration. If no data exists for a gateway for all the servers, Reporter does not generate the line that represents data for that particular gateway. If no data exists for all gateways for all servers, Reporter does not generate the chart.

Figure 9-2 shows an example of a line chart that represents the number of registered gateways per Cisco CallManager cluster.

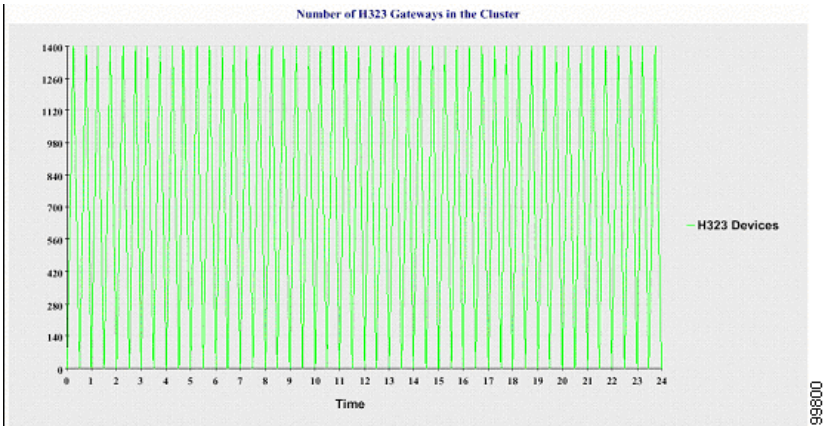
Figure 9-2 Line Chart Depicting Number of Registered Gateways per Cluster



- Number of H.323 Gateways in the Cluster—A line chart displays the number of H.323 gateways. One line represents the clusterwide details of the H.323 gateways. Each data value in the chart represents the average number of H.323 gateways for a 15-minute duration. If no data exists for H.323 gateways for all servers, Reporter does not generate the chart.

Figure 9-3 shows example line chart that represents the number of H.323 gateways per Cisco CallManager cluster.

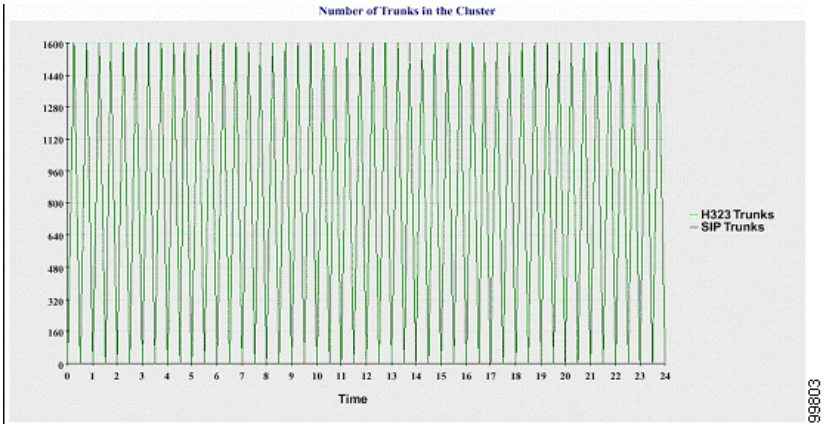
Figure 9-3 Line Chart Depicting Number of Registered H.323 Gateways per Cluster



- Number of Trunks in the Cluster—A line chart displays the number of H.323 and SIP trunks. Two lines represent the clusterwide details of the H.323 trunks and SIP trunks. Each data value in the chart represents the average number of H.323 and SIP trunks for a 15-minute duration. If no data exists for H.323 trunks for all servers, Reporter does not generate the line that represents data for the H.323 trunks. If no data exists for SIP trunks for all servers, Reporter does not generate the line that represents data for SIP trunks. If no data exists for trunks for all servers, Reporter does not generate the chart.

Figure 9-4 shows example line chart that represents the number of trunks per Cisco CallManager cluster.

Figure 9-4 Line Chart Depicting Number of Trunks per Cluster



You can read information from the log files from all servers in the Cisco CallManager cluster that match the file name pattern DeviceLog_mm_dd_yyyy_hh_mm.csv. The information that is read from the file for the Device Statistics report includes:

- Number of registered phones on each server
- Number of registered MGCP FXO, FXS, PRI, and T1CAS gateways on each server
- Number of registered H.323 gateways on each server
- Number of SIP trunks and H.323 trunks

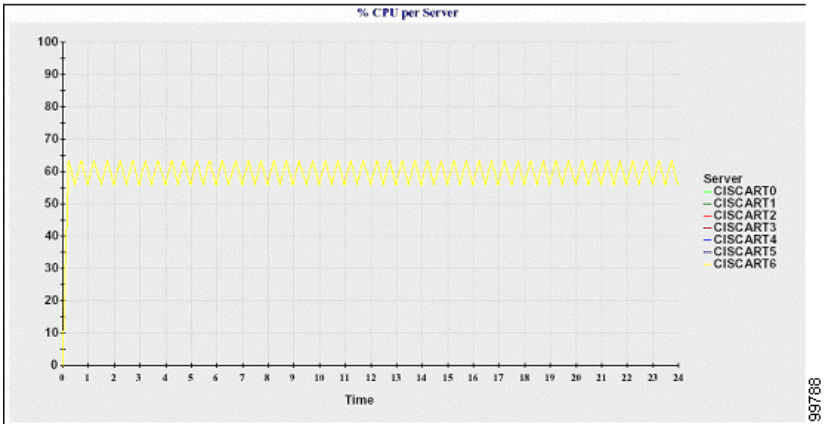
Server Statistics Report

The Server Statistics Report provides the following line charts:

- Percentage of CPU per Server—A line chart displays the percentage CPU usage per Cisco CallManager server. Each line in the chart represents the data for each server in the Cisco CallManager cluster (for which data is available). Each data value in the chart represents the average CPU Usage for a 15-minute duration. If no data exists for any one server, Reporter does not generate the line that represents that server. If no data exists for all servers, Reporter does not generate the chart. The message "No data for Server Statistics report available" displays.

Figure 9-5 shows a line chart example that represents the percentage of CPU usage per Cisco CallManager server.

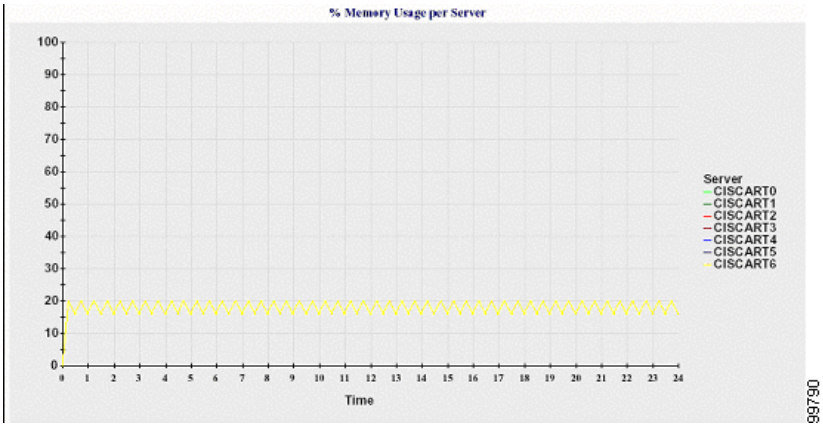
Figure 9-5 Line Chart Depicting the Percentage of CPU per Server



- Percentage of Memory Usage per Server—A line chart displays the percentage Memory Usage per Cisco CallManager server (%MemoryInUse). Each line in the chart represents the data for each server in the Cisco CallManager cluster (for which data is available). Each data value in the chart represents the average memory usage for a 15-minute duration. If no data exists for any server, Reporter does not generate the line that represents that server. If no data exists for all servers, Reporter does not generate the chart.

Figure 9-6 shows a line chart example that represents the percentage of memory usage per Cisco CallManager server.

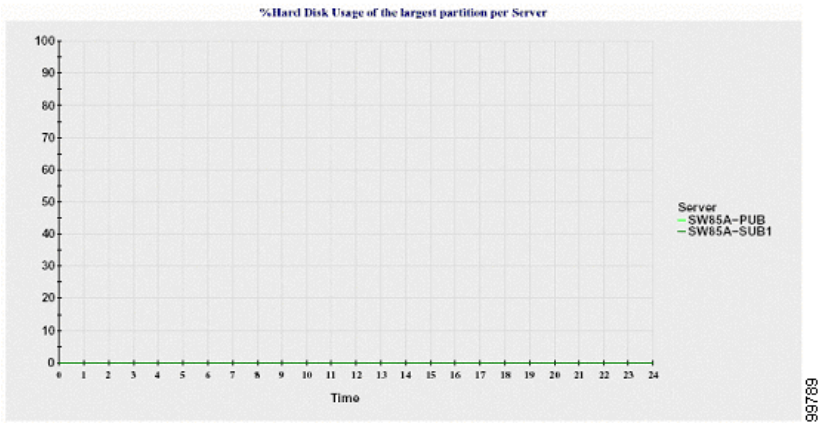
Figure 9-6 Line Chart Depicting Percentage of Memory Usage per Server



- Percentage of Hard Disk Usage of the Largest Partition per Server—A line chart displays the percentage of disk space usage for the largest partition per Cisco CallManager server (%DiskSpaceInUse). Each line in the chart represents the data for each server in the Cisco CallManager cluster (for which data is available). Each data value in the chart represents the average disk usage for a 15-minute duration. If no data exists for any one server, Reporter does not generate the line that represents that server. If no data exists for all servers, Reporter does not generate the chart.

Figure 9-7 shows a line chart example that represents the percentage of hard disk usage for the largest partition per Cisco CallManager server.

Figure 9-7 Line Chart Depicting Percentage of Hard Disk Usage of the Largest Partition per Server



You can read the information from log files, from the servers in the cluster that matches the file name pattern ServerLog_mm_dd_yyyy_hh_mm.csv. The information that is read from the file for the Server Statistics report includes:

- % CPU usage on each server
- % Memory usage (%MemoryInUse) on each server
- % Hard disk usage of the largest partition (%DiskSpaceInUse) on each server

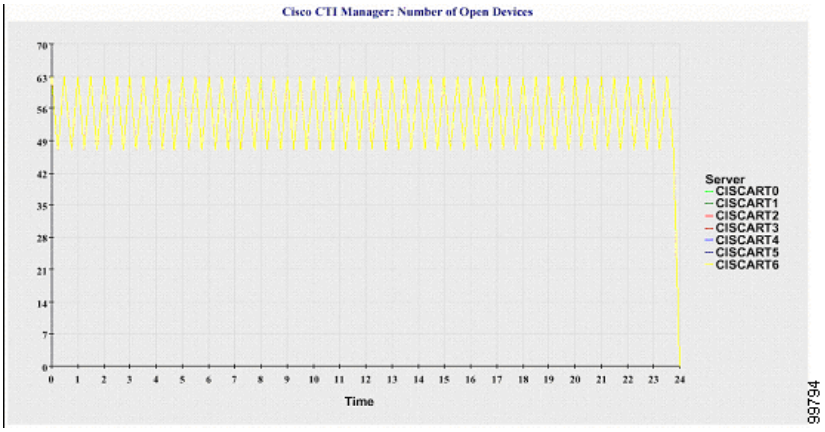
Service Statistics Report

The Service Statistics Report provides the following line charts:

- Cisco CTI Manager: Number of Open Devices—A line chart displays the number of CTI Open Devices per CTI Manager. Each line chart represents the data for each server in the Cisco CallManager cluster (on which service is activated). Each data value in the chart represents the average number of CTI open devices for a 15-minute duration. If no data exists for any one server, Reporter does not generate the line that represents that server. If no data exists for all servers, Reporter does not generate the chart. The message "No data for Service Statistics report available" displays.

Figure 9-8 shows a line chart example that represents the number of open devices per Cisco CTI Manager.

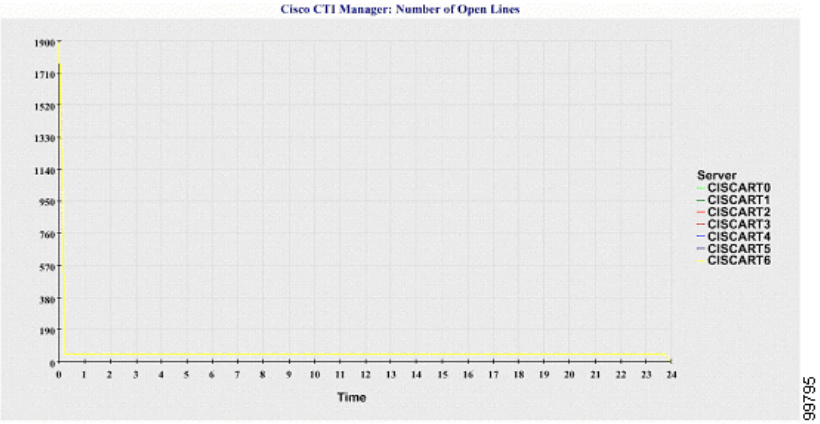
Figure 9-8 Line Chart Depicting Cisco CTI Manager: Number of Open Devices



- Cisco CTI Manager: Number of Open Lines—A line chart displays the number of CTI open lines per CTI Manager. Each line in the chart represents the data for each server in the Cisco CallManager cluster (on which service is activated). Each data value in the chart represents the average number of CTI open lines for a 15-minute duration. If no data exists for any one server, Reporter does not generate the line that represents that server. If no data exists for any of the servers, Reporter does not generate the chart.

Figure 9-9 shows a line chart example that represents the number of open lines per Cisco CTI Manager.

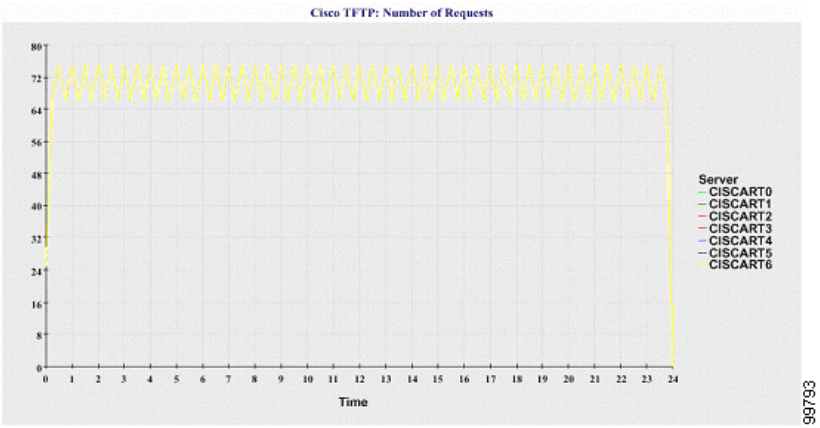
Figure 9-9 Line Chart Depicting Cisco CTI Manager: Number of Open Lines



- Cisco TFTP: Number of Requests—A line chart displays the number of Cisco TFTP requests per TFTP server. Each line in the chart represents the data for each server in the Cisco CallManager cluster (on which service is activated). Each data value in the chart represents the average number of TFTP requests for a 15-minute duration. If no data exists for any one server, Reporter does not generate the line that represents that server. If no data exists for any of the servers, Reporter does not generate the chart.

Figure 9-10 shows a line chart example that represents the number of Cisco TFTP requests per TFTP server.

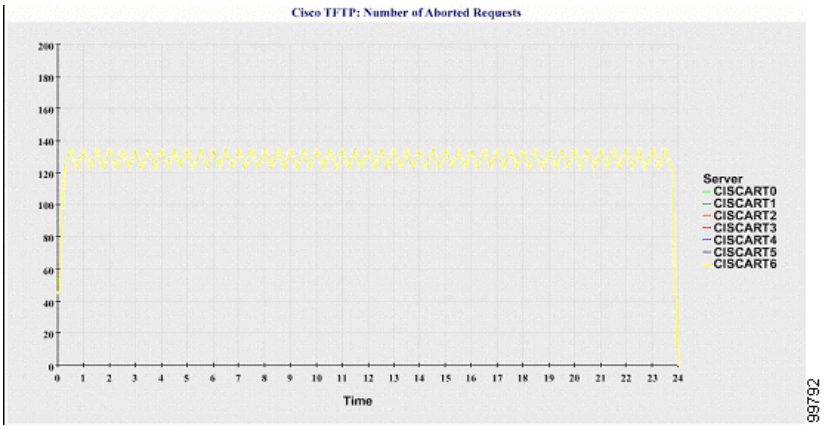
Figure 9-10 Line Chart Depicting Cisco TFTP: Number of Requests



- Cisco TFTP: Number of Aborted Requests—A line chart displays the number of Cisco TFTP Requests Aborted per TFTP server. Each line in the chart represents the data for each server in the Cisco CallManager cluster (on which service is activated). Each data value in the chart represents the average of TFTP Requests Aborted for a 15-minute duration. If no data exists for any one server, Reporter does not generate the line that represents that server. If no data exists for any of the servers, Reporter does not generate the chart.

Figure 9-11 shows a line chart example that represents the number of Cisco TFTP requests that were aborted per TFTP server.

Figure 9-11 Line Chart Depicting Cisco TFTP: Number of Aborted Requests



You can read the information from log files, from all the servers of the Cisco CallManager cluster that matches the file name pattern ServiceLog_mm_dd_yyyy_hh_mm.csv. The information that is read from the file for the Service Statistics report includes:

- For each CTI Manager - Number of open devices
- For each CTI Manager - Number of open lines
- For each Cisco TFTP server - TotalTftpRequests
- For each Cisco TFTP server - TotalTftpRequestsAborted

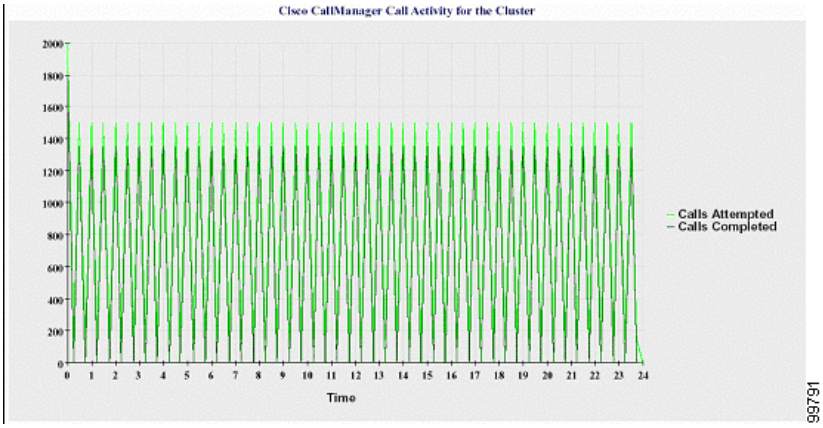
Call Activities Report

The Call Activities Report provides the following line charts:

- Cisco CallManager Call Activity for the Cluster—A line chart displays the number of calls that were attempted and calls that were completed for H.323 gateways for the entire Cisco CallManager cluster. The chart comprises two lines, one for the number of calls that were attempted and another for the number of calls that were completed. Each line represents the cluster value, which is the sum of the values for all the servers in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were attempted or calls that were completed for a 15-minute duration. If no data exists for H.323 gateways calls completed for all the servers, then Reporter does not generate the line representing data for Calls Completed. In the case that there is no data for a Cisco CallManager calls completed for all the servers, Reporter does not generate the line that represents data for Calls Completed. If no data exists for Cisco CallManager calls that were attempted for all the servers, Reporter does not generate the line that represents data for Calls Attempted. If no data exists for Cisco CallManager call activities for all the servers, Reporter does not generate the chart. The message “No data for Call Activities report available” displays.

Figure 9-12 shows a line chart example that represents the number of attempted and completed calls for the Cisco CallManager cluster.

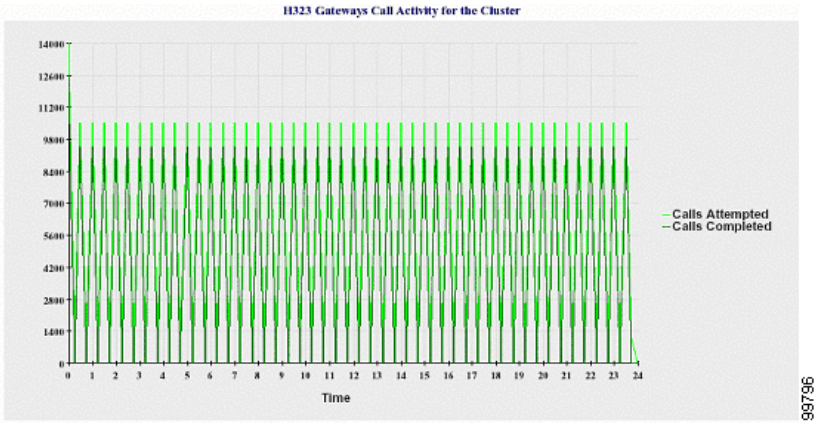
Figure 9-12 Line Chart Depicting Cisco CallManager Call Activity for the Cluster



- H.323 Gateways Call Activity for the Cluster—A line chart displays the number of calls that were attempted and calls that were completed for H.323 gateways, for the entire Cisco CallManager cluster. The chart comprises two lines, one for the number of calls that were attempted and another for the number of calls that were completed. Each line represents the cluster value, which equals the sum of the values for all the servers in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were attempted or calls that were completed for a 15-minute duration. If no data exists for H.323 gateways calls that were completed for all servers, Reporter does not generate the line that represents data for calls that were completed. If no data exists for H.323 gateways calls that were attempted for all servers, Reporter does not generate the line that represents data for calls that were attempted. If no data for H.323 gateways call activities for all servers, Reporter does not generate the chart.

Figure 9-13 shows a line chart example that represents the H.323 gateway call activity for the Cisco CallManager cluster.

Figure 9-13 Line Chart Depicting H.323 Gateways Call Activity for the Cluster

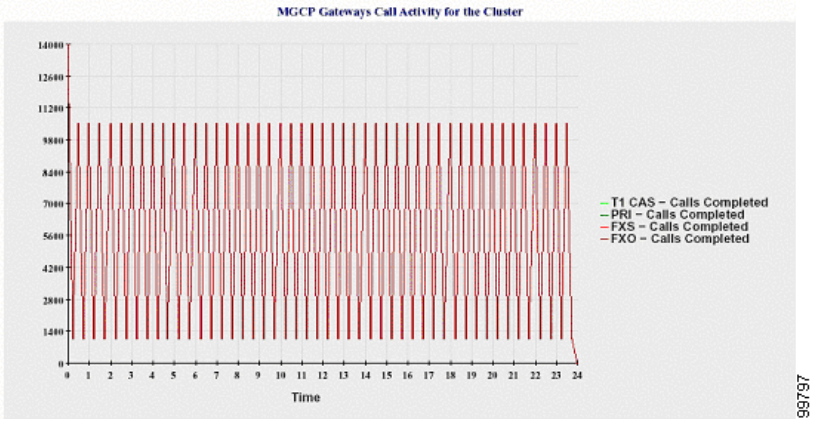


- MGCP Gateways Call Activity for the Cluster—A line chart displays the number of calls that were completed in an hour for MGCP FXO, FXS, PRI, and T1CAS gateways, for the entire Cisco CallManager cluster. The chart comprises four lines at the most, one for the number of calls that were completed for each of the gateway types (for which data is available). Each line represents the cluster value, which equals the sum of the values for all servers in the cluster (for which data is

available). Each data value in the chart represents the total number of calls that were completed for a 15-minute duration. If no data exists for a gateway for all servers, Reporter does not generate the line that represents data for calls that were completed for a particular gateway. If no data exists for all gateways for all servers, Reporter does not generate the chart.

Figure 9-14 shows a line chart example that represents the MGCP gateways call activity for the Cisco CallManager cluster.

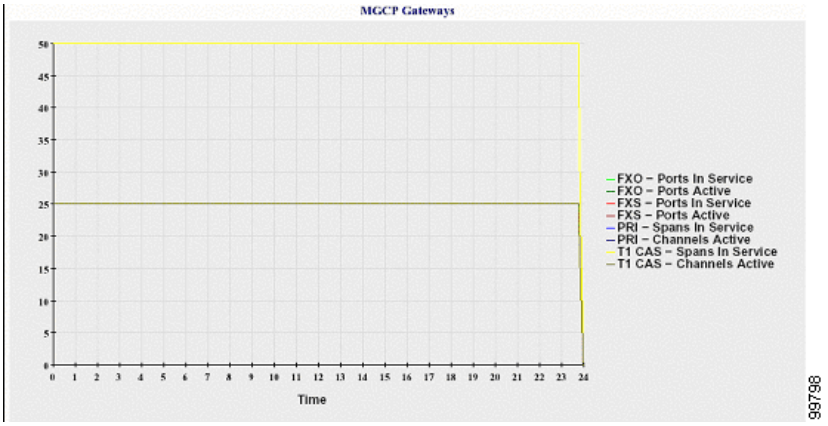
Figure 9-14 Line Chart Depicting MGCP Gateways Call Activity for the Cluster



- MGCP Gateways—A line chart displays the number of Ports In Service and Active Ports for MGCP FXO, FXS gateways and the number of Spans In Service or Channels Active for PRI, T1CAS gateways for the entire Cisco CallManager cluster. The chart comprises eight lines, two lines each for the number of Ports In Service for MGCP FXO and FXS, and two lines each for the number of Active Ports for MGCP FXO and FXS. Four more lines for the number of Spans In Service and Channels Active for PRI and T1CAS gateways exist. Each line represents the cluster value, which is the sum of the values for all servers in the cluster (for which data is available). Each data value in the chart represents the total Number of Ports In Service, Number of Active Ports, Spans In Service or Channels Active for a 15-minute duration. If no data exists for the number of Spans In Service or the Channels Active for a gateway (MGCP PRI, T1CAS) for all servers, Reporter does not generate the line that represents data for that particular gateway.

Figure 9-15 shows a line chart example that represents the MGCP gateways.

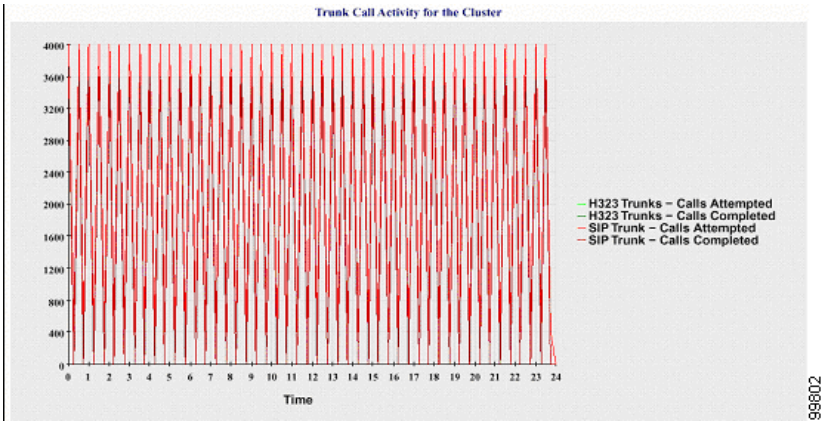
Figure 9-15 Line Chart Depicting MGCP Gateways



- Trunk Call Activity for the Cluster—A line chart displays the number of calls that were completed and calls that were attempted in an hour for SIP Trunk and H.323 Trunk for the entire Cisco CallManager cluster. The chart comprises four lines, two for the number of calls that were completed for each SIP and H.323 trunk (for which data is available) and two for the number of calls that were attempted. Each line represents the cluster value, which is the sum of the values for all the servers in the cluster (for which data is available). Each data value in the chart represents the total Number of Calls Completed or Number of Calls Attempted for a 15-minute duration. If no data exists for a trunk for all servers, Reporter does not generate the line that represents data for Calls Completed or Calls Attempted for that particular trunk. If no data exists for both the trunks for all servers, Reporter does not generate the chart.

Figure 9-16 shows a line chart example that represents the trunk call activity for the cluster.

Figure 9-16 Line Chart Depicting Trunk Call Activity for the Cluster



You can read the information from log files from all servers in the cluster that matches the file name pattern CallLog_mm_dd_yyyy_hh_mm.csv. The information that is read from the file for the Call Activities report includes:

- Calls Attempted and Calls Completed for the Cisco CallManager in each Cisco CallManager server
- Calls Attempted and Calls Completed for the H.323 gateways in each Cisco CallManager server

- Calls Completed for the MGCP FXO, FXS, PRI, and T1CAS gateways in each Cisco CallManager server
- Ports In Service, Active Ports for MGCP FXO and FXS gateways and Spans In Service, Channels Active for PRI, and T1CAS gateways in each Cisco CallManager server
- Calls Attempted and Calls Completed for H.323 Trunks and SIP Trunks

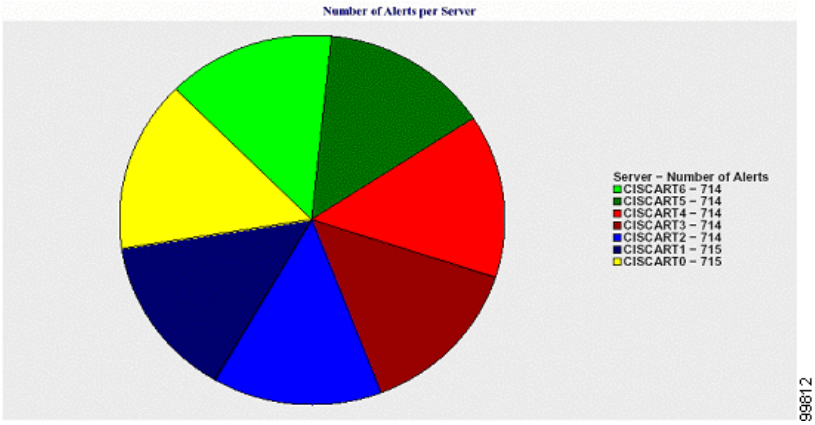
Alert Summary Report

The Alert Summary Report provides the details of alerts that are generated for a day. The Alert report comprises the following charts:

- Number of Alerts per Server—A pie chart provides the number of alerts per Cisco CallManager server. The chart displays the server-wide details of the alerts that are generated. Each sector of the pie chart represents the number of alerts generated for a particular server in the Cisco CallManager cluster. The chart has as many number of sectors as there are servers (for which Reporter generates alerts in the day) in the cluster. If no data exists for a server, no sector in the chart that represents that server. If no data exists for all servers, Reporter does not generate the chart. The message "No alerts were generated for the day" displays.

Figure 9-17 shows a pie chart example that represents the number of alerts per server.

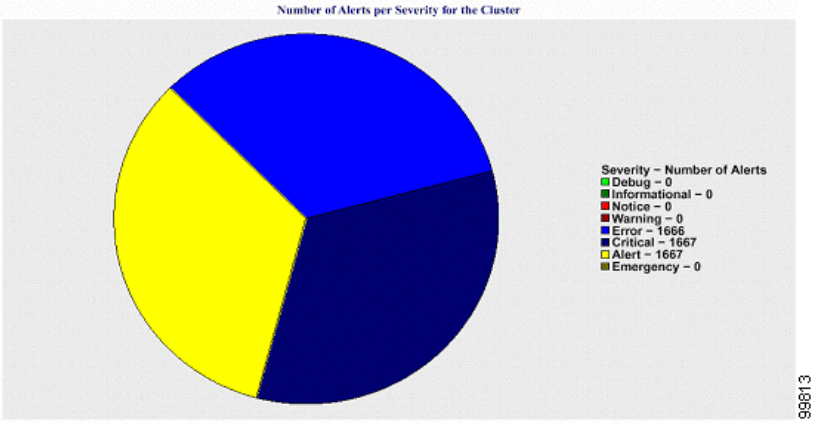
Figure 9-17 Pie Chart Depicting Number of Alerts per Server



- Number of Alerts per Severity for the Cluster—A pie chart displays the number of alerts per Alert Severity. The chart displays the severity details of the alerts that are generated. Each sector of the pie chart represents the number of alerts generated of a particular severity type. The chart provides as many number of sectors as there are severities (for which Reporter generates alerts in the day). If no data exists for a severity, no sector in the chart that represents that severity. If no data exists for all servers, Reporter does not generate the chart.

Figure 9-18 shows a pie chart example that represents the number of alerts per severity for the cluster.

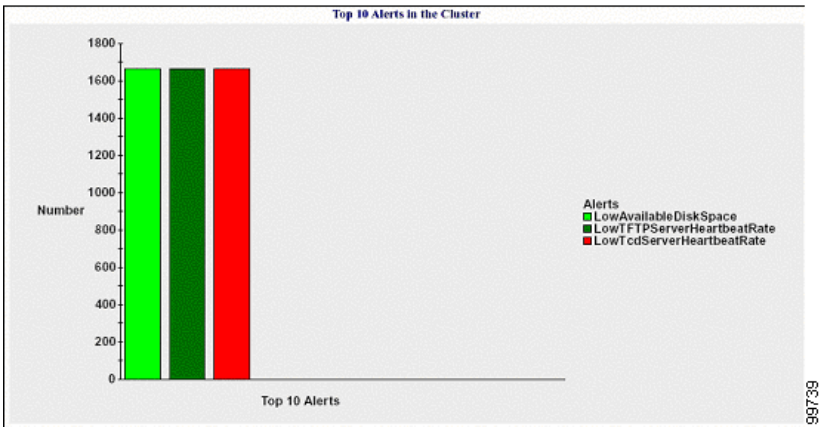
Figure 9-18 Pie Chart Depicting Number of Alerts per Severity for the Cluster



- Top 10 Alerts in the Cluster—A bar chart displays the number of alerts of a particular Alert Type. The chart displays the details of the alerts that are generated on the basis of the alert type. Each bar represents the number of alerts for an alert type. The chart displays details only for the first 10 alerts based on the highest number of alerts in descending order. If no data exists for a particular alert type, no bar represents that alert. If no data exists for any alert type, RTMT does not generate the chart.

Figure 9-19 shows a bar chart example that represents the top 10 alerts in the cluster.

Figure 9-19 Bar Chart Depicting Top 10 Alerts in the Cluster



You can read the information from log files from all servers in the cluster that match the file name pattern AlertLog_mm_dd_yyyy_hh_mm.csv. The information read from the file for Alert report includes:

- Time - Time at which the alert occurred
- Alert Name - Descriptive name
- Node Name - Server on which the alert occurred
- Monitored object - The object that is monitored
- Severity - Severity of this alert

Performance Protection Report

The Performance Protection Report provides trend analysis information on default monitoring objects that allows you to track overall system health. The report includes information for the for the last 7 days for each server.

The Performance Protection report comprises the following charts:

- Cisco CallManager Call Activity—A line chart displays the hourly rate of increase or decrease for number of calls that were attempted and calls that were completed as the number of active calls for each Cisco CallManager server. The chart comprises three lines, one for the number of calls that were attempted, one for the calls that were completed, and one for the active calls. If no data exists for call activity, Reporter does not generate the chart.
- Number of registered phones and MGCP gateways—A line chart displays the number of registered phones and MGCP gateways on each Cisco CallManager server. The chart comprises two lines, one for the number of registered phones and another for the number of MGCP gateways. If no data exists for phones or MGCP gateways, Reporter does not generate the chart.
- System Resource Utilization—A line chart displays the CPU load percentage and the percentage of memory that is used (in bytes) for the Cisco CallManager servers. The chart comprises two lines, one for the CPU load and one for the memory usage. Each line represents the cluster value, which is the average of the values for all the servers in the cluster (for which data is available). If no data exists for phones or MGCP gateways, Reporter does not generate the chart.
- Device and Dial Plan Quantities—Two tables display information from the Cisco CallManager database about the numbers of devices and number of dial plan components. The device table shows the number of IP phones, Unity connection ports, H.323 clients, H.323 gateways, MGCP gateways, MOH resources, and MTP resources. The dial plan table shows the number of directory numbers and lines, route patterns, and translation patterns.

Serviceability Reports Archive Configuration Checklist

Table 9-1 Trace Configuration and Collection Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Activate the Cisco Serviceability Reporter service. **Note** Because the Serviceability Reporter service is CPU intensive, Cisco recommends that you activate the service on a non-callprocessing server.	Activating and Deactivating Feature Services, *Cisco CallManager Serviceability Administration Guide*
Step 2	Configure the Cisco Serviceability Reporter service parameters.	Serviceability Reporter Service Parameters, page 9-2 *Cisco CallManager Administration Guide*
Step 3	View the reports generated by the Cisco Serviceability Reporter service.	Serviceability Reports Archive Configuration Checklist, *Cisco CallManager Serviceability Administration Guide*

Where to Find More Information

Related Topics

- Real-Time Monitoring Tool, page 5-1
- Real-Time Monitoring Configuration *Cisco CallManager Serviceability Administration Guide*
- Serviceability Reports Archive Configuration, *Cisco CallManager Serviceability Administration Guide*

PART 4

SNMP

CHAPTER 10

Simple Network Management Protocol

This chapter provides information on the following topics:

Simple Network Management Protocol Support

SNMP, an application layer protocol, facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

Note SNMP configuration parameters that you specified in Cisco CallManager 4.0 or Cisco CallManager 4.1 do not migrate during the Cisco CallManager 5.0 installation. You must perform the SNMP configuration procedures again.

In previous releases of Cisco CallManager, no graphical user interface existed in Cisco CallManager Serviceability for configuring Cisco CallManager SNMP settings. In Cisco CallManager 5.0, you use Cisco CallManager Serviceability to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. Likewise, in the SNMP configuration windows, you can apply the settings to all servers in the cluster; that is, if you want to do so.

This section contains information on the following topics:

SNMP Basics

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- Managed device—A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

  The first node in the Cisco CallManager cluster acts as the managed device.

- Agent—A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

  Cisco CallManager uses a master agent and subagent components to support SNMP. The master agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the master agent contains a few MIB variables that relate to MIB-II. The master agent also connects and disconnects subagents after the subagent completes necessary tasks. The SNMP master agent listens on port 161 and forwards SNMP packets for Vendor MIBs.

  The Cisco CallManager subagent interacts with the local Cisco CallManager only. The Cisco CallManager subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination.)

- Network Management System (NMS)—A SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. Cisco CallManager works with the following NMS:
  - CiscoWorks2000
  - HP OpenView
  - Third-party applications that support SNMP and Cisco CallManager SNMP interfaces

SNMP version 1 Support

SNMP version 1 (SNMPv1), the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI), operates over protocols, such as User Datagram Protocol (UDP) and Internet Protocol (IP).

The SNMPv1 SMI defines highly structured tables (MIBs) that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables contain zero or more rows, which are indexed, so SNMP can retrieve or alter an entire row with a supported command.

With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

In Cisco CallManager Serviceability, you configure SNMP v1 support in the V1/V2c Configuration window.

SNMP version 2c Support

As with SNMPv1, SNMPv2c functions within the specifications of the Structure of Management Information (SMI). MIB modules contain definitions of interrelated managed objects. The operations that are used in SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 Trap.

The Inform operation in SNMPv2c allows one NMS to send trap information to another NMS and to then receive a response from the NMS.

In Cisco CallManager Serviceability, you configure SNMP v2c support in the V1/V2c Configuration window.

SNMP version 3 Support

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested.) To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users, as described in the "SNMP Community Strings and Users" section on page 10-4.

In Cisco CallManager Serviceability, you configure SNMP v3 support in the V3 Configuration window.

Cisco CallManager SNMP Services

To support SNMP, Cisco CallManager uses the following services, which display in the Service Activation and/or Control Center windows in Cisco CallManager Serviceability.

- Cisco CCM SNMP service—This service provides SNMP access to provisioning and statistics information that is available for Cisco CallManager and implements the CISCO-CCM-MIB.

  If you use SNMP, activate this service on all servers in the cluster.

- SNMP Master Agent—This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.

Tip After you complete SNMP configuration in Cisco CallManager Serviceability, you must restart the SNMP Master Agent service in the Control Center—Network Features window.

- MIB2 Agent—This service provides SNMP access to variables that are defined in RFC 1213; for example, system, interfaces, IP and so on.
- Host Resources Agent—This service provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. This service implements the HOST-RESOURCES-MIB.
- System Application Agent—This service implements the SYSAPPL-MIB to provide a system-level view of the installed applications and their status.
- Native Agent Adaptor—This service allows you to forward requests from an SNMP Master agent to a Native SNMP agent running on the same system. Native SNMP agent supports vendor MIBs only.
- Cisco CDP Agent—This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco CallManager node. This service implements the CISCO-CDP-MIB.
- Cisco Syslog Agent—This service supports gathering of syslog messages that various Cisco CallManager components generate and enables syslog messages to be converted to SNMP traps. This service implements the CISCO-SYSLOG-MIB.

Caution Stopping any Cisco CallManager SNMP service may result in loss of data because the network management system no longer monitors the Cisco CallManager network. Do not stop the services unless the Cisco Technical Assistance Center tells you to do so.

SNMP Community Strings and Users

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. You configure SNMP community strings for SNMP v1 and v2c only.

SNMP v3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.

In Cisco CallManager 5.0, no default community string or user exists.

SNMP Traps and Informs

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowlegments from the destination whereas informs do receive acknowlegments. You must configure the notification destinations by using the SNMP Notification Destination Configuration windows.

The following list contains Cisco CallManager SNMP trap/inform messages that are sent to a configured trap destination:

- Cisco CallManager failed
- Phone failed
- Phones status update
- Gateway failed
- Media resource list exhausted
- Route list exhausted

- Gateway layer 2 change
- Quality report
- Malicious call
- Syslog message generated

Note Before you configure notification destination, verify that the required Cisco CallManager SNMP services are activated and running. Also, make sure that you have configured the privileges for the community string/user correctly.

Table 10-1 comprises information about Cisco CallManager trap/Inform parameters.

Table 10-1 Cisco CallManager Trap/Inform Configuration Parameters

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	Keep the default specification.
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change	None. The default specifies this trap as enabled.
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	Set the ccmPhoneStatusUpdateAlarmInterval to a value between 30 and 3600.
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	Set the ccmPhoneFailedAlarmInterval to a value between 30 and 3600.
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	None. The default specifies this trap as enabled.
ccmQualityReportAlarmEnable	True	ccmQualityReport **Note** This trap gets generated only if the Cisco Extended Functions service is activated and running on the local Cisco CallManager node.	None. The default specifies this trap as enabled.

Table 10-1 Cisco CallManager Trap/Inform Configuration Parameters (continued)

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
clogNotificationsEnabled	False	clogMessageGenerated	To enable trap generation, set clogNotificationsEnable to True.
clogMaxSeverity	Warning	clogMessageGenerated	When you set clogMaxSeverity to warning, a SNMP trap generates when Cisco CallManager applications generate a syslog message with at least a warning severity level.

SNMP Management Information Base (MIB)

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

The Cisco CallManager Simple Network Management Protocol (SNMP) extension agent resides in each Cisco CallManager node and exposes the CISCO-CCM-MIB that provides detailed information about devices that are known to the node. The CISCO-CCM-MIB provides device information such as device registration status, IP address, description, and model type for the node (not the cluster).

Cisco CallManager supports the following MIBs.

CISCO-CDP-MIB

Use the Cisco CallManager CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables Cisco CallManager to advertise itself to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- CdpGlobalDeviceId
- CdpInterfaceEnable
- CdpInterfaceMessageInterval
- CdpGlobalRun
- CdpGlobalMessageInterval
- CdpGlobalHoldTime

SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstalled
- sysApplRun
- sysApplMap

MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

The system supports trap functionality only. The Cisco Syslog Agent supports only the following objects of CISCO-SYSLOG-MIB:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

Vendor-Specific MIBs from HP

CPQAPLI.MIB, CPQCLUS.MIB, CPQCR.MIB, CPQFCA.MIB, CPQHLTH.MIB, CPQHOST.MIB, CPQIDA.MIB, CPQIDE.MIB, CPQNIC.MIB, CPQRECOV.MIB, CPQSCSI.MIB, CPQSINFO.MIB, CPQSM2.MIB, CPQSTAT.MIB, CPQSTDEQ.MIB, CPQSTSYS.MIB, CPQTHRSH.MIB, CPQUPS.MIB, ETHER.MIB, SVRCLU.MIB, SVRNTC.MIB, TOKEN.MIB

Vendor-Specific MIBs from IBM

UMSEVENT-MIB, UMSLMSSENSOR-MIB, HW-ENV-MONITORING-MIB

CISCO-CCM-MIB

The CISCO-CCM-MIB contains both dynamic (real-time) and configured (static) information about the local Cisco CallManager and its associated devices, such as phones, gateways, and so on. Simple Network Management Protocol (SNMP) tables contain information such as IP address, registration status, and model type.

To view the supports lists for the CISCO-CCM-MIB, click the following link:

ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

The following list of tables exists in the CISCO-CCM-MIB:

- ccmPhoneFailedTable, ccmPhoneStatusUpdateTable, ccmPhoneExtnTable, ccmPhoneTable

  For the Cisco IP Phone, the number of registered phones in ccmPhoneTable should match Cisco CallManager/ RegisteredHardware Phones perfmon counter. The ccmPhoneTable includes one entry for each registered, unregistered, or rejected Cisco IP Phone.

- ccmCTIDeviceTable, ccmCTIDeviceDirNumTable

  The ccmCTIDeviceTable stores each CTI device as one device. Based on the registration status of the CTI Route Point or CTI Port, the ccmRegisteredCTIDevices, ccmUnregisteredCTIDevices, and ccmRejectedCTIDevices counters in the Cisco CallManager MIB get updated.

- ccmSIPDeviceTable

  The CCMSIPDeviceTable stores each SIP trunk as one device.

- ccmH323Device

  The ccmH323DeviceTable contains the list of H323 devices for which the local Cisco CallManager contains information. For H.323 phones or H.323 gateways, the ccmH.323DeviceTable contains one entry for each H.323 device. (The H.323 phone and gateway do not register with Cisco CallManager. Cisco CallManager generates H.323Started alarm when it is ready to handle calls for the indicated H.323 phone and gateway.) The system provides the gatekeeper information as part of the H323 trunk information.

- ccmVoiceMailDeviceTable, ccmVoiceMailDirNumTable

  For Cisco uOne, ActiveVoice, the ccmVoiceMailDeviceTable has one entry for each voice-messaging device. Based on the registration status, the ccmRegisteredVoiceMailDevices, ccmUnregisteredVoiceMailDevices, and ccmRejectedVoiceMailDevices counters in the Cisco CallManager MIB get updated.

- ccmGatewayTable

  The ccmRegisteredGateways, ccmUnregistered gateways, and ccmRejectedGateways keep track of the number of registered gateway devices or ports, number of unregistered gateway devices or ports, and number of rejected gateway devices or ports, respectively.

  Cisco CallManager generates alarms at the device or port level. The ccmGatewayTable, based on Cisco CallManager alarms, contains device- or port-level information. Each registered, unregistered, or rejected device or port has one entry in ccmGatewayTable. The VG200 with two FXS ports and one T1 port has three entries in ccmGatewayTable. The ccmActiveGateway and ccmInActiveGateway counters track number of active (registered) and lost contact with (unregistered or rejected) gateway devices or ports.

  Based on the registration status, ccmRegisteredGateways, ccmUnregisteredGateways, and ccmRejectedGateways counters get updated.

- ccmProductTypeTable

  The table contains the list of product types that are supported in a Cisco CallManager cluster, including phone types, gateway types, media device types, H323 device types, CTI device types, voice-messaging device types and SIP device types.

Note The dynamic tables such as phoneTable, gatewayTable, and so on, get populated only if the local Cisco CallManager service is up and running. The static tables such as region, timezone, devicepool, and so on, in the Cisco CallManager MIB, get populated when the Cisco CallManager SNMP service is running.

Note The "ccmAlarmConfigInfo" and "ccmQualityReportAlarmConfigInfo" groups in the CISCO-CCM-MIB define the configuration parameters that relate to the notifications that the "SNMP Traps and Informs" section on page 10-4 describes.

SNMP Trace Configuration

In Cisco CallManager Serviceability, you can configure trace for Cisco CCM agent. A default setting exists for all the agents. For Cisco CDP Agent and Cisco Syslog Agent, you can use CLI to change trace settings.

SNMP Configuration Checklist

Table 10-2 provides an overview of the steps for configuring SNMP.

Table 10-2 SNMP Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Install and configure the SNMP NMS.	SNMP product documentation that supports the NMS
Step 2	In the Control Center window, verify that the system started the Cisco CallManager SNMP services.	• Cisco CallManager SNMP Services, page 10-3 • Service Management, page 2-1 • Managing Services, *Cisco CallManager Serviceability Administration Guide*
Step 3	In the Service Activation window, activate the Cisco CCM SNMP service.	• Cisco CallManager SNMP Services, page 10-3 • Service Management, page 2-1 • Managing Services, *Cisco CallManager Serviceability Administration Guide*
Step 4	If you are using SNMP v1/v2c, configure the community string.	SNMP Community String Configuration, *Cisco CallManager Serviceability Administration Guide*
Step 5	If you are using SNMP v3, configure the SNMP user.	SNMP User Configuration, *Cisco CallManager Serviceability Administration Guide*

Table 10-2 SNMP Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 6	Configure the notification destination for traps or Informs.	• For SNMP v1/v2c—SNMP Notification Destination Configuration for V1/V2c, *Cisco CallManager Serviceability Administration Guide* • For SNMP v3—SNMP Notification Destination Configuration for V3, *Cisco CallManager Serviceability Administration Guide* • SNMP Traps and Informs, page 10-4
Step 7	Configure the system contact and location for the MIB2 system group.	MIB2 System Group Configuration, *Cisco CallManager Serviceability Administration Guide*
Step 8	Restart the Master Agent service.	• Cisco CallManager SNMP Services, page 10-3 • Service Management, page 2-1 • Managing Services, *Cisco CallManager Serviceability Administration Guide*
Step 9	On the NMS, configure the Cisco CallManager trap parameters.	SNMP product documentation that supports the NMS

Troubleshooting

Review this section for troubleshooting tips.

Make sure that all of the feature and network services listed in "Cisco CallManager SNMP Services" section on page 10-3 are running.

Cannot poll any MIBs from the system

This condition means that the community string or the snmp user is not configured on the system or they do not match with what is configured on the system.

Note By default, no community string or user is configured on the system.

Check whether the community string or snmp user is properly configured on the system by using the SNMP configuration windows.

Cannot receive any notifications from the system

This condition means that the notification destination is not configured correctly on the system.

Verify that you configured the notification destination properly in the Notification Destination (V1/V2c or V3) Configuration window.

Where to Find More Information

Related Topics

- Service Management, page 2-1
- Managing Services, *Cisco CallManager Serviceability Administration Guide*
- SNMP V1/V2c Configuration, *Cisco CallManager Serviceability Administration Guide*
- SNMP V3 Configuration, *Cisco CallManager Serviceability Administration Guide*
- MIB2 System Group Configuration, *Cisco CallManager Serviceability Administration Guide*

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

T

Z