Network Management

Revised: March 1, 2018

Network management is a service consisting of a wide variety of tools, applications, and products to assist network system administrators in provisioning, operating, monitoring and maintaining new and existing network deployments. A network administrator faces many challenges when deploying and configuring network devices and when operating, monitoring, and reporting on the health of the network infrastructure and components such as routers, servers, switches and so forth. Network management helps system administrators monitor each network device and network activity so that they can isolate and investigate problems in a timely manner for better performance and productivity.

With the convergence of rich media and data, the need for unified management is greater than ever. The Cisco Prime Collaboration (Prime Collaboration) offers a set of integrated tools that help to test, deploy, and monitor Cisco Unified Communications and TelePresence systems. Prime Collaboration implements the various management phases to strategically manage the performance and availability of Cisco Unified Communications applications including voice, video, contact center, and rich media applications. The network management phases typically include: plan, design, implement, and operate (PDIO). Table 27-1 lists the PDIO phases and the major tasks involved with each phase.

Table 27-1 Network Management Phases and Tasks

Plan & Design	Implement	Operate
Assess the network infrastructure for Cisco Unified Communications capability. For example, predict overall call quality. Prepare the network to support Cisco Unified Communications. Analyze network management best practices.	Deploy and provision Cisco Unified Communications. For example, configure the dial plan, partitioning, user features, and so forth. Enable features and functionality on the existing infrastructure to support Cisco Unified Communications.	Manage changes for users, services, IP phones, and so forth. Generate reports for operations, capacity planning, executive summaries, and so forth. Track and report on user experiences. For example, use sensors to monitor voice quality. Monitor and diagnose problems such as network failures, device failures, call routing issues, and so forth.

This chapter provides the design guidance for the following management tools and products that fit into the implementation and operation phases of Cisco Unified Communications Management:

- Cisco Prime Collaboration manages provisioning of initial deployments and ongoing operational activation for Unified Communications and TelePresence services. Cisco Prime Collaboration provides comprehensive monitoring with proactive and reactive diagnostics for the entire Cisco Unified Communications system. It also provides a reliable method of monitoring and evaluating voice quality in Cisco Unified Communications systems. For details, refer to the related product documentation available at

  https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

- Cisco TelePresence Management Suite (TMS) offers visibility and centralized control of your telepresence videoconferencing network, including remote systems. For details, refer to the related product documentation available at

  https://www.cisco.com/c/en/us/products/conferencing/telepresence-management-suite-tms/index.html

For information on which software versions are supported with Cisco Unified Communications Manager (Unified CM), refer to the latest version of the *Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service*, available at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html

What's New in This Chapter

Table 27-2 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 27-2 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:	Revision Date
Cisco Prime License Manager has been replaced by Cisco Smart Software Licensing	Cisco Smart Software Licensing, page 27-21	March 1, 2018
Other minor corrections and updates	Various sections of this chapter	March 1, 2018

Cisco Prime Collaboration

Cisco Prime Collaboration provides comprehensive voice and video network monitoring with diagnostics for the Cisco Collaboration systems, including the underlying transport infrastructure. Prime Collaboration is a converged application that eliminates the need to manage the video deployments separately from voice. It is delivered as two separate applications, Prime Collaboration Assurance and Prime Collaboration Provisioning, which are installed on separate virtual machines. Prime Collaboration is available in two modes: Standard and Advanced mode.

Prime Collaboration Assurance application provides:

- End-to-end service monitoring for Cisco Collaboration applications
- Real-time service troubleshooting and diagnostics for Cisco TelePresence systems and phones
- Video service readiness assessment

- Diagnostics tests using Cisco IP Service Level Agreements (IP SLA) and Video SLA Assessment Agent (VSAA)
- Service-level and inventory reports for voice and video systems

Note Prime Collaboration Assurance Advanced also includes Prime Collaboration Analytics. If you have purchased the Prime Collaboration Analytics license, you can access the Prime Collaboration Analytics dashboards. Prime Collaboration Analytics helps you identify traffic trends, technology adoption trends, and over/under-utilized resources in your network. You can also track intermittent and recurring network issues and address service quality issues.

Prime Collaboration Provisioning application provides:

- Standard services (phone, line, and voicemail, for example) to be ordered for subscribers (the owner of the individual phone, voicemail, or other service)
- Configuration templates that provide the ability to auto-configure the Cisco Unified Communications voice infrastructure in a consistent way
- Easy addition of the Provisioning application to an existing Cisco Unified Communications network
- Simplified policy-driven Day 2 provisioning interface to move, add, delete, or change phone users
- A Self-Care feature that enables end users to modify personal options quickly and easily

For information on the benefits and key features of Prime Collaboration and guidelines for deployment (white papers), refer to the Cisco Prime Collaboration documentation available at

https://www.cisco.com/go/primecollaboration

Failover and Redundancy

Prime Collaboration does not currently support failover. However, it can support Network Fault Tolerance when deployed on server platforms with dual Ethernet network interface cards (NICs) that support NIC teaming. This feature allows a server to be connected to the Ethernet through two NICs and, therefore, two cables. NIC teaming prevents network downtime by transferring the workload from the failed port to the working port. NIC teaming cannot be used for load balancing or for increasing the interface speed.

Prime Collaboration Assurance provides geographic redundancy through the use of VMware vSphere replication. It requires VMware activation at remote sites only.

Cisco Prime Collaboration Server Performance

Prime Collaboration runs only in a virtual environment and it requires a minimum of one virtual machine per component. If you want Assurance and Provisioning, you will need two virtual machines (one for each). For specific system requirements and capacity information, refer to the latest version of the *Cisco Prime Collaboration Provisioning Install and Upgrade Guide*, available at

https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html

Network Infrastructure Requirements for Cisco Collaboration and Network Management Applications

Cisco highly recommends that you enable Domain Name Service (DNS) in the network to perform a reverse lookup on the IP address of the device to get the hostname for the device. If DNS is not desired, then host files may be used for IP address-to-hostname resolution.

Network Time Protocol (NTP) must be implemented to allow network devices to synchronize their clocks to a network time server or network-capable clock. NTP is a critical network service for network operation and management because it ensures accurate time-stamps within all logs, traps, polling, and reports on devices throughout the network.

You should enable Cisco Discovery Protocol (CDP) within the network to ensure proper monitoring. Prime Collaboration's automated device discovery is based on a CDP table. Ping Sweep may be used instead of CDP, but IP phones discovered using Ping Sweep are reported in "unmanaged" state. Simple Network Management Protocol (SNMP) must also be enabled on network devices to allow Prime Collaboration to get information on network devices at configured polling intervals and to receive alerts and faults via trap notification sent by the managed devices.

For more information on Cisco Unified Communications network requirements, see the chapter on Network Infrastructure, page 3-1.

Assurance

Cisco Prime Collaboration Assurance is a comprehensive video and voice service assurance and management system with a set of monitoring, troubleshooting, and reporting capabilities that help ensure end users receive a consistent, high-quality video and voice collaboration experience. Prime Collaboration Assurance is available in two modes: Standard and Advanced.

Prime Collaboration Advanced provides all the features that enable integrated assurance management of applications and the underlying transport infrastructure. This includes real-time monitoring and troubleshooting of Cisco TelePresence solutions and the entire Unified Communications system.

Prime Collaboration Standard provides basic assurance features that help you manage Unified Communications and TelePresence components. The features include:

- Support for Unified Communications components including voicemail and IM and Presence
- Fault monitoring for core Unified Communications components (Cisco Unified CM and Cisco Unity Connection)
- Pre-configured and customizable performance metrics dashboards that display term trends for core Unified Communications components
- Support for TelePresence components, including Cisco TelePresence Video Communication Server (VCS)
- Contextual cross-launch of serviceability pages of Unified Communications components
- Single-level role-based access control (RBAC)

Prime Collaboration Standard also includes the following features to help you manage the Unified Communications and TelePresence components:

- Device Inventory Management

  You can discover and manage endpoints that are registered to Cisco Unified Communications Manager (phones and TelePresence endpoints), Cisco TelePresence VCS, and Cisco TelePresence Management Suite (TMS). As part of the discovery, the device details are also retrieved and stored in the Prime Collaboration database. After the discovery is complete, you can perform the following device management tasks:

  – Add or remove devices

  – Manage device credentials

  – Discover devices

- Monitoring and Fault Management

  Service operators need to quickly isolate the source of any service degradation in the network for all voice and video sessions in an enterprise. Prime Collaboration provides a detailed analysis of the service infrastructure and network-related issues.

  Prime Collaboration periodically imports information from the managed devices based on the polling parameters you configure.

  The Home page includes several pre-configured dashlets that help you monitor system performance, device status, device discovery, CTI applications, and voice messaging ports. These dashlets enable you to monitor a set of predefined management objects that monitor the health of the system. From the dashlets, you can launch contextual serviceability pages.

  Prime Collaboration ensures near real-time quick and accurate fault detection. Prime Collaboration enables you to monitor the events that are of importance to you. You can set up Prime Collaboration to send notifications for alarms.

  In addition to the faults that are present in the Cisco TelePresence Management System and Unified Communications applications, it also displays the custom tickets that are raised on Cisco TMS.

  Using the Alarm browser, you can view the alarms and events in the system and initiate troubleshooting. You can also configure Prime Collaboration to send fault notifications, and you can view call connection/disconnection details related to the Cisco TMS applications in the Call Events UI.

Cisco Prime Collaboration Assurance provides a unified view of the entire Cisco Unified Communications infrastructure and presents the current operational status of each element of the Cisco Unified Communications network. Prime Collaboration also provides diagnostic capabilities for faster problem isolation and resolution. In addition to monitoring Cisco gateways, routers, and switches, Prime Collaboration continuously monitors the operational status of various Cisco Unified Communications elements such as:

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unified Communications Manager Express (Unified CME)
- Cisco Unified Communications Manager Session Management Edition
- Cisco Unity Connection
- Cisco Unity Express

- Cisco Unified Contact Center Enterprise (Unified CCE), Unified Contact Center Express (Unified CCX), and Unified Customer Voice Portal (Unified CVP)

Note Cisco Prime Collaboration Service Level View does not support multiple Cisco Unified Contact Center Enterprise (Unified CCE) deployments.

- Cisco IM and Presence
- Cisco Emergency Responder
- Cisco Unified Border Element
- Cisco Unified Endpoints

Note Cisco Prime Collaboration supports Unified Communications and TelePresence applications running in a virtualized environment but does not provide monitoring of VMware or hardware. Use vCenter for managing VMware hosts. For Unified Computing System (UCS) B-series Blade servers, UCS Manager provides unified, embedded management of all software and hardware components in the Cisco UCS. It controls multiple chassis and manages resources for thousands of virtual machines. For UCS C-series servers, the Cisco Integrated Management Controller provides the management service.

For more information on the supported products (particularly Cisco endpoints) and versions supported by Prime Collaboration, refer to the Cisco Prime Collaboration data sheet available at

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

One protocol that Prime Collaboration uses to monitor the Unified Communications elements is Simple Network Management Protocol (SNMP). SNMP is an application-layer protocol using UDP as the transport layer protocol. There are three key elements in SNMP managed network:

- Managed devices — Network devices that have an SNMP agent (for example, Unified CM, routers, switches, and so forth).
- Agent — A network management software module that resides in a managed device. This agent translates the local management information on the device into SNMP messages.
- Manager — Software running on a management station that contacts different agents in the network to get the management information (for example, Prime Collaboration).

The SNMP implementation supports three versions: SNMP v1, SNMP v2c, and SNMP v3. SNMP v3 supports authentication, encryption, and message integrity. SNMP v3 may be used if security is desired for management traffic. Prime Collaboration supports all three versions of SNNP. SNMP v1 and v2c read/write community strings or SNMP v3 credentials must be configured on each device for agent and manager to communicate properly. Prime Collaboration needs only SNMP read access to collect network device information.

For more information on SNMP, refer to the Cisco Prime Collaboration documentation available at

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

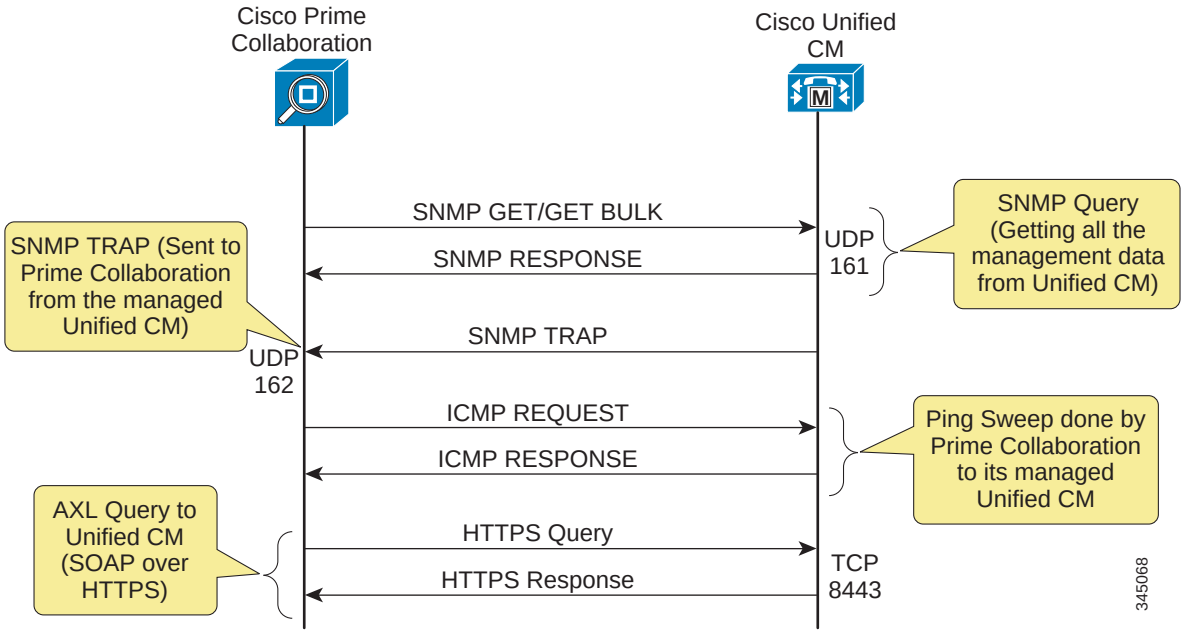
Assurance Design Considerations

Cisco Prime Collaboration interfaces with other devices in the network in the following ways:

- Simple Network Management protocol (SNMP) to manage all Cisco Unified Communications servers, gateways, and switches.
- Administrative XML Layer (AXL) to manage Unified CM. AXL is implemented as a Simple Object Access Protocol (SOAP) over HTTPS web service.
- HTTP to the IP phone to collect serial number and switch information. HTTP must be enabled on the IP phones.
- Enhanced event processing with Cisco Unified CM remote syslog integration, and leveraging the Cisco Real-Time Monitoring Tool (RTMT) interface for pre-collected Unified CM cluster-wide data
- Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) to Cisco Unified IP Phones for synthetic tests.
- Internet Control Message Protocol (ICMP) or Ping Sweep for Cisco IOS routers and switches, and for other voice as well as non-voice devices.

Figure 27-1 shows the system-level overview of how Prime Collaboration leverages multiple interfaces with Unified CM to gather performance counters and alarms.

Figure 27-1 Prime Collaboration and Unified CM System-Level Integration



Call Quality Monitoring (Service Experience)

Cisco Prime Collaboration Assurance Advanced monitors the quality of calls on the Cisco Unified Communications network. It relies on Unified CM and Network Analysis Modules (NAMs) to monitor and gather quality statistics on real calls rather than simulated calls in the network. Then it compares the collected quality statistics against predefined thresholds.

Prime Collaboration Assurance Advanced is also responsible for sending voice quality information to Cisco Prime Analytics (available only with Prime Collaboration Advanced) so that Analytics can perform call data analysis and generate reports.

Note A set of global call quality thresholds can be defined as one per supported codec type. Different thresholds can be grouped together based on the Unified CM cluster being monitored.

Voice Quality Measurement

Voice quality is the qualitative and quantitative measure of the sound and conversational quality of the IP phone call. Voice quality measurement describes and evaluates the clarity and intelligibility of voice conversations. Prime Collaboration uses the Network Analysis Module (NAM) and Unified CM to monitor and report voice quality information.

Unified CM Call Quality Monitoring

Unified CM stores end-of-call video and audio information and metrics in its call detail records (CDRs) and call management records (CMRs). The CMRs and CDRs are transferred to Prime Collaboration via Secure File Transfer Protocol (SFTP) every 60 seconds. To integrate with Unified CM, Prime Collaboration must be configured as a Billing Application Server in the Unified CM Unified Serviceability configuration web page. Up to three Billing Application Servers can be configured per Unified CM cluster. The following settings must be configured for the Billing Application Server:

- Hostname or IP address of the Prime Collaboration Assurance virtual machine
- Username and password for SFTP file transfer
- Protocol: SFTP
- Directory path on the Prime Collaboration virtual machine to which CDR and CMR files are transferred

Note Cisco Jabber and endpoints running Cisco CE or TE software do not generate end-of-call audio and video information. Thus, there are no CMRs for these endpoints.

In the past, the emphasis was on using the Cisco Voice Transmission Quality (CVTQ) algorithm as one means to monitor voice quality. CVTQ is based on the Klirrfaktor (K-factor) method to estimate the MOS value of voice calls. With Cisco CSR 12.*x*, packet counts, concealment ratios, and concealment second counters represent primary statistics because they can alert the network operator before network impairment has an audible impact or is visible through MOS. Table 27-3 describes these counters as well as metrics computed from them.

Table 27-3 Counters and Metrics to Measure Call Quality

Counter or Metric	Description
Concealment	Measures packet (frame) loss and its effect on voice quality in an impaired network
CS – concealed seconds	Number of seconds when there is some concealment (might not be audible)
SCS – severely concealed seconds	Number of seconds when loss is greater than 5% (audible)
SCSR (SCS Ratio) – SCS/Duration	Metric to measure voice quality
CSR (CS Ratio) – CS/Duration	Metric to measure network quality

As noted in Table 27-3, SCSR represents a measure of voice quality and is used by Prime Assurance to grade calls. For calls less than 20 seconds in duration, the following SCSR values are used to estimate call quality:

Grade	SCSR Value
Good	Less than 0.20
Acceptable	0.20 <= SCSR <= 0.30
Poor	Greater than 0.30

For calls of 20 seconds or longer in duration, the following SCSR values are used to estimate call quality:

Grade	SCSR Value
Good	Less than 0.03
Acceptable	0.03 <= SCSR <= 0.07
Poor	Greater than 0.07

Cisco Network Analysis Module (NAM)

Cisco NAM is a traffic analysis module that leverages Remote Monitoring (RMON) and some SNMP Management Information Bases (MIBs) to enable network administrators to view all layers of the Unified Communications infrastructure to monitor, analyze, and troubleshoot applications and network services such as QoS for voice and video applications. Voice instrumentation added in Cisco NAM 4.0 enables NAM integration with Prime Collaboration for call metrics through NAM-embedded data collection and performance analysis.

The Cisco NAM complements Prime Collaboration to deliver an enterprise-wide voice management solution. The NAM Appliances come with a graphical user interface for troubleshooting and analysis, and they provide a rich feature set for voice quality analysis with RTP and voice control and signaling monitoring.

Cisco Prime Collaboration polls the NAM every 60 seconds for voice quality metrics. It then does a MOS calculation on the data. This enables Prime Collaboration to correlate CDR and call stream reports from the NAM for enhanced analysis.

For more information on Cisco NAM, refer to the following site:

https://www.cisco.com/go/nam

Comparison of Voice Quality Monitoring Methods

Unified CM call quality (CDRs and CMRs) and NAM complement each other and provide a total solution for voice quality measurement. The following list notes key differences between voice quality monitoring with Unified CM and Cisco NAM:

- The Cisco NAM provides voice quality statistics every 60 seconds. Unified CM provides voice quality statistics after the call is completed (ended).
- Unified CM monitors only the call segment within its own cluster.
- Unified CM voice quality monitoring is best used to gauge the overall voice call quality in the network.

Even if Unified CM call quality metrics are not used, Prime Collaboration uses Unified CM CDR information to correlate with the NAM report for the following information:

- Source and/or destination extension number
- Device types
- Interface through which the call flowed in the case of a call to or from a gateway
- Call disconnect reason, where possible
- Exact Unified CM server (not just the Unified CM cluster) to which the phone is connected

Trunk Utilization

Cisco Prime Collaboration provides real-time Unified CM trunk utilization performance graphs. It is also tightly integrated with Cisco Prime Analytics in order to provide the call information it collects to Analytics for long-term trending and reporting purposes. The call information is provided from the CDR and CMR records Prime Collaboration gathers from Unified CM.

Failover and Redundancy

The Unified CM publisher server is responsible for transferring CDR and CMR files to Prime Collaboration via SFTP. If the publisher server is unavailable, there is no failover mechanism for Prime Collaboration to obtain the new CDR and CMR files that contain MOS values of calls in the Unified CM cluster.

Voice Monitoring Capabilities

Cisco Prime Collaboration supports the following voice quality monitoring capacities:

- Any of the following scenarios:
  - 5,000 sensor-based RTP streams per minute (with NAM modules)
  - 1,600 Unified CM calls per minute
  - 1,500 RTP streams and 666 Unified CM calls per minute

- Prime Collaboration automatically selects and gathers voice quality information (via CDR and CMR files) for all Cisco Unified IP Phones configured in a given Unified CM cluster. There is no configuration option to monitor only certain IP phones in the cluster.

Note When Cisco Prime Collaboration is operating at full capacity, its projected database growth (for Syslog, CDR, and CMR files) is estimated to be about 2.4 GB per day.

Assurance Ports and Protocol

Table 27-4 lists the ports used by the various protocol interfaces for Cisco Prime Collaboration for Assurance. Cisco recommends opening these ports in the corporate internal firewalls (if applicable) to allow communications between Prime Collaboration and other devices in the network

Table 27-4 Cisco Prime Collaboration Port Utilization for Assurance

Protocol	Port	Service
UDP	161	SNMP Polling
UDP	162	SNMP Traps
TCP	80	HTTP
TCP	443	HTTPS
TCP	1741	CiscoWorks HTTP server
UDP	22	SFTP
TCP	43459	Database
UDP	514	Syslog
TCP	8080	Determining status of Unified CM web service
TCP	8443	SSL port between Unified CM and Prime Collaboration

Note The Cisco NAM is accessed remotely over HTTPS with a non-default port. Prime Collaboration will authenticate with each Cisco NAM and maintain the HTTP/S session.

All the management traffic (SNMP) originating from Prime Collaboration or managed devices is marked with a default marking of DSCP 0x00 (PHB 0). The goal of network management systems is to respond to any problem or misbehavior in the network. To ensure proper and reliable monitoring, network management data must be prioritized. Implementing QoS mechanisms ensures low packet delay, low loss, and low jitter. Cisco recommends marking the network management traffic with an IP Precedence of 2, or DSCP 0x16 (PHB CS2), and providing a minimal bandwidth guarantee. The DSCP value must be configured in the Windows Operating System.

If managed devices are behind a firewall, the firewall must be configured to allow management traffic. Prime Collaboration has limited support in a network that uses Network Address Translation (NAT). It must have IP and SNMP connectivity from the Prime Collaboration server to the NAT IP addresses for the devices behind the NAT. Prime Collaboration contains static NAT support.

Bandwidth Requirements

Prime Collaboration polls the managed devices for operational status information at every configured interval, and it has the potential to contain a lot of important management data. Bandwidth must be provisioned for management data, especially if you have many managed devices over a low-speed WAN. The amount of traffic varies for different types of managed devices. For example, more management messages may be seen when monitoring Unified CM as compared to monitoring a Cisco Voice Gateway. Also, the amount of management traffic will vary if the managed devices are in a monitored or partially monitored state and if any synthetic tests are performed.

Analytics

Cisco Prime Collaboration Analytics provides many additional benefits to Prime Assurance. It provides trending to identify degradation over time. It can also utilize trending to provide capacity planning and quality of service (QoS) information. The capacity planning feature allows administrators to plan for growth and also to identify over- or under-utilized resources (for example, TelePresence endpoints) in their network. Analytics can generate automated reports that provide actionable information to CIOs and IT planners. Reports can be customized to meet unique business needs.

Analytics supports the following predefined dashboards:

- Technology Adoption
- Asset Usage
- Traffic Analysis
- Capacity Analysis
- Service Experience

Custom dashboards and dashlets can also be created if desired.

The Technology Adoption dashboard provides visibility into the progress of your voice and video deployment by showing devices deployed and minutes used. This information allows for more intelligent technology investment decisions based on current adoption analysis.

The Asset Usage dashboard shows long-term utilization trends for collaboration network resources. It provides information such as least used and most used resources such as endpoints.

The Traffic Analysis dashboard provides a means to analyze long-term service quality issues and identify voice and video traffic patterns. It offers options to show the top *N* callers, top *N* dialed numbers, top *N* off-net traffic locations, and top *N* call traffic locations.

The Capacity Analysis dashboard provides options that allow tracking of unused or under-utilized voice and video assets such as conferencing devices, call admission control bandwidth, and trunks. The information provided can assist in optimizing equipment and network costs.

The Service Experience dashboard helps identify call quality issues in the collaboration deployment. It can show top *N* endpoints with quality issues or allow filtering based on quality level. It also provides a means to analyze call failures, identify service usage by group of users or endpoints, and help effectively allocate the IT expense.

For detailed information on feature support and functionality, refer to the Cisco Prime Collaboration Analytics product documentation available at https://www.cisco.com.

Note Currently there is no redundancy or failover support with Analytics.

Analytics Server Performance

Analytics is included in the Prime Assurance OVA and runs on the same virtual machine. Note that Analytics does require a separate license.

Provisioning

Prime Collaboration Provisioning is available in the following forms:

- Prime Collaboration Provisioning Standard
- Prime Collaboration Provisioning Advanced

Prime Collaboration Provisioning Standard is a simplified version of Cisco Prime Collaboration Provisioning. It provides simplified provisioning across all collaboration services. You can provision all services including phones, voicemail clients, and video endpoints. Provisioning support is available for a single Unified Communications cluster with limited authorization roles.

Advanced Provisioning provides more advanced features such as delegation to individual domains, template support for configuring infrastructure instances, advanced batch provisioning, and so on. Table 27-5 lists the features available in Prime Collaboration Provisioning Standard and Advanced.

Table 27-5 Prime Collaboration Provisioning Standard and Advanced Features

Features	Standard	Advanced
Delegation of roles or Role-Based Access Control (RBAC)	A single user role is applicable to all domains. You cannot delegate user roles to different domains.	Any user role can be assigned to a specific logical domain based on a region or a group.
Ordering workflow roles	The ordering workflow activities (such as approving an order, assigning MAC addresses, shipping endpoints, or end user receipt of an endpoint) are not available.	The ordering workflow activities can be greatly customized based on the end user requirement. The activity roles can be enabled or disabled, and assigned to different users for an efficient ordering workflow.
Batch provisioning	Allows you to deploy a large number of services by combining them into a single batch. **Note:** Batch Provisioning is available for a single cluster only.	Provides advanced batch options such as importing users and services, and adding or modifying users and services across multiple clusters. You can also batch-import infrastructure settings across multiple clusters.
Infrastructure templates	The Infrastructure Configuration templates cannot be customized.	You can create templates to initially configure or reconfigure Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, and Cisco Unity Express. You can add, edit, or delete the configuration settings, including adding or updating keywords and scheduling template provisioning.
Unified CM cluster support	You can configure a single cluster only.	You can configure multiple clusters.
API	Support for North Bound Interface (NBI) is not available.	Support for North Bound Interface (NBI) is available.

Cisco Prime Collaboration provides a simplified web-based provisioning interface for both new and existing deployments of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Express (Unified CME), Cisco Unity Connection, and Cisco Unity Express. Prime Collaboration provides provisioning for both the infrastructure and subscribers for Day 1 and Day 2 needs. Day 1 needs include configuring new deployments and adding more sites or locations; Day 2 needs include services for ongoing moves, adds, and changes on various components of the Cisco Unified Communications solution.

Cisco Prime Collaboration also exposes northbound APIs to allow Cisco and third parties to integrate with external applications such as HR systems, custom or branded user portals, other provisioning systems, and directory servers.

For details on Prime Collaboration system requirements and installation steps, provisioning users and the infrastructure of supported components, and capacity information, refer to the Cisco Prime Collaboration documentation available at

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

To provide a better understanding of how Prime Collaboration can be used as a network management solution for provisioning various Cisco Unified Communications components, the next section presents some of the basic concepts of Prime Collaboration.

Provisioning Concepts

Cisco Prime Collaboration serves as a provisioning interface for the following components of a Cisco Unified Communications system:

- Call processors
  - Cisco Unified Communications Manager (Unified CM)
  - Cisco Unified Communications Manager Express (Unified CME)
- Message processors
  - Cisco Unity Connection
  - Cisco Unity Express
- Presence processors
  - Cisco IM and Presence
  - Cisco Voice Gateways
  - Cisco VG224, VG204, and VG202 Analog Voice Gateways

Note For more information on component version compatibility, refer to the Prime Collaboration information at https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html.

The following sections describe some of the Prime Collaboration concepts involved in configuring those components.

Domain

Domains are used for administrative purposes to create multiple logical groups within a system. Domains have the following characteristics:

- A domain can be mapped to a geographical location or an organization unit.
- One domain can contain multiple call processors and multiple optional message processors.
- A given call processor or message processor can be a member of multiple domains.
- A domain can partition subscribers so that they can be administered separately.

Service Area

Service areas represent offices. Service areas determine the dial plans and other voice-related configuration settings in the domain. In reality, each office may have multiple service areas. The service area determines attributes such as device group, route partition, and calling search space used within Unified CM. Service areas have the following characteristics:

- Each service area is assigned to a single call processor and one optional message processor.
- Each service area should be associated with one dial plan.

Work Flow and Managing Orders

When deploying a new site or making moves, adds and changes to an existing site, users make all changes to the underlying systems through a two-stage process of creating an order and then processing that order. You can set policies for both of these stages. For example, you can configure the system so that one group of users can only create and submit orders, while another group of users can view and perform processing-related activities. Prime Collaboration contains an automation engine that performs the order processing, including service activation and business flow, based on how Prime Collaboration is configured.

The workflow coordinates activities of the ordering process (approval, phone assignment, shipping, and receiving).

Configuration Templates

Prime Collaboration enables you to configure Unified CM, Unified CME, Cisco Unity Express, and Cisco Unity Connection in a consistent way through the use of configuration templates. You can use these templates to configure any of these products, to perform an incremental rollout on these existing products, and to deploy a new service across existing customers.

Batch Provisioning

Creating users and provisioning their services can also be done automatically through batch provisioning for rolling out a new office or transitioning from legacy systems.

Best Practices

The following best practices and guidelines apply when using Prime Collaboration to provision Cisco Unified Communications components for any new and/or existing deployments:

- Managed devices must be up and running before using Prime Collaboration for further day-one activities such as rolling out a new site and day-two activities such as moves, adds, and changes.
- Pre-configuration is required for Cisco Unified CM, Cisco Unity Connection, Unified CME, Survivable Remote Site Telephony (SRST), Cisco Unity Express, and Cisco IM and Presence Service.

- Define the correct domains, service areas, and provisioning attributes.
- Modify only the workflow rules if necessary.
- Consider the use of Subscriber Types, Advanced Rule settings, and other configuration parameters.

The following basic tasks help support these best practices:

- Add call processors such as Unified CM, and/or Unified CME and message processors such as Cisco Unity, Unity Connection, and/or Unity Express.
- Create domains and assign call processors and message processors to the created domains.
- Provision the voice network by creating and using templates to configure Unified CMs or Unified CMEs, or import current voice infrastructure configurations from an existing deployment.
- Perform bulk synchronization of LDAP users into Prime Collaboration, if applicable.
- Set up the deployment by creating service areas for each domain (typically one per dial plan) and assigning subscriber (user) types to each service area.
- Create administrative users for each domain.
- Order, update, or change subscriber or user services.

Prime Collaboration Design Considerations

The following design considerations apply to Prime Collaboration for provisioning:

- Set up domains in one of the following ways:
  - Create a single domain for multiple sites, with multiple call processors and multiple message processors.
  - Create a domain for each site, consisting of one call processor and zero or more optional message processors.
  - Create multiple domains if different administrators are required to manage a subset of the subscribers.
- Create multiple service areas for multiple dial plans.
- Add only the Unified CM publisher as the call processor for Prime Collaboration. Any changes made to the Unified CM publisher through Prime Collaboration will be synchronized to all the Unified CM subscriber servers.
- Use configuration templates for Unified CM, Unified CME, or Cisco Unity Express.
- Use Cisco IOS commands for Unified CME and Cisco Unity Express configuration templates.
- Add Cisco Unified CM infrastructure data objects for Unified CM configuration templates.
- Change and modify the existing configuration templates for batch provisioning for large quantities of phones and lines (DNs).
- Create multiple domains if you want different domain administrators to manage different sets of subscribers for Day 2 moves, adds, and changes of services (such as phones, lines, and voicemail), even for a single-site deployment.
- Create one service area for one dial plan.
- Create multiple service areas if multiple dial plans are required for the device pools, location, calling search space, and phones.

- Prime Collaboration is an IPv6-aware application with the following characteristics:
  - Prime Collaboration communicates with Unified CM over an IPv4 link. The Prime Collaboration user configuration interface allows users to enter only IPv4 IP addresses because Unified CM has SOAP AXL interfaces in IPv4 only. Therefore, Prime Collaboration must use IPv4 addresses to communicate with the AXL interfaces on Unified CM.
  - Prime Collaboration handles the IPv6 addresses contained in SIP trunk AXL response messages.
  - Support of IPv6-aware functions does not affect support for current Cisco Unified Communications Manager Express, Cisco Unity Express, and Cisco Unity Connection devices.

Redundancy and Failover

If Prime Collaboration fails in the middle of the configuration process, changes made to the configured devices from the Prime Collaboration GUI might not be saved and cannot be restored. Administrators must use manual steps to continue the configuration process by using other tools such as telnet or login (HTTP) to the managed devices until Prime Collaboration comes back live. Manually added configuration changes to the managed device will not automatically show up in the Prime Collaboration dashboard or database unless you also perform synchronization from Prime Collaboration for the call processors (Unified CM and/or Unified CME), message processors (Unity Connection and/or Unity Express), and domains.

Provisioning Ports and Protocol

Table 27-6 lists the ports used by the various protocol interfaces for Prime Collaboration. Cisco recommends opening those ports in the corporate internal firewalls (if applicable) to allow communications between Prime Collaboration and other devices in the network.

Table 27-6 Prime Collaboration Port Utilization for Provisioning

Protocol	Port	Service
TCP	80	HTTP[1] [2]
TCP	8443	HTTPS[2]
TCP	22	SSH[3]
SSH	23	Telnet[3]
TCP	1433	Database[4]

1. To access the Prime Collaboration Administration web page.
2. Prime Collaboration provisions Unified CM via Administrative XML Layer (AXL) Simple Object Access Protocol (SOAP).
3. For Prime Collaboration to communicate with Unified CME and Cisco Unity Express.
4. For Prime Collaboration to connect to the database of Cisco Unity Connection.

Cisco TelePresence Management Suite (TMS)

Cisco TelePresence Management Suite (TMS) supports scheduling of video endpoint and conferencing devices. Scheduling ensures endpoint and port resource availability and provides convenient methods to connect to TelePresence conferences. Most organizations already use calendaring applications to schedule conferences. In this case, calendaring integration enables users to schedule conferences with their existing calendaring client.

Calendaring Options

Calendaring integration gives users the ability to schedule video conferences and invite participants directly from their calendaring application while viewing availability information of resources regardless of where meetings are created. Calendaring options include:

- Cisco TelePresence Management Suite Extension for Microsoft Exchange (TMSXE)

  Allows conference organizers to schedule conferences using their Microsoft Outlook client.

- Cisco TelePresence Management Suite Extension for IBM Lotus Notes (TMSXN)

  Allows conference organizers to schedule conferences using their IBM Lotus Notes client.

- Cisco TelePresence Management Suite Extension Booking API (TMSBA)

  Allows conference organizers to schedule conferences using additional groupware calendaring systems through API integration.

- Cisco TMS Web-based user interface

  Allows users or administrators to schedule conferences through a web-based interface. This is part of the Cisco TMS core application and does not require additional installation or integration.

For more information on Cisco TMS Extensions and APIs, refer to the product documentation available at

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/tsd-products-support-series-home.html

Cisco TMS also allows user and administrators to schedule conferences through a web-based interface. This is part of the Cisco TMS core application and does not require additional installation or integrations.

Cisco highly recommends integrating your corporate calendaring application with the scheduling and management platform chosen by your organization. However, you may also choose to schedule conferences using the TMS web interfaces.

When deploying Cisco TMS calendar integration as your corporate calendaring application, choose the appropriate extension for your environment. For example, if Microsoft Exchange is the existing calendaring application, use TMSXE. TMSXE is installed on a standalone server, and TMSXN is installed on the Lotus Domino server. The integration software is installed separately from Cisco TMS and communicates with your calendaring server using HTTP or HTTPS.

Cisco recommends having your video conferencing resources (Cisco TelePresence Video Communication Server or Cisco MCU) dedicated for either scheduled or permanent/instant conferences. This is because permanent or instant conferences could consume scheduled resources, which would result in undesirable consequences on the scheduled conferences, such as scheduled video participants being unable to join or joining as audio-only due to lack of resources on the server.

Reporting

Cisco TMS provides various types of reporting and analysis functionality, including:

- Asset management reports: ticket logs, device events, device alarms, and connectivity
- Detailed call history reports for managed endpoints and infrastructure
- Scheduling activity reports, including user-based, scheduling interface used, conference event logs, and conference reports

However, some of these functions work only in certain deployments. For example, when an endpoint such as the Cisco TelePresence TX9000 or Cisco TelePresence System EX90 is registered to Cisco Unified Communications Manager (Unified CM), Cisco TMS cannot generate reports for that endpoint. Cisco TMS can generate only call history and call detail record (CDR) reports for an endpoint registered to the Cisco TelePresence Video Communication Server (VCS). For those endpoints that are registered to Unified CM, CDRs can be downloaded from Unified CM.

Organizations that require more customized reports, business knowledge, and integration with Business Intelligence Applications can use the Cisco TelePresence Management Suite Analytics Extension (TMSAE), which is an online analytical processing system for Cisco TMS that provides advanced reporting functionality for your video network. For more information on Cisco TMSAE, refer to the product documentation available at

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/tsd-products-support-series-home.html

Management

The main functions of management in the TelePresence environment include: provisioning, monitoring, maintenance, and resource management. Cisco TelePresence Management Suite (Cisco TMS) enables management of the TelePresence environment, along with a scheduling interface that it supports in a TelePresence environment.

Endpoint and Infrastructure Management

Cisco TMS can manage endpoints registered to both Cisco VCS and Cisco Unified CM. There are two types of device management: direct managed and provisioned.

Direct-managed devices are manually added into the Cisco TMS system navigator. Cisco TMS supports 5,000 direct-managed devices. Cisco TMS communicates with the endpoints directly via HTTP or SNMP protocols. When a direct-managed endpoint is registered to Unified CM, Unified CM handles most management capabilities such as software upgrades. When a direct-managed endpoint is registered to Cisco VCS, Cisco TMS handles management and provisioning of the endpoint, including capabilities such as software upgrades.

Cisco TMS can also directly manage infrastructure devices such as Cisco VCS, Cisco MCU's, and others. Currently Cisco TMS supports scheduling and management of conferencing devices registered with Cisco VCS only.

Provisioned endpoints are not in the TMS system navigator, but rather are provisioned by Cisco TMS through the Cisco TMS Provisioning Extension (TMSPE). Cisco TMS supports 100,000 provisioned devices. The provisioning method dramatically increases the scale that Cisco TMS can support. It also simplifies the procedure for a bulk deployment because there is no need to add the systems manually. However, Cisco TMS has less control on provisioned endpoints compared to direct-managed endpoints. In addition, scheduling is not supported for provisioned endpoints.

Cisco TMS provides the functionality of phone books for direct-managed endpoints registered to Cisco VCS as well as provisioned endpoints. Phone books provide ease of locating users and dialing out.

Cisco TMS also provides interfaces to monitor both scheduled and instant video conferences.

For more information, refer the latest version of the *Cisco TelePresence Management Suite Administrator Guide*, available at

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html

Provisioning

The Cisco TMS Provisioning Extension (TMSPE) is a provisioning application for Cisco TMS and Cisco VCS. Cisco TMSPE enables video conferencing network administrators to create and manage large deployable video conferencing solutions. Cisco TMSPE is an add-on replacement for the TMS agent on the Cisco TMS server, and it provides the following main features:

- Ability to import users from Microsoft and generic LDAP sources (LDAP, LDAPS, AD)
- User personalization and administrative device configuration control for devices supported by Cisco TMS Provisioning Extension (for example, Jabber video, Cisco IP Video Phone E20, and Cisco TelePresence System EX Series and MX Series)
- Multi-tiered phone books for devices supported by Cisco TMSPE
- End-user FindMe portal on Cisco TMS using Microsoft Active Directory (AD) login instead of Cisco VCS Web user interface
- Support for up to 100,0000 users and devices

For further information, refer to the latest version of the *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*, available at

https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-and-configuration-guides-list.html

Phone books

Phone books help users maintain their contacts and dial them. Cisco TMS phone books can be created and populated from different sources such as Microsoft Active Directory (AD), Cisco Unified CM, an H.350 server, and gatekeepers.

There are two types of phone books: local phone books and global phone books. Local phone books (also called *favorites*) are a file stored on an endpoint specific to the end user. Contacts can be added, modified, and deleted as desired by the user.

Global or corporate phone books are pushed from Cisco TMS to the endpoints. They cannot be modified from the endpoint because they are automatically populated from AD, an H.350 server, or the local Cisco TMS database. Administrators can select the phone books for specific users and push them to the appropriate endpoints.

Maintenance and Monitoring

Cisco TMS has a Software Manager repository where the software images of endpoints and infrastructure devices can be added and then used to upgrade matching endpoints and infrastructure devices registered with Cisco VCS. Administrators can select a number of devices and upgrade them from Cisco TMS at one time. Cisco TMS provides the status of the upgrade. Using Cisco TMS to do upgrades is more convenient and easier than upgrading the endpoints and infrastructure devices manually.

Cisco TMS also provides monitoring capabilities for conferences. Cisco TMS lists all scheduled conferences, and the state of the conference (for example, Active) is displayed in TMS's Conference Control Center, with details of packet loss per participant for active conferences. Errors are displayed in TMS's Ticketing Service; for example, if there are configuration errors, Cisco TMS discovers them and opens a ticket associated with the appropriate device. Each ticket has an ID and severity level.

Cisco Smart Software Licensing

Cisco Collaboration System Release (CSR) 12.0 and later releases incorporate Cisco Smart Software Licensing and the Cisco Smart Software Manager (SSM) for management of an organization’s collaboration licenses. Cisco SSM provides a centralized method for applying, tracking, and managing licenses on Cisco Unified CM, Cisco Unity Connection, and Cisco Emergency Responder as well as other Cisco products. Cisco Smart Software Manager assists the administrator by automating many of the steps necessary to license users on the application servers.

Cisco Smart Software Licensing consists of the Cisco hosted Cisco Smart Software Manager web portal, where an organization's collaboration application entitlements and licenses are tracked and synchronized to collaboration components.

Customers purchase licenses, and these licenses are automatically applied to the customer's Cisco Smart Account and synchronized via Cisco SSM with the on-premises applications. Cisco Smart Software Manager registers on-premises collaboration application instances to Cisco Licensing Services and synchronizes the organization’s licenses against the applications.

The following Unified Communications applications use Cisco Smart Software Licensing:

- Cisco Unified Communications Manager (Unified CM) — including Cisco IM and Presence, which is licensed through Unified CM, and Cisco Unified Communications Manager Session Management Edition (Unified CM SME)
- Cisco Unity Connection
- Cisco Emergency Responder

Appropriate licenses must first be acquired and applied to the Cisco Smart Account for managing software and entitlement using the Cisco Smart Software Manager portal. Next, an organization administrator generates a product instance registration token on the Cisco Smart Software Manager portal at https://software.cisco.com. The administrator then registers the collaboration application product instance using the registration token copied from the Cisco Smart Software Manager portal. Once registered, the applications will synchronize with Cisco Smart Software Manager and receive user and feature licensing entitlement information.

An application is allowed 90 days of non-compliance, during which the system will function normally and the administrators can make changes if there are insufficient licenses or if the system has lost communication with Cisco SSM. If the system remains out of compliance (that is, if sufficient licenses are not acquired or communication to Cisco SSM is not restored) for 90 days, the collaboration application functionality is reduced as follows:

- Cisco Unified Communications Manager (Unified CM) — call control

  When the system is out of compliance for 90 days, Unified CM will continue to handle calls but no user or device moves, adds, changes, or deletions (MACD) will be allowed.

- Cisco Unity Connection — voice messaging

  When the system is out of compliance, the system will continue to allow administrative changes but will not provide voice messaging services. That is, the system will no longer answer calls, thus preventing callers from leaving messages and preventing users from retrieving voice messages.

- Cisco Emergency Responder

  When the system is out of compliance, the Cisco Phone Tracking Engine service is stopped and the system stops tracking phones and updating locations.

For more information on Cisco Smart Software Licensing and licensing management with the Cisco Smart Software Manager, refer to the information at

https://www.cisco.com/go/smartlicensing

Deployment Scenarios

Cisco Smart Software Licensing is automatically enabled on the publisher node of all supported applications. Licensing is managed by the Cisco Smart Licensing Manager Service, which is activated and started automatically on the publisher node in each cluster. The publisher node manages the licensing for all other nodes in the cluster.

In order for the collaboration applications to register and synchronize licensing information with the Cisco Smart Software Manager (SSM), the Cisco Smart Licensing Manager Service running on the publisher node of each cluster must communicate over the Internet to Cisco SSM services. This communication is either direct or is mediated by an intermediary.

The collaboration application attempts to communicate directly with the Cisco SSM service over the Internet using HTTPS. In some organizations, outbound HTTPS traffic is allowed, and this traffic is passed to the online Cisco SSM service without issue. In cases where organizations do not allow direct outbound HTTPS traffic from their data center applications to the Internet, Cisco Smart Software Licensing communications may be directed to the Internet by an HTTP proxy. In either case, when the application communicates with the Cisco SSM online services (with or without an HTTP proxy), it does so directly over the Internet.

Alternatively, communications between the collaboration application publisher nodes may be directed to an on-premises Cisco Smart Software Manager satellite system. This is the mediated method of Smart Licensing communications. The Cisco SSM satellite system is a virtual machine (VM) deployed in the on-premises data center. The SSM satellite system acts as an intermediary and relays communications between the on-premises collaboration applications and the Internet-hosted, online Cisco SSM service. The SSM satellite must periodically connect to the online Cisco SSM service to synchronize. This periodic synchronization is facilitated by direct HTTPS communications between the Cisco SSM satellite system and the online Cisco SSM service. This is the Cisco SSM satellite connected mode. As mentioned previously, if the organization has restrictions on outbound HTTPS traffic to the Internet, either an HTTP proxy is used or, alternatively, a report file from the SSM satellite system may be manually uploaded periodically to the online service to maintain registration and authorization.

The main consideration for choosing between direct and mediated deployments of Cisco SSM is the organization's network and security policies related to Internet and online services access. If your organization restricts outbound access to the Internet, consider mediated deployments with Cisco SSM satellite, noting the requirement for a separate Cisco Smart Software Manager satellite VM in the on-premises data center.

Deployment Recommendations

Generally speaking, direct or proxy communication is recommended between the on-premises collaboration application (Unified CM, Unity Connection, and Emergency Responder) cluster publisher nodes and the web-hosted Cisco Smart Software Manager service. This does require outbound HTTPS communications from the application publisher nodes through the organization's firewall to the Cisco Smart Software Manager service. If the organization's policy does not allow for direct outbound web communications, cluster publisher nodes may leverage a new or existing standard HTTP/HTTPS proxy server within the organization to enable firewall traversal and access to the web-hosted Cisco Smart Software Manager service.

When creating product registration tokens and registering collaboration application publisher instances within Cisco SSM, administrators may use different virtual accounts and/or registration tokens under the same Smart Account to group specific product types or products in specific locations for ease of license administration and management.

Creating multiple virtual accounts is recommended because it simplifies license management by allowing licenses to be pooled and shared across multiple products and virtual accounts across the organization. Further, by segmenting product instances and tokens across virtual accounts, organizations can more easily track and account for the costs of licenses along more granular accounting lines in order to better manage operating costs and other expenses.

Note Because licenses may not be pooled, moved, or managed across different Cisco Smart Accounts, Cisco recommends that the organization establish only a single Smart Account (with multiple Virtual Accounts as required) unless there are specific organizational policies or requirements (regulations, laws, or other restrictions) that offset the limitations of multiple Smart Accounts.

Redundancy

The online Cisco SSM service is highly available; however, in the case of an Internet connection issue where the collaboration application system is out of compliance, the system will continue to operate normally for 90 days. User and device provisioning is not possible once the system reaches full non-compliance. In order to maintain normal system operation, the online Cisco SSM must be reachable consistently.

When Cisco Smart Software Licensing is deployed in mediated mode with the Cisco SSM satellite system, install and configure at least two SSM satellite VMs to ensure high availability. Cisco SSM satellite systems rely on an active/standby redundancy scheme, whereby if the active or primary system fails or loses connectivity to collaboration applications or the online Cisco SSM service, the standby or backup system takes over SSM operations.

Capacity Planning for Cisco Smart Software Manager

The online Cisco SSM service provides near infinite scale, given the elastic nature of compute resources within the service data centers. This means that, effectively, an organization can license infinite numbers of collaboration applications using Cisco SSM.

On the other hand, when running in mediated mode, Cisco SSM satellite VMs do have a capacity limit. A single Cisco SSM satellite VM can handle up to 4,000 product instance registrations. When deploying Cisco SSM in mediated mode, be sure to deploy VMs in sufficient quantity to handle all the product instances that require licenses for the deployment.

Additional Tools

In addition to the network management tools mentioned above, the following tools also provide troubleshooting and reporting capabilities for Cisco Unified Communications systems:

- Cisco Unified Analysis Manager, page 27-24
- Cisco Unified Reporting, page 27-25

Cisco Unified Analysis Manager

Cisco Unified Analysis Manager is included with the Cisco Unified Communications Manager Real-Time Monitoring Tool (RTMT). RTMT runs as a client-side application and it uses HTTPS and TCP to monitor system performance, device status, device discovery, and CTI applications for Unified CM. RTMT can connect directly to devices via HTTPS to troubleshoot system problems.

Unlike the other RTMT functions, Unified Analysis Manager is unique in that it supports multiple Unified Communications elements instead of just one. When the Unified Analysis Manager is launched, it collects troubleshooting information from your Unified Communications system and provides an analysis of that information. You can use this information to perform your own troubleshooting operations, or you can send the information to Cisco Technical Assistance Center (TAC) for analysis.

Unified Analysis Manager supports the following Unified Communications elements:

- Cisco Unified Communications Manager
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- Cisco IOS Voice Gateways
- Cisco Unity Connection
- Cisco IM and Presence

Unified Analysis Manager provides the following key features and capabilities:

- Supports collection of Unified Communications application hardware, software, and license information from Unified Communications elements.
- Supports setting and resetting of trace level across Unified Communications elements.
- Supports collection and export to a define FTP server of log and trace files from Unified Communications elements.
- Supports analysis of the call path (call trace capability) across Unified Communications elements.

For more details on the report options, refer to the information about the Cisco Unified Analysis Manager in the latest version of the *Cisco Unified Real-Time Monitoring Tool Administration Guide*, available at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Cisco Unified Reporting

The Cisco Unified Reporting web application generates reports for troubleshooting or inspecting Cisco Unified Communications Manager cluster data. It is a convenient tool that you can access from the Unified Communications Manager console. The tool facilitates gathering data from existing sources, comparing the data, and reporting irregularities. 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. Each report provides data for all active cluster nodes that are accessible at the time the report is generated.

For example, the following reports can be used for general management of a Unified CM cluster:

- Unified CM Cluster Overview — Provides an overview of the cluster, including Unified CM version, hostname, and IP address of all servers, a summary of the hardware details, and so forth.
- Unified CM Device Counts Summary — Provides the number of devices by model and protocol that exist in the Cisco Unified Communications Manager database.

The following report can be used for debugging a Unified CM cluster:

- Unified CM Database Replication Debug — Provides debugging information for database replication.

The following report can be used for maintenance of a Unified CM cluster:

- Unified CM Database Status - Provides a snapshot of the health of the Unified CM database. This report should be generated before an upgrade to ensure the database is healthy.

For more information on the report options, refer to the latest version of the *Cisco Unified Reporting Administration Guide*, available at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

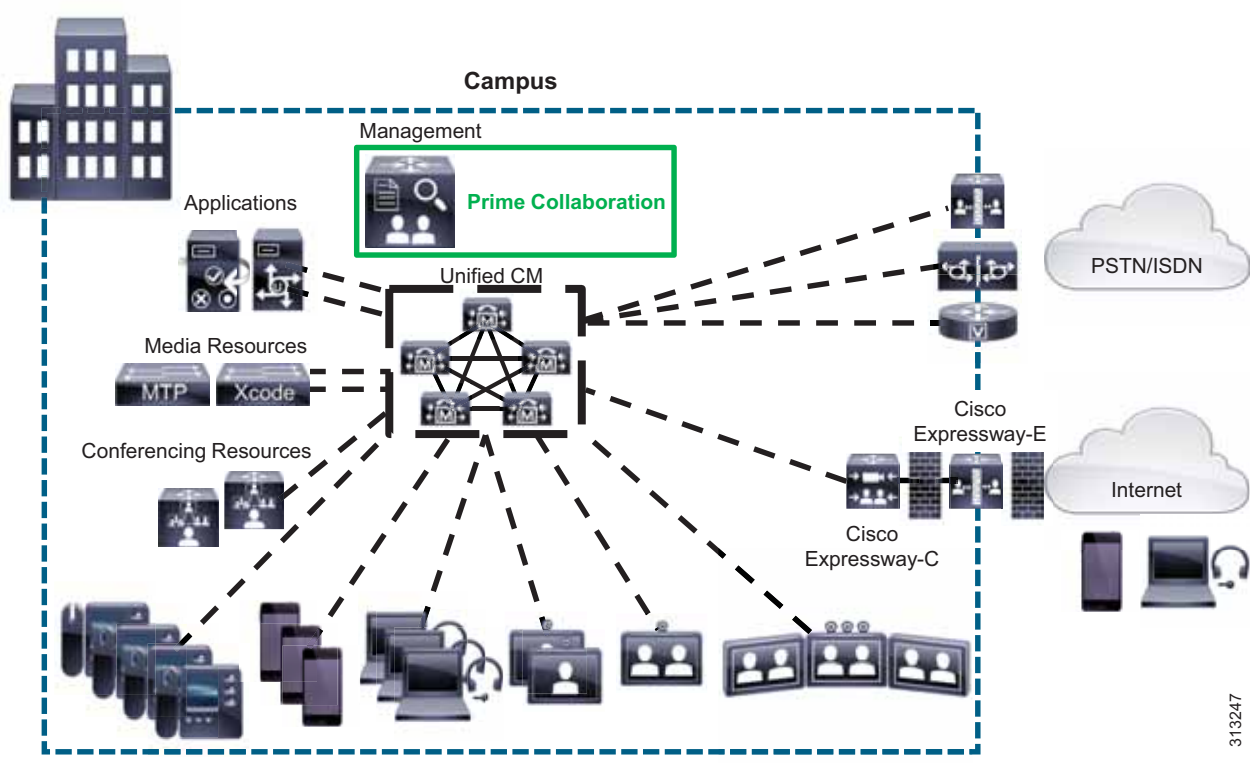
Integration with Cisco Collaboration Deployment Models

This section discusses how to deploy Cisco Collaboration and network management applications in various deployment models. For detailed information on the deployment models, see the chapter on Collaboration Deployment Models, page 10-1.

Campus

In the campus model, Cisco network management applications, along with call processing agents, are deployed at a single site (or campus) with no telephony services provided over an IP WAN. An enterprise would typically deploy the single-site model over a LAN or metropolitan area network (MAN). Figure 27-2 illustrates the deployment of Cisco network management applications in the single-site model.

Figure 27-2 Campus Deployment



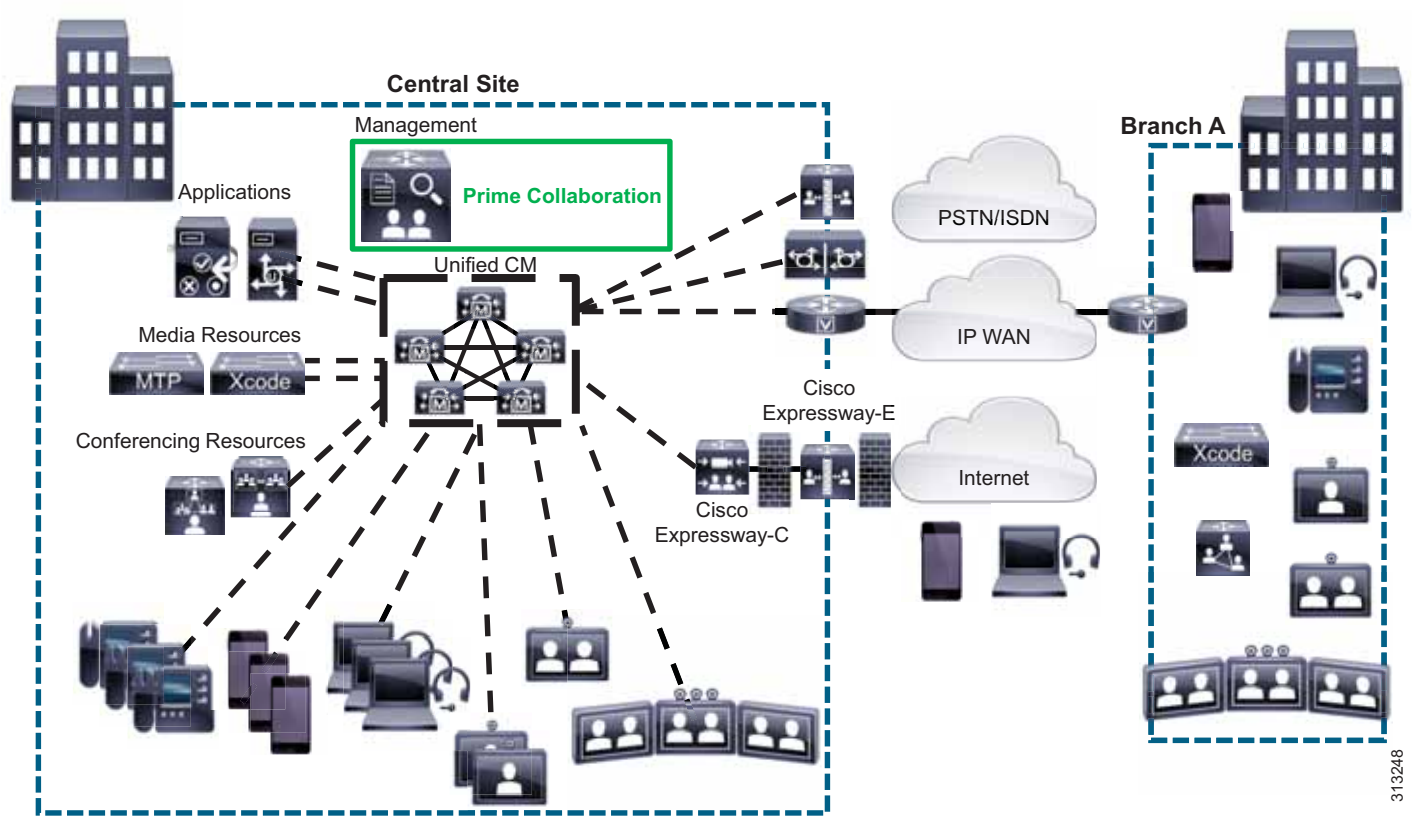
The following design characteristics and recommendations apply to the single-site model for deploying Prime Collaboration:

- Cisco recommends deploying Unified CM voice quality monitoring to monitor overall voice quality in the network.
- Cisco recommends deploying the Cisco NAM to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.

Multisite WAN with Centralized Call Processing

The multisite WAN model with centralized call processing is really an extension of single-site model, with an IP WAN between the central site and remote sites. The IP WAN is used to transport voice traffic between the sites and call control signaling between the central site and the remote sites. Figure 27-3 illustrates the deployment of Cisco network management applications in a multisite WAN model with centralized call processing.

Figure 27-3 Multisite WAN Deployment with Centralized Call Processing



The following design characteristics and recommendations apply to the multisite model for deploying Prime Collaboration with centralized call processing:

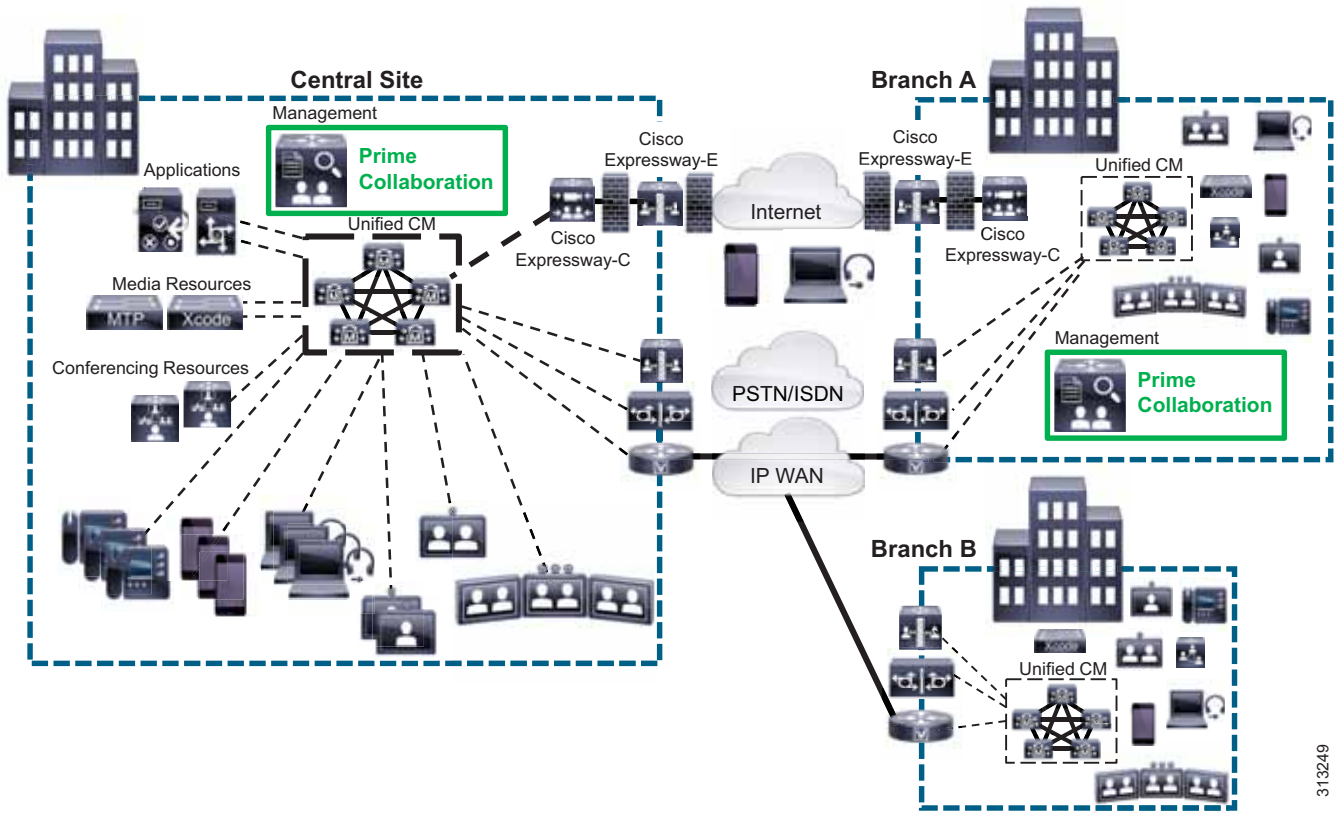
- Cisco recommends deploying all network management applications (including Prime Collaboration) in the central site to locate them with the call processing agent. The benefit of such an implementation is that it keeps the network management traffic between call processing agent and network management applications within the LAN instead of sending that traffic over the WAN circuit.
- Multiple Prime Collaborations can be deployed, with each instance managing multi-site and multi-cluster Unified Communications environments. In this deployment scenario, Cisco recommends that you deploy a Manager of Managers (MoM). Each Prime Collaboration can provide real-time notifications to the higher-level MoM using SNMP traps, syslog notifications, and email to report the status of the network being monitored.
- Cisco recommends deploying Unified CM voice quality monitoring to monitor overall voice quality in the network.

- Cisco recommends using the Service Level Agreement (SLA) feature and Synthetic test feature to check for network infrastructure status.
- Cisco recommends deploying the Cisco NAM to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.

Multisite WAN with Distributed Call Processing

The multisite WAN model with distributed call processing consists of multiple independent sites, each with its own call processing agent connected to an IP WAN. Figure 27-4 illustrates the deployment of Cisco network management applications in a multisite WAN model with distributed call processing.

Figure 27-4 Multisite WAN Deployment with Distributed Call Processing



A multisite WAN deployment with distributed call processing has many of the same requirements as a single site or a multisite WAN deployment with centralized call processing in terms of deploying Prime Collaboration. Follow the best practices and recommendations from these other models in addition to the ones listed here for the distributed call processing model:

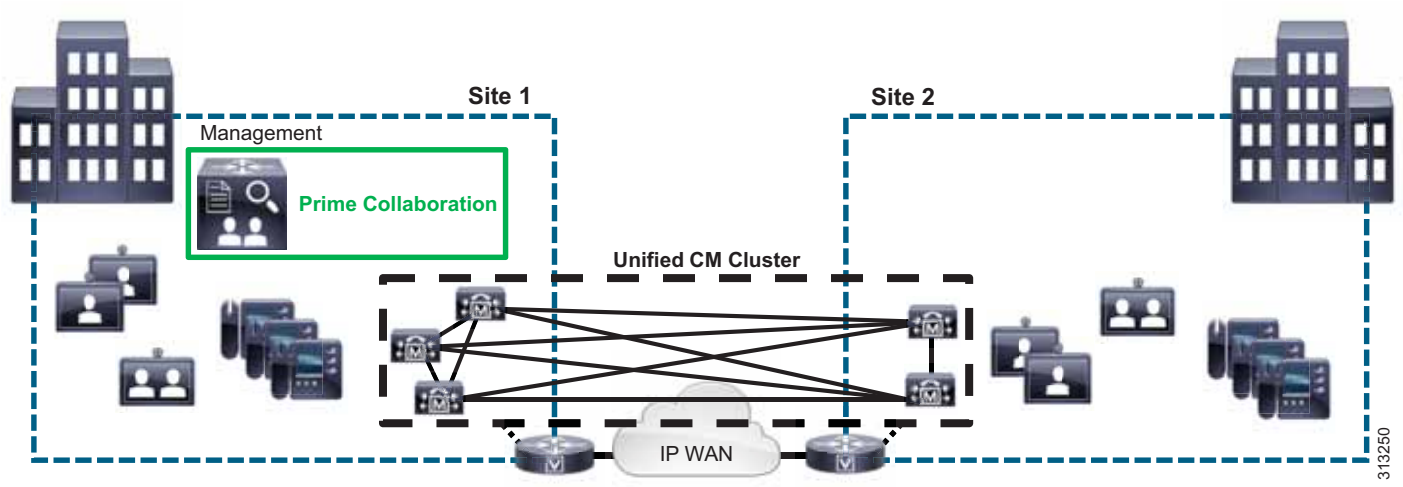
- If only one Cisco Prime Collaboration deployment is used to manage multiple Unified CM clusters, Cisco recommends deploying Prime Collaboration along with the Unified CM cluster that has the highest call volume and the most endpoints.

- Multiple Prime Collaborations can be deployed, with each instance managing multi-site and multi-cluster Unified Communications environments. In this deployment scenario, Cisco recommends that you deploy a Manager of Managers (MoM). Each Prime Collaboration can provide real-time notifications to the higher-level MoM using SNMP traps, syslog notifications, and email to report the status of the network being monitored.
- Cisco recommends deploying Unified CM voice quality monitoring to monitor overall voice quality in the network.
- Cisco recommends deploying the Cisco NAM to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.

Clustering over the WAN

Clustering over the WAN refers to a single Cisco Unified CM cluster deployed across multiple sites that are connected by an IP WAN with QoS features enabled. This deployment model is designed to provide call processing resiliency if the IP WAN link fails. Figure 27-5 illustrates the deployment of Cisco network management applications with clustering over the WAN.

Figure 27-5 Clustering over the WAN



Note There is no native high-availability or redundancy support for Prime Collaboration with this model.

The following design characteristics and recommendations apply when deploying Prime Collaboration with clustering over the WAN:

- Cisco recommends deploying Prime Collaboration in the headquarter site where Unified CM publisher is located.
- Multiple Prime Collaborations can be deployed, with each instance managing multi-site and multi-cluster Unified Communications environments. In this deployment scenario, Cisco recommends that you deploy a Manager of Managers (MoM). Each Prime Collaboration can provide real-time notifications to the higher-level MoM using SNMP traps, syslog notifications, and email to report the status of the network being monitored.

- Cisco recommends deploying Unified CM voice quality monitoring to monitor overall voice quality in the network.
- Cisco recommends deploying the Cisco NAM to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.