CHAPTER 1

Overview

This chapter gives a conceptual overview of Cisco Unified Communications Manager (Cisco Unified CM) and Cisco Unified CM Business Edition 5000, possible deployment models, Simple Network Management Protocol (SNMP) including traps, Management Information Bases (MIBs), syslogs, and alerts/alarms. It contains the following sections:

Cisco Unified Communications Manager

The Cisco Unified CM serves as the software-based call-processing component of the Cisco Unified Communications family of products. A wide range of Cisco Media Convergence Servers provides high-availability server platforms for Cisco Unified Communications Manager call processing, services, and applications.

The Cisco Unified CM system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco Unified CM open telephony application programming interface (API).

Cisco Unified CM provides signaling and call control services to Cisco integrated telephony applications as well as third-party applications. Cisco Unified CM performs the following primary functions—

- Call processing
- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services

- Operations, administration, maintenance, and provisioning (OAM&P)
- Programming interface to external voice-processing applications such as Cisco IP Communicator, Cisco Unified IP Interactive Voice Response (IP IVR), and Cisco Unified Communications Manager Attendant Console

Supported Deployment Models

Three types of Cisco Unified CM supported deployments exist—Single site, multisite WAN with centralized call processing, and multisite WAN with distributed call processing. The following paragraphs describe each of these:

- Single Site—Consists of a call processing agent cluster that is located at a single site, or campus, with *no* telephony services that are provided over an IP WAN. An enterprise would typically deploy the single-site model over a LAN or metropolitan area network (MAN), which carries the voice traffic within the site. In this model, calls beyond the LAN or MAN use the public switched telephone network (PSTN).
- Multisite WAN with Centralized Call Processing—Consists of a single call processing agent cluster that provides services for many remote sites and uses the IP WAN to transport Cisco Unified Communications traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites.
- Multisite WAN with Distributed Call Processing—Consists of multiple independent sites, each with its own call processing agent cluster that is connected to an IP WAN that carries voice traffic between the distributed sites.

Cisco Unified CMBE supports three main types of deployment models—Single-site, multisite WAN with centralized call processing, and multisite WAN deployment with distributed call processing. Cisco Unified CMBE is a single-platform deployment, running both Cisco Unified CM and Cisco Unity Connection on the same server. Each type is described in the following paragraphs:

- Single-Site—Consists of Cisco Unified CM and Cisco Unity Connection running on the same hardware platform located at a single site or campus, with no telephony services provided over an IP WAN.
- Multisite WAN with Centralized Call Processing—Consists of a single call processing appliance that provides services for up to 20 sites (one central site and 19 remote sites), and this model uses the IP WAN to transport IP telephony traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites.
- Multisite WAN with Distributed Call Processing—Consists of independent sites, each with its own call processing agent connected to an IP WAN that carries voice traffic between the distributed sites. The multisite WAN deployment with distributed call processing enables Cisco Unified CMBE to operate with Cisco Unified CM or other Cisco Unified CMBE deployments. With this model, Cisco Unified CMBE supports the use of H.323 intercluster trunks as well as SIP trunks to interconnect with Cisco Unified CM deployments or other Cisco Unified CMBE deployments. Each site can be a single site with its own call processing agent, a centralized call processing site and all of its associated remote sites, or a legacy PBX with Voice over IP (VoIP) gateway.

Managed Services

Two general types of managed services exist:

- Basic services that provide connectivity to the network—Routing, Domain Name System (DNS), and quality of service (QoS).
- High-valued services that the Service Provider offers to its customers—Videoconferencing, mobile IP, VPNs, VoIP, and Wireless. The high-valued services use the basic services as a backbone.

The service provider may require these server types and services:

- Web server with the ability to display web pages, even during high usage hours, to meet the demands of customers. The web pages get used to pay bills, check minutes of usage in the case of a cell phone, and buy new products. The web server and application server work together to display information that the service provider customer requires.
- Dedicated application server with the ability to advise customers when a product is out of stock, when bill is past due, or when need arises to buy more minutes.
- Mail server with the ability to notify customers to confirm an order or send a receipt for purchases.
- Secure gateway with VPN with the ability to have secure communications between the service provider and its customers and suppliers.

Be aware that any one of these services is critical to the operations of a service provider. Managing these services to ensure continuous operation requires a system that monitors fault, configuration, performance and security across all of the network elements. The introduction of element-to-element synchronization and the issues of using different vendor products complicates the task.

Cisco Unified Serviceability and SNMP attempt to address some of these network management issues:

- Are infrastructure elements functioning? If not, which are failing?
- What cause the failure? For example, recent configuration changes.
- What is the impact of the failure on the network as a whole and the impact on the elements within the network?
- What is the impact of the failure on services and customers?
- How long to correct the failure?
- Are there backup facilities?
- Are there any pending failures?
- How many packets were sent and received on a particular device? How many web pages were accessed.
- How were other devices used—how often and how long?

Cisco Unified CM supports SNMP v1, v2, and v3. SNMP remotely monitors, configures, and controls networks. SNMP sends fault messages to assigned managers as SNMP trap or inform request Protocol Data Units (PDUs). For more information, see Chapter 4, “Simple Network Management Protocol.”

Cisco Unified Serviceability, a component of Cisco Unified CM Administration includes its own set of error messages and alarms. Both applications use Management Information Base (MIB) text files to manage alarms and alerts, notifications, and error messages. For more information, see Chapter 6, “Cisco Unified Serviceability Alarms and CiscoLog Messages.”

Cisco Unified Serviceability

Cisco Unified Serviceability, a web-based troubleshooting tool, enables the following functions:

- Saves alarms and events for troubleshooting and provides alarm definitions.
- Saves trace information to various log files for troubleshooting.
- Monitors real-time behavior of components by using the Cisco Unified Real-Time Monitoring Tool (RTMT).
- Provides feature services that you can activate, deactivate, and view through the Service Activation window.
- Provides an interface for starting and stopping feature and network services.
- Generates and archives daily reports; for example, alert summary or server statistic reports.
- Allows Cisco Unified Communications Manager to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a server.
- Monitors the number of threads and processes in the system; uses cache to enhance the performance.

For information about configuring service parameters, refer to the *Cisco Unified Communications Manager Administration Guide*. For information about configuring Serviceability features, refer to the *Cisco Unified Serviceability Administration Guide*.

This section contains the following topics:

Trace Tools

Trace tools assist you in troubleshooting issues with your voice application. Cisco Unified Serviceability supports SDI (System Diagnostic Interface) trace, SDL (Signaling Distribution Layer) trace for Cisco CallManager and Cisco CTIManager services, 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 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.

In the Alarm Configuration window, you can direct alarms to various locations, including SDI trace log files or SDL trace log files. If you want to do so, you can configure trace for alerts in the RTMT. 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 RTMT.

Troubleshooting Trace

The Troubleshooting Trace Settings window allows you to choose the services in Cisco Unified Serviceability for which you want to set predetermined troubleshooting trace settings. In this window, you can choose a single service or multiple services and change the trace settings for those services to the predetermined trace settings.

If you have clusters (Cisco Unified Communications Manager only), you can choose the services on different Cisco Unified Communications Manager servers in the cluster, so the trace settings of the chosen services get changed to the predetermined trace settings. You can choose specific activated services for a single server, all activated services for the server, specific activated services for all servers in the cluster, or all activated services for all servers in the cluster. In the window, N/A displays next to inactive services.

When you open the Troubleshooting Trace Settings window after you apply troubleshooting trace settings to a service, the service that you set for troubleshooting displays as checked. In the Troubleshooting Trace Settings window, you can reset the trace settings to the original settings.

After you apply Troubleshooting Trace Setting to a service, the Trace Configuration window displays a message that troubleshooting trace is set for the given service(s). From the Related Links drop-down list box, you can choose the Troubleshooting Trace Settings option if you want to reset the settings for the service. For the given service, 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 after you apply troubleshooting trace settings.

Trace Collection

Use Trace and Log Central, an option in the RTMT, to collect, view, and zip various service traces and/or other log files. With the Trace and Log Central option, you can collect SDL/SDI traces, Application Logs, System Logs (such as Event View Application, Security, and System logs), and crash dump files.

For more information on trace collection, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Cisco Unified Reporting

Cisco Unified Reporting web application, which is accessed at the Cisco Unified Communications Manager console, generates reports for troubleshooting or inspecting cluster data. This tool provides a snapshot of cluster data without requiring multiple steps to find the data. The tool design facilitates gathering data from existing sources, comparing the data, and reporting irregularities.

A report combines data from one or more sources on one or more servers into one output view. For example, you can view a report that shows the hosts file for all servers in the cluster. The application gathers information from the publisher server and each subscriber server. A report provides data for all active cluster nodes that are accessible at the time that the report is generated.

Some reports run checks to identify conditions that could impact cluster operations. Status messages indicate the outcome of every data check that is run.

Only authorized users can access the Cisco Unified Reporting application. By default, this includes administrator users in the Standard Cisco Unified CM Super Users group. As an authorized user, you can view reports, generate new reports, or download reports at the graphical user interface (GUI).

Administrator users in the Standard Cisco Unified CM Super Users group can access all administrative applications in the Cisco Unified Communications Manager Administration navigation menu, including Cisco Unified Reporting, with a single sign onto one of the applications.

Cisco Unified Reporting includes the following capabilities:

- A user interface for generating, archiving, and downloading reports
- Notification message if a report will take excessive time to generate or consume excessive CPU

Generated reports in Cisco Unified Reporting may use any of the following data sources:

- RTMT counters
- CDR CAR
- Cisco Unified CM DB
- Disk files
- Operating System API calls
- Network API calls
- Prefs (Windows registry)
- CLI
- RIS

Cisco Unified Real-Time Monitoring Tool

RTMT is a client-side application that uses HTTPS and TCP to monitor system performance, device status, device discovery, CTI applications, and voice messaging ports. RTMT can connect directly to devices by using HTTPS to troubleshoot system issues. RTMT performs the following tasks:

- Monitor a set of predefined management objects that monitor the health of the system.
- 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.

In addition to SNMP traps, RTMT can monitor and parse syslog messages that are provided by the hardware vendors, and then send these alerts to RTMT Alert Central. You can configure RTMT to notify the Cisco Unified CM system administrator if and when the alerts occur. You can configure the notifications for e-mail or Epage or both.

For more information, refer to *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Call Detail Records and Call Management Records

Call Detail Records (CDRs) and Call Management Records (CMRs) get used for post-processing activities such as generating billing records and network analysis. When you install your system, the system enables CDRs by default. CMRs remain disabled by default. You can enable or disable CDRs or CMRs at any time that the system is in operation.

The CDR Management (CDRM) feature, a background application, supports the following capabilities:

- Collects the CDR/CMR files from the Cisco Unified Communications Manager server or node to the CDR Repository server or node.
- Collects and maintains the CDR/CMR files on the server where you configure CAR.
- Maintains the CDR/CMR files on the CDR Repository node or CDR server.
- Allows third-party applications to retrieve CDR/CMR files on demand through a SOAP interface.
- Accepts on-demand requests for searching file names.
- Pushes CDR/CMR files from individual nodes within a cluster to the CDR Repository server or node.
- Sends CDR/CMR files to up to three customer billing servers via FTP/SFTP.
- Monitors disk usage of CDR/CMR files on the server where you configure CAR or on the CDR Repository server or node.
- Periodically deletes CDR/CMR files that were successfully delivered. You can configure the amount of storage that is used to store flat files. Predefined storage limits exist. If the storage limits are exceeded, the CDR Repository Manager deletes old files to reduce the disk usage to the preconfigured low water mark. The post-processing applications can later retrieve the buffered historical data to re-get any lost, corrupted, or missing data. The CDRM feature, which is not aware of the flat file format, does not manipulate the file contents.

CDRM includes two default services, the CDR Agent and the CDR Repository Manager, and one activate service, CDR onDemand Service.

For more information, refer to the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.

Call Detail Record Analysis and Reporting

Cisco Unified Serviceability supports Call Detail Record (CDR) Analysis and Reporting (CAR) and is is available in the Tools menu. CAR generates reports for Quality of Service (QoS), traffic, and billing information. For its primary function, CAR generates reports about the users of Cisco Unified Communications Manager and reports on system status with respect to call processing. CAR also performs CAR database management activities. You can perform these tasks in one of the following ways:

- Automatically configure the required tasks to take place.
- Manually perform the tasks by using the web interface.

CAR processes the CDRs from flat files that the CDR repository service places in the repository folder structure. CAR processes CDRs at a scheduled time and frequency. By default, CDR data loads continuously 24 hours per day and 7 days per week; however, you can set the loading time, interval, and duration as needed. In addition, the default setting loads only CDR records. CMR records do not get loaded by default.

CAR provides e-mail alerts for various events, including the following events:

- Charge Limit Notification indicates when the daily charge limit for a user exceeds the specified maximum.
- QoS Notification indicates when the percentage of good calls drops below a specified range or the percentage of poor calls exceeds a specified limit.

For more information, refer to the *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*.

Management Information Base

The Management Information Base (MIB) converts object identifiers (OIDs) that are numerical strings into an ASCII text file. The OIDs identify data objects. The OID represents specific characteristics of a device or application and can have one or more object instances (variables). Managed objects, alarms, notifications, and other valuable information get identified by the OID and get listed in the MIB.

The OID gets logically represented in a tree hierarchy. The root of the tree stays unnamed and splits into three main branches—Consultative Committee for International Telegraph and Telephone (CCITT), International Organization for Standardization (ISO), and joint ISO/CCITT.

These branches and those that fall below each category have short text strings and integers to identify them. Text strings describe object names, while integers allow computer software to create compact, encoded representations of the names. For example, the Cisco MIB variable authAddr represents an object name and gets denoted by the number 5, which is listed at the end of OID 1.3.6.1.4.1.9.2.1.5.

The OID in the Internet MIB hierarchy represents the sequence of numeric labels on the nodes along a path from the root to the object. The OID 1.3.6.1.2.1 represents the Internet standard MIB. It also can get expressed as iso.org.dod.internet.mgmt.mib.

The Cisco MIB set comprises a collection of variables that are private extensions to the Internet standard MIB II and many other Internet standard MIBs. RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets—MIB-II* documents MIB II.

Cisco Unified CM and Cisco Unified CMBE support the following MIBs:

- CISCO-CCM-MIB
- CISCO-CCM-CAPABILITY
- CISCO-CDP-MIB
- CISCO-SYSLOG-MIB
- HOST-RESOURCES-MIB
- MIB-II
- SYSAPPL-MIB
- Vendor-specific MIBs

For descriptions of the supported MIBs, see the following chapters:

- Chapter 7, “Cisco Management Information Base”
- Chapter 8, “Industry-Standard Management Information Base”
- Chapter 9, “Vendor-Specific Management Information Base”