



CHAPTER 26

Network Management

Last revised on: January 29, 2008

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 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 voice and data, the need for unified management is apparent. The Cisco Unified Communications Management suite offers a set of integrated tools that help to test, deploy, and monitor the Cisco Unified Communications system. A network manager 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 26-1](#) lists the PDIO phases and the major tasks involved with each phase.

Table 26-1 *Network Management Phases and Tasks*

Plan & Design	Implement	Operate
Assess the network infrastructure for Cisco Unified Communications capability. (For example, predict overall call quality.)	Deploy and provision Cisco Unified Communications. (For example, configure the dial plan, partitioning, user features, and so forth.)	Manage changes for users, services, IP phones, and so forth.
Prepare the network to support Cisco Unified Communications.	Enable features and functionality on the existing infrastructure to support Cisco Unified Communications. (For example, configure voice ports, gateway functionality on routers, and so forth.)	Generate reports for operations, capacity planning, executive summaries, and so forth.
Analyze network management best practices.		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:

- Implement & Operate
 - Cisco Unified Provisioning Manager (Unified PM) manages provisioning of initial deployments and ongoing operational activation for IP communications services.
- Operate
 - Cisco Unified Operations Manager (Unified OM) provides comprehensive monitoring with proactive and reactive diagnostics for the entire Cisco Unified Communications system.
 - Cisco Unified Service Monitor (Unified SM) provides a reliable method of monitoring and evaluating voice quality in Cisco Unified Communications systems.
 - Cisco Unified Service Statistics Manager (Unified SSM) provides advanced statistics analysis and reporting capabilities for Cisco Unified Communications deployments.
 - Cisco Monitor Manager (MM) can be deployed in small or medium business (SMB) locations with 5 to 250 users to actively monitor key device parameters in Cisco Unified Communications systems.
 - Cisco Monitor Director works in conjunction with Cisco Monitor Manager for support of active voice and data network management in SMB sites at managed service-provider locations.
 - Cisco netManager provides managing, monitoring, and diagnostic functionality for Cisco Unified Communication systems in the SMB environment.

For a complete list of the features supported by each product, refer to the related product documentation available at <http://www.cisco.com>.

Network Infrastructure Requirements for Cisco Unified Network Management Applications

A well designed network is the foundation for operating and managing a Cisco Unified Communications network. The Cisco Unified Communications network must conform to the following strict requirements:

- Average IP packet loss $\leq 1\%$
- Average delay variation (jitter) ≤ 30 ms
- Average one-way packet delay ≤ 150 ms

Domain Name Service (DNS) must be enabled 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.

Cisco Discovery Protocol (CDP) must be enabled within the network to ensure proper monitoring. Unified OM'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 network management

applications such as Unified OM, Cisco Monitor Manager, and Cisco Monitor Director to get information on network devices at configured polling intervals and to receive alerts and faults via trap notification sent by the managed devices.

Server platforms with dual Ethernet network interface cards (NICs) can support NIC teaming for Network Fault Tolerance with Unified OM. This feature allows a server to be connected to the Ethernet via 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 increasing the interface speed.

Trivial File Transfer Protocol (TFTP) must be enabled in the network to provide the Cisco 1040 Sensor with a TFTP-based process to download its configuration files.

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

Cisco Unified Operations Manager

Cisco Unified Operations Manager (Unified OM) 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. Unified OM also provides diagnostic capabilities for faster problem isolation and resolution. In addition to monitoring Cisco gateways, routers, and switches, Unified OM 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 Unity and Unity Connection
- Cisco Unity Express
- Cisco Unified Contact Center Enterprise and Unified Contact Center Express
- Cisco Unified Presence
- Cisco Emergency Responder
- Cisco Unified MeetingPlace Express (Unified MPE)
- Cisco Unified IP Phones

For more information on the products and versions supported by Unified OM, refer to the Cisco Unified Operations Manager data sheet available at <http://www.cisco.com>.

Unified OM monitors the network using 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, Unified OM).

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. Unified OM 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. Unified OM needs only SNMP read access to collect network device information.

For more information on SNMP, refer to the documentation available at <http://www.cisco.com>.

Cisco Unified Operations Manager Design Considerations

Unified OM interfaces with other devices in the network in the following ways:

- Simple Network Management protocol (SNMP) to manage all Cisco Unified Communications servers.
- AVVID XML layer (AXL) to manage Unified CM. AXL is implemented as a Simple Object Access Protocol (SOAP) over HTTPS web service.
- 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 IP phones, Cisco IOS routers and switches, and other voice as well as non-voice devices.
- Windows Management Instrumentation (WMI) for Windows-based PCs and servers.

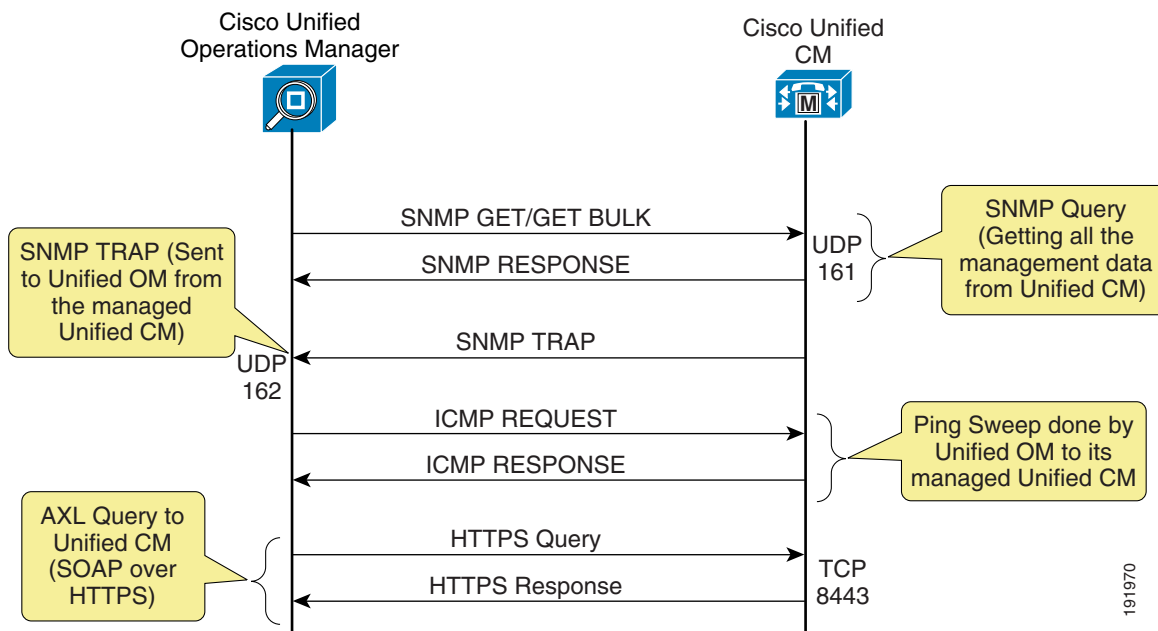
Figure 26-1 shows the system-level overview of Unified OM integrated with Unified CM.



Note

Cisco Unified Operations Manager supports only SNMP polling and traps. Syslog messages are not supported by the Unified OM server.

Figure 26-1 Unified OM and Unified CM System-Level Integration



Failover and Redundancy

Unified OM provides a choice of the following optional failover and redundancy configurations:

- Warm standby — All unified OM servers are active and polling
- Cold standby — Only one Unified OM server is active and polling

In warm standby mode, one backup Unified OM server can be deployed in the network. All the Unified OM servers are actively polling or collecting information from the network devices. Cisco recommends having a default polling interval on one of the active Unified OM servers, which is referred to as the primary Unified OM server. All the other active or secondary Unified OM servers must be configured with a longer polling interval (for example, 15 minutes). This will help reduce the bandwidth needed for management data as well as prevent the managed devices from frequently responding to SNMP queries from multiple Unified OM servers. A higher-level “manager of managers” must be used to manage multiple Unified OM servers. If the primary Unified OM server fails, the polling interval on the secondary Unified OM server can be reduced to resume normal operation and collection of data.

In cold standby mode, two or more Unified OM servers can be deployed in the network. Only one Unified OM server is actively polling or collecting information from the network devices. Cisco recommends having a default polling interval on the active Unified OM server, which is referred to as the primary Unified OM server. All the other secondary Unified OM servers are configured, but polling is disabled on these servers. A higher-level “manager of managers” must be used to manage multiple Unified OM servers. If the primary Unified OM server fails, the polling on the secondary Unified OM server can be enabled to resume normal operation and collection of data.

In both modes, the secondary servers must be backed up periodically with the configuration on the primary servers. This keeps all the servers in synchronization with the configuration and reduces downtime if the primary Unified OM server fails.

Ports and Protocols

Table 26-2 lists the ports used by the various protocol interfaces for Cisco Unified Operations Manager. Cisco recommends opening these ports in the corporate firewall to allow communication between Unified OM and other devices in the network.

Table 26-2 **Unified OM Port Utilization**

Protocol	Port	Service
UDP	161	SNMP polling
UDP	162	SNMP traps
TCP	80	HTTP
TCP	443	HTTPS
TCP	1741	CiscoWorks HTTP server
UDP	514	Syslog
TCP	8080	Determining status of Unified CM web service
TCP	8443	SSL port between Unified CM and Unified OM

All the management traffic (SNMP) originating from Unified OM 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)

If managed devices are behind a firewall, the firewall must be configured to allow management traffic. Unified OM has limited support in a network that uses Network Address Translation (NAT). Unified OM must have IP and SNMP connectivity from the Unified OM server to the NAT IP addresses for the devices behind the NAT. A single Unified OM server cannot manage duplicate IP addresses across NAT domains. If overlapping IP address ranges exist, then a separate Unified OM server must be deployed for each NAT domain.

Bandwidth Requirements

Unified OM polls the managed devices for operational status information at every interval configured, and it has the potential to contain a lot of important management data. Bandwidth must be provisioned for management data, especially if you have a lot of managed devices over a low-speed WAN. The amount of traffic will vary for different types of managed devices. For example, more management messages may be seen when monitoring a Unified OM 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.

Cisco Unified Operation Manager Server Performance

Unified OM is supported in single-server mode. However, multiple Unified OM servers can be deployed to manage large networks. Each Unified OM can be configured to send management information to a higher-level “manager of managers”.

[Table 26-3](#) lists the minimum hardware requirements for Unified OM as well as the maximum number of devices that it can manage per platform.

Table 26-3 *Unified OM Hardware Platforms and Device Capacities*

Maximum Number of Device Supported	CPU	Physical Memory	Hard Disk Capacity	Discovery Time
1,000 phones and 100 Cisco Unified Communications devices ¹	One 2GHz Pentium, Xeon, or Opteron	2 GB	Dual 36 GB	20 to 30 minutes
10,000 phones and 1,000 Cisco Unified Communications devices ¹	One 2GHz Pentium, Xeon, or Opteron	4 GB	Dual 72 GB	120 to 150 minutes
30,000 phones and 2,000 Cisco Unified Communications devices ¹	One 2GHz Pentium, Xeon, or Opteron	4 GB	Dual 72 GB	240 to 270 minutes

1. All Cisco Unified Communications devices (for example, Unified CM, Unified CME, Unity Express, voice gateways, gatekeepers, and so forth) except for IP phones.

Cisco Unified Service Monitor

Cisco Unified Service Monitor (Unified SM) monitors voice quality of calls on the Cisco Unified Communications network. It relies on Unified CM and the Cisco 1040 Sensor to monitor and gather voice quality statistics on real calls rather than simulated calls in the network. Then it compares the collected voice quality statistics against a predefined Mean Opinion Score (MOS) threshold. If the voice quality falls below the threshold, Unified SM sends SNMP trap messages to Unified OM to indicate that a potential issue has been identified. Unified SM is also responsible for sending voice quality information to Cisco Unified Service Statistics Manager (Unified SSM) so that Unified SSM can perform call data analysis and generate reports.

**Note**

A set of global call quality thresholds can be defined in Unified SM, one per supported codec type. Different thresholds can be grouped together based on the Cisco 1040 Sensor being implemented or the Unified CM cluster being monitored.

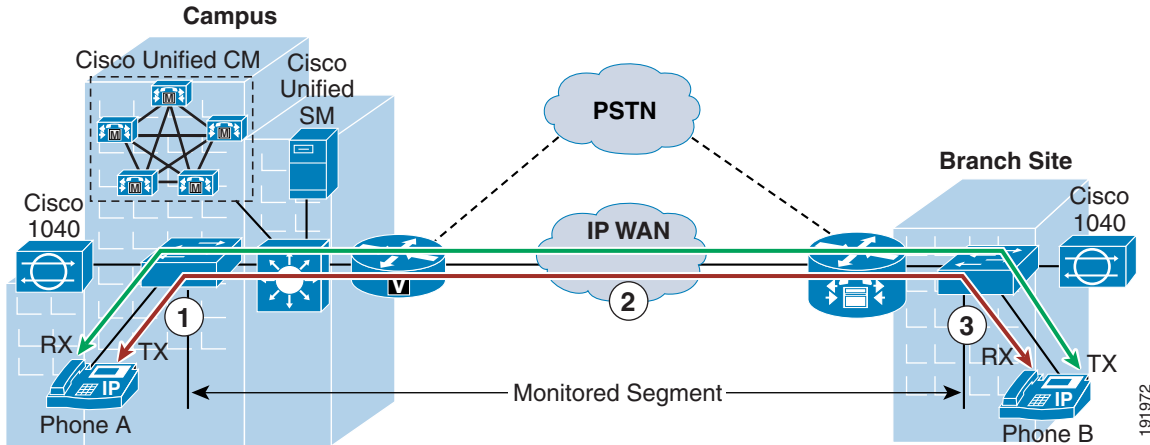
Voice Quality Measurement

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. Unified SM uses the Cisco 1040 Sensor and Unified CM to monitor and report voice quality information.

Cisco 1040 Sensor Voice Quality Monitoring

The Cisco 1040 Sensor is a hardware device that predicts a subjective quality rating that an average listener might experience on the VoIP calls. It operates by measuring various quality impairment metrics that are included in the IP header of RTP streams, such as packet loss, delay, jitter, and concealment ratio. This computed quality rating is converted to a MOS value. The MOS value is included in Syslog messages that are sent to Unified SM every 60 seconds, thus the Cisco 1040 Sensor monitors the voice quality almost on a real-time basis.

The Cisco 1040 Sensor has two Fast Ethernet interfaces, one of which is used to manage the sensor itself and the other is connected to the Switch Port Analyzer (SPAN) port on the Cisco Catalyst switch to monitor the actual RTP streams. In order to monitor voice quality of calls across the WAN, you must deploy a pair of Cisco 1040 Sensors at both sides of the WAN cloud, as illustrated in [Figure 26-2](#).

Figure 26-2 Voice Quality Monitoring with the Cisco 1040 Sensor

There are two call legs, transmitting and receiving, for each phone. Each call leg can be divided into three segments along the call path. For example, for the transmitting call leg of phone A in Figure 26-2, segment 1 runs between phone A and the campus access switch, segment 2 is between the two access switches, and segment 3 is between the access switch at the branch site and phone B. Both segments 1 and 3 are within a local area network, which presents the fewest transmission impairments to voice quality. Therefore, it is reasonably safe to assume that voice quality degradation will not occur in these two segments, and it is unnecessary to monitor those RTP streams.

Segment 2 spans across the WAN circuit and several network devices along the call path. It is more likely to experience degradation of voice quality due to packet loss, delay, and jitter inherent in the WAN. Therefore, the RTP streams (from campus to branch) should be monitored by the Cisco 1040 Sensor at the branch site. By the same token, the sensor in the central site should monitor the incoming RTP streams in that segment across the WAN. These RTP streams provide important voice quality statistics, and their associated MOS values should be analyzed carefully.

Strategic vs. Tactical Monitoring

There are two strategies for deploying Cisco 1040 Sensors: strategic monitoring and tactical monitoring. With strategic monitoring, the Cisco 1040 Sensor is deployed to continuously monitor all or subsets of IP phones in the network. With tactical monitoring, the Cisco 1040 Sensor is deployed in a site where a voice quality issue has been identified. The Cisco 1040 Sensor complies with FCC Class-B standards, and it can be deployed easily in the enterprise environment.

In a small network, Cisco recommends deploying strategic monitoring to monitor all IP phones on a continuous basis. In a medium to large network, Cisco recommends deploying strategic monitoring to continuously monitor a subset of IP phones, while using tactical monitoring to troubleshoot any voice quality issues experienced by the rest of the IP phones.

Design Considerations for the Cisco 1040 Sensor

Consider the following design factors when deploying a Cisco 1040 Sensor:

- A Cisco 1040 Sensor can monitor 100 simultaneous RTP streams. By monitoring the incoming RTP stream only, as illustrated in Figure 26-2, the Cisco 1040 Sensor can provide the full benefit of monitoring 100 (instead of 50) simultaneous voice calls. An environment with a high call volume tends to require the use of more Cisco 1040 Sensors.

- If there are more RTP streams than the Cisco 1040 Sensor can handle, the Cisco 1040 Sensor will perform sampling of those RTP streams, and the resulting MOS value will be diluted. Cisco recommends that you do not operate the Cisco 1040 Sensor in sampling mode because doing so will result in an inaccurate MOS value.
- The Cisco 1040 Sensor utilizes the Cisco Catalyst switch's SPAN port to monitor the actual RTP streams. Different types of Catalyst switches have different quantities of SPAN ports that can be configured. For example, a maximum of two SPAN ports can be configured on the Cisco Catalyst 6500 and 4500 switches, while the maximum limit for Cisco Catalyst 3550 switch is only one. Therefore, the types of Catalyst switches that have been deployed in the network will determine how many Cisco 1040 Sensors can be deployed.
- If there is a trunking connection between multiple Cisco Catalyst switches and if the call volume is low, there is no need to deploy a Cisco 1040 Sensor for every Catalyst switch. Remote Switch Port Analyzer (RSPAN) can be used so that a single Cisco 1040 Sensor can monitor IP phones on other switches within the same VLAN.
- It is inefficient to deploy a Cisco 1040 Sensor at every site that has just a few IP phones and a small call volume. In such cases, Cisco Enhanced Switched Port Analyzer (ESPA) can be used so that one Cisco 1040 Sensor can monitor voice streams across multiple networks.

Unified CM Voice Quality Monitoring

Unified CM utilizes the Cisco Voice Transmission Quality (CVTQ) algorithm to monitor voice quality. CVTQ is based on the Klirrfaktor (K-factor) method to estimate the MOS value of voice calls. At the end of each call, Unified CM stores the MOS value in Call Detail Records (CDRs) and Call Management Records (CMRs), which are transferred to Unified SM via Secure File Transfer Protocol (SFTP) every 60 seconds. In order to integrate with Unified CM, Unified SM 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 Unified SM server
- Username and password for SFTP file transfer
- Protocol: SFTP
- Directory path on the Unified SM server to which CDR and CMR files are transferred

CVTQ is supported natively by Unified CM 6.x and Cisco Unified IP Phones running in both SCCP and SIP modes. The phone models that support CVTQ include Cisco Unified IP Phones 7906G, 7911G, 7931G, 7940G, 7941G, 7941G-GE, 7942G, 7945G, 7960G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G-GE, and 7975G.

As a comparison to the Cisco 1040 Sensor, which performs a full-depth inspection on various quality impairment metrics, the K-factor method inspects only one dimension of quality impairments, packet loss, which is really a network effect. Thus, CVTQ is a less sophisticated algorithm than the one that the Cisco 1040 Sensor uses to monitor the quality of calls. Cisco recommends using CVTQ to flag a voice quality issue and using the Cisco 1040 Sensor to validate and troubleshoot the issue.

Failover and Redundancy

A primary and secondary Unified SM can be configured to provide redundancy and failover support to the Cisco 1040 Sensor. After missing three consecutive SCCP keepalive messages from the primary Unified SM, the Cisco 1040 Sensor will try to register with the secondary Unified SM. The Cisco 1040 Sensor will also send Syslog messages to the secondary Unified SM after the registration failover process succeeds.

You can configure up to three Unified SMs, or Billing Application Servers, in Unified CM. Failure of one Unified SM will not prevent the remaining two servers from obtaining CDR and CMR files from Unified CM.



Note

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

Unified SM Server Performance

Unified SM operates only in single-server mode. However, multiple Unified SMs (all connected to Cisco Unified Operations Manager) can be deployed to manage large networks. [Table 26-4](#) lists the minimum hardware requirements for Unified SM as well as the maximum number of devices that it can manage per platform.

Table 26-4 Unified SM Hardware Platforms and Device Capacities

Maximum Number of Device Supported	CPU	Physical Memory	Hard Disk Capacity
1,000 phones and 100 Cisco Unified Communications devices ¹	Single or dual Pentium, Xeon, or Opteron greater than 2 GHz	2 GB	Dual 36 GB
10,000 phones and 1,000 Cisco Unified Communications devices ¹	Dual Pentium, Xeon, or Opteron greater than 2 GHz	4 GB	Dual 72 GB
30,000 phones and 2,000 Cisco Unified Communications devices ¹	Dual Pentium, Xeon, Opteron greater than 2 GHz	4 G	Dual 72 GB

1. All Cisco Unified Communications devices (for example, Unified CM, Unified CME, Unity Express, voice gateways, gatekeepers, and so forth) except for IP phones.

Unified SM supports the following voice quality monitoring capacities:

- Unified SM supports up to 50 Cisco 1040 Sensors.
- Unified SM supports, concurrently, up to 90,000 RTP streams per hour being monitored by Cisco 1040 Sensor and up to 15,000 CVTQ-based calls per hour being monitored by Unified CM.
- Unified SM automatically selects and monitors all Cisco Unified IP Phones configured in a given Unified CM cluster, and there is no configuration option to monitor only certain IP phones in the cluster.

**Note**

When Unified SM 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.

Ports and Protocol

Table 26-5 lists the ports used by the various protocol interfaces for Cisco Unified Service Monitor. Cisco recommends opening these ports in the corporate firewall to allow communication between Unified SM and other devices in the network.

Table 26-5 Unified SM Port Utilization

Protocol	Port	Service
TCP	80	HTTP
TCP	443	HTTPS
TCP	1741	CiscoWorks HTTP server
UDP	22	SFTP
UDP	162	SNMP traps
TCP	43459	Database
UDP	5666	Syslog ¹
TCP	2000	SCCP ²
UDP	69	TFTP ³

1. Unified SM receives Syslog messages from the Cisco 1040 Sensor.
2. Unified SM communicates with the Cisco 1040 Sensor via SCCP.
3. The Cisco 1040 Sensor downloads its configuration file via TFTP.

Comparison of Voice Quality Monitoring Methods

The following list notes key differences between voice quality monitoring with the Cisco 1040 Sensor and with CVTQ:

- The Cisco 1040 Sensor monitors voice calls based on packet loss, delay, jitter, and concealment ratio. CVTQ monitors voice calls based on packet loss only.
- The Cisco 1040 Sensor provides voice quality statistics every 60 seconds. CVTQ provides voice quality statistics after the call is completed.
- The Cisco 1040 Sensor is compatible with all Cisco Unified CM releases and all types of endpoints connecting to the Cisco Catalyst switch. CVTQ supports only Unified CM 4.2 and later releases.
- For inter-cluster calls, the Cisco 1040 Sensor monitors the end-to-end call segment. CVTQ monitors only the call segment within its own cluster.
- Cisco recommends using the Cisco 1040 Sensor to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues. CVTQ-based voice quality monitoring should be used to gauge the overall voice call quality in the network.

Cisco Unified Service Statistics Manager

The Cisco Unified Service Statistics Manager (Unified SSM) performs advanced call statistics analysis and generates reports for executives, operations, and capacity planning functions. Unified SSM is fully dependent on Unified OM and Unified SM to obtain call statistics information; therefore, Unified OM and Unified SM must be implemented and operating before you deploy Unified SSM. Unified SSM provides both out-of-the-box reports as well as customizable reports that provide visibility into key metrics such as call volume, service availability, call quality, resource utilization, and capacity across the Cisco Unified Communications system. For the detailed information on feature support and functionality, refer to the Cisco Unified Service Statistics Manager product documents available at <http://www.cisco.com>.

Integration with Unified OM and Unified SM

Unified SSM can integrate with only one Unified OM but multiple Unified SMs. Unified SSM extracts call statistics data from Unified OM and Unified SM databases. The data extraction process is performed by the Unified SSM agent.

The Unified SSM agent facilitates communication between Unified SSM and Unified OM or Unified SM, and it is responsible for transmitting call statistics data from Unified OM or Unified SM to Unified SSM. Unified SSM then stores the extracted data in its own SQL database.

If Unified OM and Unified SM are deployed on the same Cisco Media Convergence Server (MCS) as Unified SSM, there is no need to install the Unified SSM agent on Unified OM or Unified SM. With such a co-resident deployment, Unified SSM is able to extract call statistic data directly from the Unified OM and Unified SM databases instead of transferring the data across the network.

If Unified OM and Unified SM are deployed separately from Unified SSM, then the Unified SSM agent must be installed on every instance of Unified OM and Unified SM. The executable installation file of the Unified SSM agent can be downloaded from the Unified SSM Web Administration page and installed locally on Unified OM and Unified SM. With Unified SSM agents distributed on Unified OM and Unified SM, Unified SSM is able to control and manage the data extraction process. Unified SSM connects all distributed Unified SSM agents via TCP on port 12124, and Unified SSM agents send call statistics data back to Unified SSM via TCP on port 12126.

There are two different data collection approaches within Unified SSM. The first approach is called *raw data collection*. With this approach, Unified SSM instructs the Unified SSM agent to retrieve all call statistics data directly from the Unified OM and Unified SM databases. All retrieved data is then saved in Unified SSM's database for up to 30 days. The advantage of this approach is that it provides Unified SSM with a comprehensive data source to perform detailed analysis and report generation.

The second approach is called *monitor-based data collection*. With this approach, Unified SSM instructs the Unified SSM agent to transfer the processed call statistics data only. The advantage of this approach is fewer traffic loads over the network, and the processed data can be stored in the Unified SSM database for up to three months. In order to process the original call statistics data in the Unified OM and Unified SM databases, a specific monitor instance must be created in the Unified SSM Administration console and that monitor instance must be associated with the appropriate Unified SSM agent. The monitor instance extracts only the data based on predefined attributes. For example, for Call Volume Monitor, the attributes include number of completed calls on-net, number of failed calls on-net, average duration per call on-net, and so forth. Each monitor instance has a unique list of predefined attributes. The monitor instance then polls and extracts the data every 15 minutes, and the Unified SSM agent aggregates the processed data from its associated monitor instance(s) and send it to Unified SSM every 30 minutes.

For a comprehensive list on all attributes of each monitor type and its configuration guidelines, refer to the Cisco Unified Service Statistics Manager product documents available at <http://www.cisco.com>.

**Note**

Currently there is no redundancy or failover support with Unified SSM.

Unified SSM Server Performance

Unified SSM operates only in a single-server mode. Table 26-6 lists the minimum hardware requirements for Unified SSM as well as the maximum number of devices that it can manage per platform.

Table 26-6 Unified SSM Hardware Platforms and Device Capacities

Maximum Number of Device Supported	CPU	Physical Memory	Hard Disk Capacity
1,000 phones and 100 Cisco Unified Communications devices ¹	Single or dual Pentium, Xeon, or Opteron greater than 2.0 GHz	3 GB	Dual 60 GB
10,000 phones and 1,000 Cisco Unified Communications devices ¹	Single or dual Pentium, Xeon, or Opteron greater than 3.0 GHz	4 GB	Dual 72 GB
30,000 phones and 2,000 Cisco Unified Communications devices ¹	Dual Pentium, Xeon, or Opteron greater than 3.0 GHz	4 GB	Dual 72 GB

1. All Cisco Unified Communications devices (for example, Unified CM, Unified CME, Unity Express, voice gateways, gatekeepers, and so forth) except for IP phones.

Ports and Protocol

Table 25-y lists the ports used by the various protocol interfaces for Cisco Unified Service Statistics Manager. Cisco recommends opening these ports in the corporate firewall to allow communication between Unified SSM and other devices in the network.

Table 26-7 Unified SSM Port Utilization

Protocol	Port	Service
TCP	80	HTTP
TCP	443	HTTPS
TCP	2662	Database
TCP	12130	Syslog
TCP	12124	Unified SSM and Unified SSM agent communication ¹
TCP	12125	Unified SSM and Unified SSM agent communication ²

1. Unified SSM connects all distributed Unified SSM agents.
2. Unified SSM agents send call statistics data back to Unified SSM.

Cisco Unified Provisioning Manager

The Cisco Unified Provisioning Manager (Unified PM) is a web-based provisioning application based on the Java 2 Enterprise Edition (J2EE) architecture. Unified PM 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, Cisco Unity Connection, and Cisco Unity Express. Unified PM provides provisioning for both the infrastructure and subscribers (or phone users) 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.

Unified PM can be installed in simple or advanced mode to support up to 30,000 phones and 60,000 lines. In simple mode, Unified PM is installed on one system as a single server. Advanced mode allows a two-system installation, where the Unified PM database server is installed on one server and the web and application server are on a separate system to support from 10,000 to 30,000 phones.

For more details on system requirements and installation steps, provisioning users and the infrastructure of supported components, and capacity information, refer to the Cisco Unified Provisioning Manager documentation available at <http://www.cisco.com>.

**Note**

Unified PM 1.1 supports Cisco Unified CM 6.0, Cisco Unified CME 4.1, Cisco Unity 5.0, Cisco Unity Connection 2.0 and Cisco Unity Express 3.0. For more information on component version compatibility, refer to the Unified PM data sheets at <http://www.cisco.com/go/cupm>.

To provide a better understand of how Unified PM can be used as a network management solution for provisioning various Cisco Unified Communications components, this section first presents some of the basic concepts of Unified PM.

Call Processors and Message Processors

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

- Call processors
 - Cisco Unified Communication Manager (Unified CM)
 - Cisco Unified Communications Manager Express (Unified CME)
- Message processors
 - Cisco Unity
 - Cisco Unity Connection
 - Cisco Unity Express

The following sections describe some of the Unified PM 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.

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

Users and Subscribers

A *user* is a person who is authorized to perform various tasks in Unified PM, based on assigned user roles. When installed, Unified PM creates a Unified PM Admin (also called a Super Admin in Unified PM) who has global administrative rights and complete authorization to perform all tasks in Unified PM.

User roles determine the level of access within Unified PM. Domain-specific users can be assigned more than one user role to have rights to specific tasks in a domain. Individual user roles are related to either policy or workflow tasks. A user can be an administrator or a phone user.

A *subscriber* in Unified PM is an entity that uses IP telephony services provided by the underlying voice applications. A subscriber is the same as a phone user in Unified CM. Users in Unified PM can also have services themselves; thus, a user (an administrator) can also be a subscriber (or a phone user).

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. Unified PM contains an automation engine that performs the order processing, including service activation and business flow, based on how Unified PM is configured.

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

Configuration Templates

Unified PM enables you to configure Unified CM, Unified CME, and Cisco Unity Express in a consistent way through the use of configuration templates. You can use these templates to configure a new deployment of Unified CM, Unified CME, or Cisco Unity Express; to perform an incremental rollout on an existing Unified CM, Unified CME, or Cisco Unity Express; 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 Unified PM to provision Cisco Unified Communications components for any new and/or existing deployments:

- 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.
- 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.

**Note**

Unified PM does not provide distributed installation of the application server and database server, nor does it support any of the clustering features of the application server.

Unified PM Design Considerations

The following design considerations apply to Unified PM:

- Deploy a one-system simple-mode installation of Unified PM for up to 10,000 phones.
- Deploy a two-system or dual-processor Microsoft Windows system in advanced mode, with the Unified PM database installed on a separate system from the web and application server.
- If a two-system advanced-mode installation is used for 10,000 to 30,000 phones, both the database server and the web and application server must be co-located, regardless of the deployment model used.
- One Unified PM can support up to 30,000 phones or 60,000 lines (DNs).
- 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.
- Create two service areas if more than 15,000 phones and two Cisco Unity servers are deployed.
- Add only the Unified CM publisher as the call processor for Unified CM. Any changes made to the publisher 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.

Launching Cisco Unified Operations Manager

Unified PM can launch Cisco Unified Operations Manager (Unified OM) to obtain subscriber or user phone information. Unified PM allows its users to launch Unified OM by means of the Details button on the subscriber record. The Details button launches the IP Phone Details dialog box from Unified OM. To provide the launch point, the hostname or IP address and port number of the Unified OM server must be stored in the configuration file `<Install Dir>\sep\ipt.properties` file. The following two entries can be edited by the system administrator to store the IP address or hostname and port number information of the Unified OM to be launched (both entries are left empty after Unified PM is installed):

```
dfc.ipt.operationsmanager.host:  
dfc.ipt.operationsmanager.port:
```

Unified PM must be stopped and restarted for the changes to take effect. When launched, Unified OM displays its screen in a separate browser window.

Unified PM provides the URL for Cisco Unified Operations Manager (unified OM) to launch the Subscriber Record screen from its Phone Information screen. Refer to the CUOM section in this chapter for more details.

Redundancy and Failover

Once Unified PM is installed and set up, it can be used for Day 1 and Day 2 provisioning activities unless an upgrade or patch update is required. Unified PM currently does not have true redundancy and failover support. When multiple Unified PM systems are deployed, there is no synchronization between their multiple databases.

If Unified PM fails in the middle of the configuration process, changes made to the configured devices from the Unified PM 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 Unified PM comes back live. Manually added configuration changes to the managed device will not automatically show up in the Unified PM dashboard or database unless one of the following steps is performed:

- Synchronization from the Unified PM GUI for the call processors (Unified CM and/or Unified CME), message processors (Cisco Unity, Unity Connection, and/or Unity Express), and domains
- Synchronization by using a script under the Microsoft Windows scheduler that comes with the Unified PM installation, to run synchronization periodically (for example, every night)

Unified PM uses the Unified CM publisher server for all the database changes that are replicated to the Unified CM subscriber servers. If the Unified CM publisher fails, access to any of the information on the Unified CM server or cluster (including phones) becomes unavailable if the publisher is the only call

processor associated with the domain or service area. Therefore, only certain features are available for provisioning even if other Unified CM servers or subscribers are in the domain or service area. Cisco does not recommend adding more Unified CM subscribers as call processors due to the fact that Unified CM configuration changes cannot be made if the Unified CM publisher server fails and that association of any additional Unified CM subscriber servers will introduce a lot of overhead.

Cisco Unified Provisioning Manager Server Performance

Table 26-8 lists system requirements and capacity information for Unified PM. For the most current capacity information, refer to the latest Cisco Unified Provisioning Manager documentation available at <http://www.cisco.com>.

Table 26-8 Unified PM Capacity and System Requirements

Maximum Device Support	CPU	Physical Memory	Hard Disk Capacity
500 to 1000 phones, or 1000 to 2000 lines (DNs)	One 3.0 GHz Intel P4 processor	2 GB	1 x 30 GB
1000 to 10,000 phones or 2000 to 20,000 lines (DNs)	One 3.0 GHz Intel P4 processor	4 GB	1 x 60 GB
10,000 to 30,000 phones or 20,000 to 60,000 lines (DNs)	Two-server installation: 1 Database server 1 Web and application server Or dual 3.0 GHz Intel P4 processor	4 GB	Dual 60 GB

Unified PM requires a 100 Mbps network interface card (NIC). Unified PM supports an unlimited number of call processors (Unified CM and Unified CME) and message processors (Cisco Unity, Unity Express, and Unity Connection) with up to 30,000 phones or 60,000 lines. Synchronization time depends upon the number of deployed phones and lines (DNs).

Ports and Protocol

Table 26-9 lists the ports used by the various protocol interfaces for Unified PM. Cisco recommends opening those ports in the corporate firewall to allow communication between Unified PM and other devices in the network.

Table 26-9 Unified PM Port Utilization

Protocol	Port	Service
TCP	80	HTTP ^{1 2}
TCP	8443	HTTPS ²
UDP	22	SSH ³
TCP	23	Telnet ³
TCP	1433	Database ⁴

1. To access the Unified PM Administration web page.

2. Unified PM provisions Unified CM via AVVID XML Layer (AXL) Simple Object Access Protocol (SOAP).
3. For Unified PM to communicate with Unified CME and Cisco Unity Express.
4. For Unified PM to connect to the database of Cisco Unity and Cisco Unity Connection.

Cisco Monitor Manager and Cisco Monitor Director

In a Cisco Unified Communications distributed deployment where components such as Cisco Unified Communications Manager Express (Unified CME), Cisco Unity Express, and Cisco Unified IP Phones are located at the remote branch offices or small to medium-sized businesses (SMBs) for call processing and message processing, monitoring and managing the health of the networking devices for remote branch offices and SMBs becomes essential. This section describes the tools for monitoring and reporting of the network infrastructure and Cisco Integrated Services Router (ISR) based IP telephony monitoring on Unified CME, Cisco Unity Express, and IP phones using Cisco Monitor Manager and Cisco Monitor Director.

Cisco Monitor Manager and Cisco Monitor Director provide complete network monitoring and reporting solutions for network infrastructure and Cisco ISR based IP telephony monitoring in the SMB environment for up to 250 users. With these tools, the following devices can be implemented, monitored, and reported in the SMB environment.

- Cisco Unified Communications Manager Express (Unified CME)
- Cisco Unity Express
- Cisco Unified IP Phones with support of Cisco Unified Communication 500 Series and Cisco Catalyst Express 500 Series switches
- Cisco 521 Wireless Express Access Point
- Cisco 500 Series Wireless Express Mobility Controller
- Security appliances: Cisco ASA 5505 and 5510; Cisco PIX 501, 506, 506E, 515, and 515E

For more information on supported devices and features, refer to the documentation available at <http://www.cisco.com/go/sbcs>.

Cisco Monitor Director receives the following reports from Cisco Monitor Manager:

- Network Summary Report
- Performance Summary Report
- Monthly Report, which includes the top five devices with the most intensive CPU and memory usage, aggregated bandwidth, and PSTN trunk utilization, based on real-time and historical monitoring

Cisco Monitor Manager and Cisco Monitor Director use licensing provided by Macrovision FLEXlm to provide base licenses (that is, limited or standard licenses) to ensure that the product runs as self-managed, and add-on licenses (that is, Managed Service Provider (MSP) license) to allow Cisco Monitor Director to receive the reports from Cisco Monitor Manager. Cisco Monitor Manager with an MSP license sends reports and alerts to Cisco Monitor Director via HTTPS or SSL, and Cisco Monitor Director checks if Cisco Monitor Manager has the MSP license. If not, Cisco Monitor Director will not accept any requests from Cisco Monitor Manager. (For more information on licensing, refer to the Cisco Monitor Manager and Cisco Monitor Director product documentation available at <http://www.cisco.com>.)

Table 26-10 lists the supported releases of Unified CME, Cisco Unity Express, and Cisco IOS. (For the latest information on supported releases, refer to the Cisco Monitor Manager and Cisco Monitor Director product documentation available at <http://www.cisco.com>.)

Table 26-10 Supported Cisco Unified CME, Cisco Unity Express, and Cisco IOS Releases

Cisco Unity Express Supported Releases	Compatible Cisco Unified Communications Manager Express (Unified CME) Releases	Minimum Cisco IOS Release Required for Unified CME Release
2.3	3.4 4.0, 4.1	12.3(14)T 12.4T, 12.4(4)XC
2.2.2	3.3 4.0, 4.1	12.3(14)T 12.4(4)XC
3.0	4.0, 4.1	12.3(14)T, 12.4T, 12.4(4)XC

Cisco Monitor Manager and Cisco Monitor Director Design Considerations

Cisco Monitor Manager and Cisco Monitor Director are Microsoft Windows-based applications. They do not require that any of the agent software or hardware be deployed on the managed devices.

Interaction Overview

Cisco Monitor Manager requires Level 15 user credentials to retrieve information from the device, so managed devices should be configured with at least one user with privilege Level 15 to allow access.

Cisco Monitor Manager uses Cisco Discovery Protocol (CDP) to auto-discover the entire data network and the Cisco Unified Communications voice network. Cisco Monitor Manager uses HTTPS when retrieving configuration and performance information from managed Cisco ISR routers, switches, voice gateways, Unified CME, Cisco Unity Express, access points, and security devices at SMB sites where possible, and it can fallback to HTTP if HTTPS is not supported by a managed Cisco device.

Cisco Monitor Manager uses SNMP for voice monitoring and data collection. Users must enable and configure SNMP on managed devices; otherwise, Cisco Monitor Manager shows only the device capabilities and will not collect any voice data. Cisco Monitor Manager uses its Reseller Controller module to communicate with Cisco Monitor Director to send collected data, alerts, and reports over HTTPS. SNMP credentials are encrypted via Advanced Encryption Standard (AES). The SNMP Management Information Bases (MIBs) used for Unified CME, Cisco Unity Express, and IP phones are CISCO-CCME-MIB and CISCO-UNITY-EXPRESS-MIB, respectively.

Cisco Monitor Manager and Cisco Monitor Director Deployment Models

Cisco Monitor Manager can be deployed as a standalone server in self-managed SMB sites or used in conjunction with Cisco Monitor Director at value-added resellers (VARs) managed service provider (MSP) location.

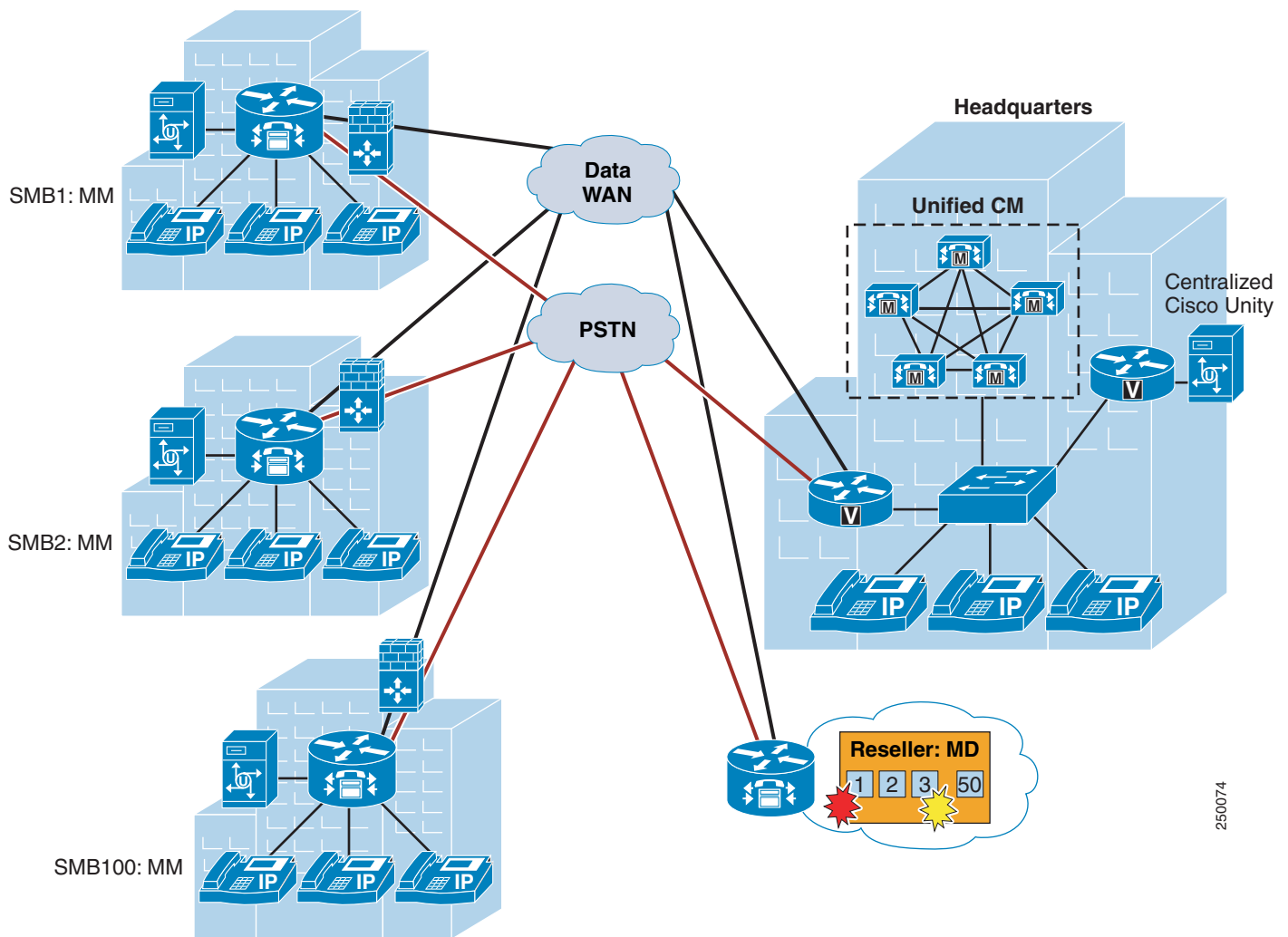
When deployed in self-managed SMB sites, Cisco Monitor Manager monitors the networks 24 hours a day 7 days a week and provides comprehensive real-time monitoring, alerting, and reporting capabilities for the SMB class of Cisco Unified Communications and data systems by periodically polling and collecting inventory and performance-monitoring data. Cisco Monitor Director is a centralized proactive network management application to allow managed service providers (MSPs) to have full visibility into

their SMB customers' networks and provide comprehensive automated monthly reporting by proactively and centrally monitoring the operational health of the data and IP telephony network of SMB customers. Cisco Monitor Director supports up to 50 SMBs 24 hours a day, 7 days a week.

When deployed in Cisco VAR-managed environment, Cisco Monitor Manager provides distributed intelligence, comprehensive alerts, and reports to the Cisco Monitor Director application, which resides at the Cisco VAR managed service provider (MSP) location. Cisco Monitor Manager communicates with Cisco Monitor Director via a highly secure and reliable Secure Socket Layer (SSL). A dedicated VPN setup between Cisco Monitor Manager and Cisco Monitor Director is not required.

Figure 26-3 illustrates a typical deployment of Cisco Monitor Manager (MM) at SMBs and Cisco Monitor Director (MD) at a VAR MSP location.

Figure 26-3 Example Deployment of Cisco Monitor Manager and Cisco Monitor Director



250074

Server Co-Residency and Integration with Other Device Managers

Cisco Monitor Manager or Cisco Monitor Director can reside on the same server with Cisco Configuration Assistant 1.0, a network configuration application for SMBs, to provide a one-box solution of monitoring and configuration management tools for a complete system of voice, data, video, and wireless networking products, as part of a Smart Business Communications System (SBCS) portfolio. Cisco Monitor Manager can import devices from a Cisco Configuration Assistant community. Cisco Monitor Manager needs 1 GB of RAM to co-reside with Cisco Configuration Assistant, while Cisco Monitor Director requires 2 GB of RAM to co-reside with Cisco Configuration Assistant. (For more information on system requirements, refer to the Cisco Monitor Manager and Cisco Monitor Director product documentation available at <http://www.cisco.com>.)

Cisco Monitor Manager can serve as the launch point of various Cisco device managers such as Cisco Router and Security Device Manager, Cisco Adaptive Security Device Manager, Cisco PIX Device Manager, Smartports, and others.

Redundancy and Failover

Cisco Monitor Managers is deployed in SMB sites to remotely discover, monitor, alert, and report on supported IP telephony and data network devices for up to 250 IP phones or users. Cisco Monitor Manager and Cisco Monitor Director do not support any database synchronization or load balancing between multiple Cisco Monitor Managers and Cisco Monitor Directors. Cisco Monitor Manager and Cisco Monitor Director are required to run 24 hours a day 7 days a week without any memory leaks or performance degradation over time. No hot standby capabilities or features are supported across multiple Cisco Monitor Managers and Cisco Monitor Directors, but failure of Cisco Monitor Manager or Cisco Monitor Director will not impact any network operations.

Cisco Monitor Manager and Cisco Monitor Director do not provide automated backup or restore functionality. Database backup is not scheduled by default. Users may perform backup for Cisco Monitor Manager and Cisco Monitor Director by scheduling the database backup script using the Microsoft Windows task scheduler. The backup script is part of the Cisco Monitor Manager and Monitor Director installation. For more information on the backup script and procedures, refer to the Cisco Monitor Manager and Cisco Monitor Director product documentation available at <http://www.cisco.com>.

Cisco Monitor Manager and Cisco Monitor Director Server Performance

Table 26-11 lists capacity information for supported devices with limited or standard licenses. (For the latest information on supported capacities and licenses, refer to the Cisco Monitor Manager and Cisco Monitor Director product documentation available at <http://www.cisco.com>.)

Table 26-11 Cisco Monitor Manager and Cisco Monitor Director Capacity Information

License Type	CPU	Physical Memory	Hard Disk Capacity	Network Devices (Router, switch, and firewall)	Access Points	IP Phones	SMB Sites
Cisco Monitor Manager limited license (not MSP)	Pentium IV 1 GHz	1 GB	40 GB	5	5	48	1

Table 26-11 Cisco Monitor Manager and Cisco Monitor Director Capacity Information (continued)

License Type	CPU	Physical Memory	Hard Disk Capacity	Network Devices (Router, switch, and firewall)	Access Points	IP Phones	SMB Sites
Cisco Monitor Manager standard license (not MSP)	Pentium IV 2 GHz	2 GB	40 GB	20	50	250	1
Cisco Monitor Director with MSP license	Pentium IV 3 GHz	2 GB	60 GB	NA	NA	NA	50

Protocol and Ports

Table 26-12 lists the ports used by the various protocol interfaces for Cisco Monitor Manager and Cisco Monitor Director. Cisco recommends opening these ports in the corporate firewall to allow communication between Cisco Monitor Manager, Cisco Monitor Director, and other devices in the network.

Table 26-12 Cisco Monitor Manager and Cisco Monitor Director Port Utilization

Protocol	Port	Service
TCP	80	HTTP
TCP	443	HTTPS
UDP	69	TFTP
UDP	514	Syslog
UDP	161	SNMP Polling

Cisco netManager

Cisco netManager performs roles similar to Unified OM in terms of providing management, monitoring, and diagnostic functionality for the entire Cisco Unified Communications system, including Cisco Unified Communications products and applications as well as the underlying IP transport infrastructure. The key difference between Cisco netManager and Unified OM is that Cisco netManager provides network management service for SMB-sized data and voice networks. Cisco netManager can manage up to 100 Cisco Unified Communications devices and 1,000 Cisco Unified IP Phone devices that belong to two Unified CM clusters and 10 Unified CME sites. For a complete list of devices support by Cisco netManager, refer to the Cisco netManager product documentation available at <http://www.cisco.com>.

Cisco netManager can be installed on a Windows-based server/workstation running the Windows 2003 Server operating system with Service Pack 1 or the Windows XP operating system with Service Pack 2. (For more information on Cisco netManager system requirements, refer to the Cisco netManager product documents available at <http://www.cisco.com>.) Cisco netManager does not require any agent software to be installed on devices being monitored. Cisco netManager utilizes open interfaces such as SNMP, WMI, and HTTP to interface with other devices in the network.

Cisco netManager presents topological views of the Cisco Unified Communications network upon completing discovery of the device connectivity information. The topological views show both the physical and logical connectivity between various devices in the Cisco Unified Communications network. Cisco netManager performs periodic auto-discovery every 4 hours to detect Cisco Unified IP

Phones associated with the managed Unified CM and Unified CME. Cisco netManager pulls Cisco Unified IP Phone information from Unified CM and Unified CME. Every 2 minutes, Cisco netManager verifies the registration status of all detected Cisco Unified IP Phones.

Cisco netManager periodically polls the managed Cisco Unified Communications devices for performance and other dynamically changing related information, and it generate events when abnormal conditions are detected. The abnormal condition could be a status failure or a violation of a threshold.

**Note**

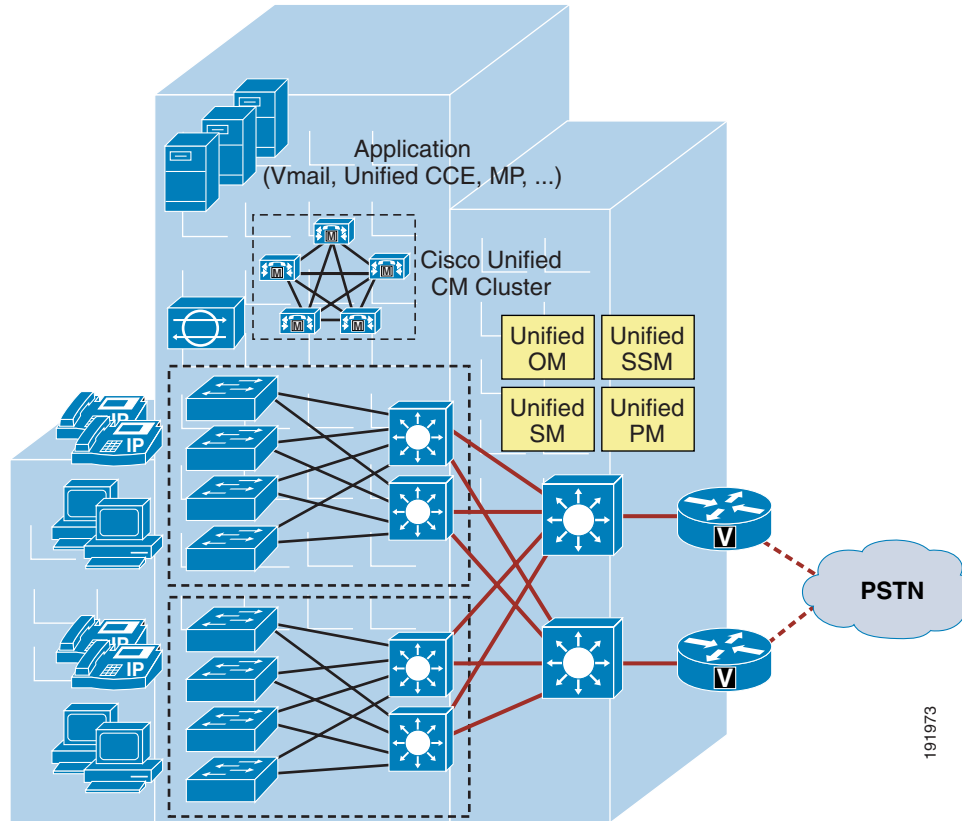
There are no failover or redundancy mechanisms available with Cisco netManager.

Integration with Cisco Unified Communications Deployment Models

This section discusses how to deploy Cisco Unified Network Management applications in various Cisco Unified Communications deployment models. For detailed information on the deployment models, see the chapter on [Unified Communications Deployment Models, page 2-1](#).

Single Site

In the single-site model, Cisco Unified 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 26-4](#) illustrates the deployment of Cisco Unified Network Management applications in the single-site model.

Figure 26-4 Single-Site Deployment

The following design characteristics and recommendations apply to the single-site model for deploying Unified OM, Unified SM, Unified SSM, and Unified PM:

- All network management applications can be deployed standalone on a dedicated Cisco Media Convergence Server (MCS) platform. However, there are many scenarios where Unified OM, Unified SM, and Unified SSM can be deployed co-resident on a shared MCS platform. Such a co-resident deployment provides the benefits of reducing the number of servers in the network and reducing the amount of network traffic that is sent between the various network management applications. The following guidelines indicate when to use co-resident or standalone deployments:
 - For less than 1,000 IP phones, deployed Unified OM, Unified SM, and Unified SSM co-resident.
 - For 1,000 to 5,000 IP phones, use one of the following deployment options:
 - Deploy Unified OM and Unified SM co-resident, and deploy Unified SSM standalone.
 - Deploy Unified OM and Unified SSM co-resident, and deploy Unified SM standalone.
 - Deploy Unified SM and Unified SSM co-resident, and deploy Unified OM standalone.
 - For 5,000 to 10,000 IP phones, deploy Unified OM and Unified SM co-resident, and deploy Unified SSM standalone.
 - For more than 10,000 IP phones, deploy standalone Unified OM, Unified SM, and Unified SSM.



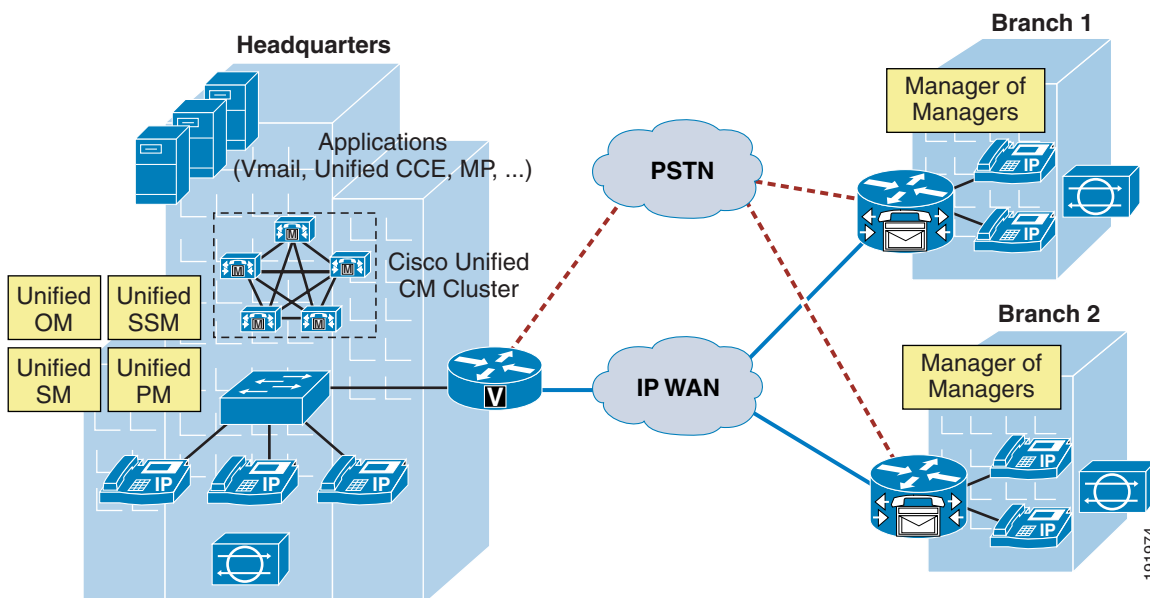
Note A single Cisco Unified Operations Manager can support a maximum of 500 route lists.

- Cisco recommends deploying CVTQ-based voice quality monitoring to monitor overall voice quality in the network.
- Cisco recommends deploying the Cisco 1040 Sensor to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.
- Each Unified OM can support a maximum 30,000 IP phones and 30 Unified CM clusters.
- Unified SM can support, concurrently, a maximum of 90,000 RTP streams per hour being monitored by the Cisco 1040 Sensor and 15,000 CVTQ-based calls per hour being monitored by Unified CM.
- Each Unified SM can support a maximum of 10 Unified CM clusters.
- Each Unified SSM can support a maximum of 30,000 IP phones and 10 Unified CM clusters.
- Each Unified PM can support a maximum of 30,000 IP phones and multiple Unified CM clusters.

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 26-5](#) illustrates the deployment of Cisco Unified Network Management applications in a multisite WAN model with centralized call processing.

Figure 26-5 Multisite WAN Deployment with Centralized Call Processing



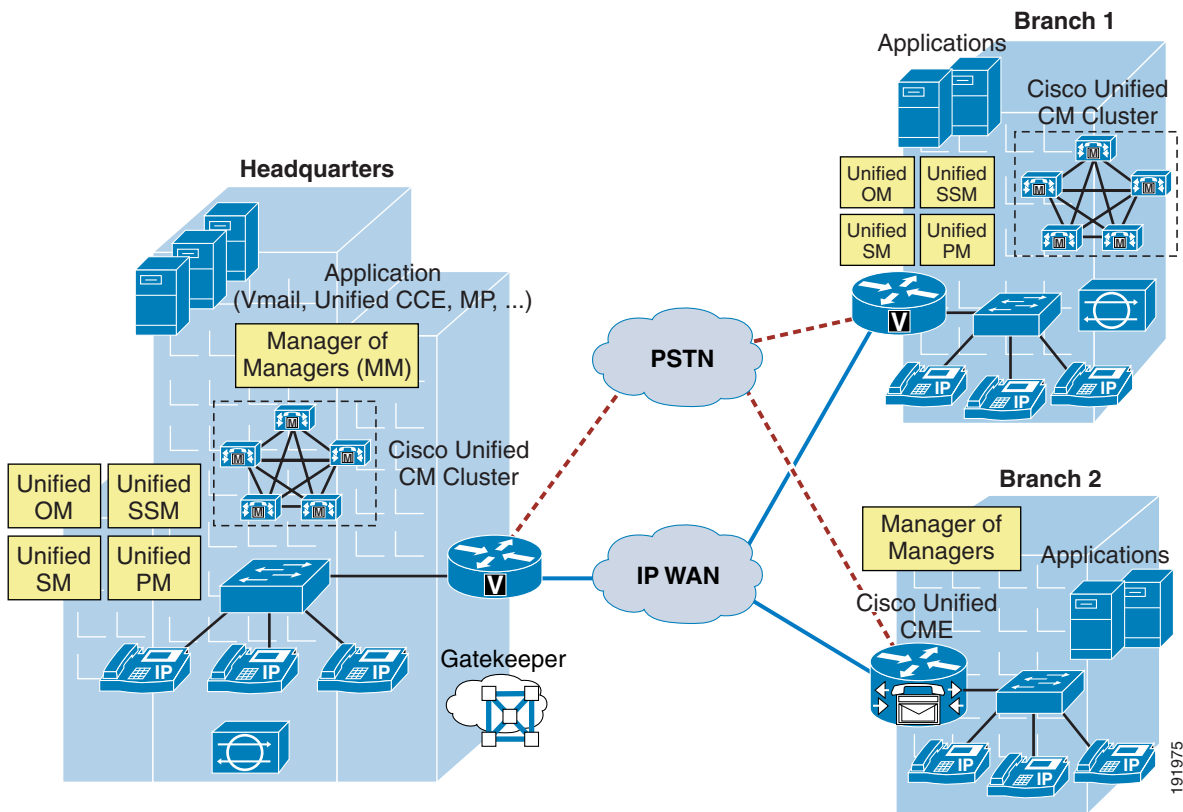
The following design characteristics and recommendations apply to the multisite model for deploying Unified OM, Unified SM, Unified SSM, and Unified PM with centralized call processing:

- Cisco recommends deploying all network management applications (including Unified OM, Unified SM, Unified SSM, and Unified PM) 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.
- Unified SM supports up to 50 Cisco 1040 Sensors. In order to monitor the voice streams of all 1000 remote sites, you can use Cisco ESPAN so that one Cisco 1040 Sensor can monitor voice streams from different remote sites across the network layer.
- All network management applications can be deployed standalone on a dedicated Cisco Media Convergence Server (MCS) platform. However, there are many scenarios where Unified OM, Unified SM, and Unified SSM can be deployed co-resident on a shared MCS platform. Such a co-resident deployment provides the benefits of reducing the number of servers in the network and reducing the amount of network traffic that is sent between the various network management applications. For detailed information on these deployment options, see the section on [Single Site, page 26-24](#).
- Cisco recommends deploying CVTQ-based voice quality monitoring to monitor overall voice quality in the network.
- Cisco recommends deploying the Cisco 1040 Sensor to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.
- Each Unified OM can support a maximum 30,000 IP phones.
- Unified SM can support, concurrently, a maximum of 90,000 RTP streams per hour being monitored by the Cisco 1040 Sensor and 15,000 CVTQ-based calls per hour being monitored by Unified CM.
- Each Unified SSM can support a maximum of 30,000 IP phones.
- Each Unified PM can support a maximum of 30,000 IP phones.

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 26-6 illustrates the deployment of Cisco Unified Network Management applications in a multisite WAN model with distributed call processing.

Figure 26-6 Multisite WAN Deployment with Distributed Call Processing



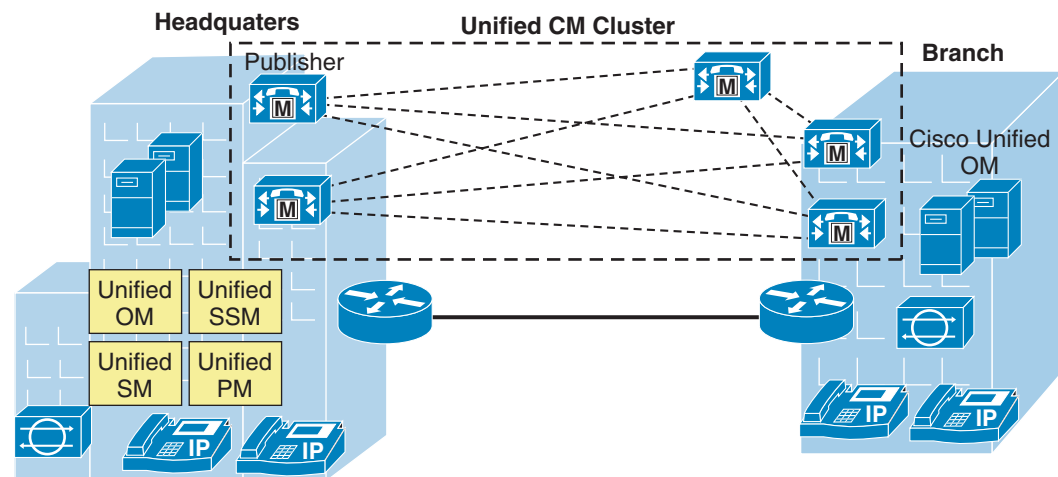
A multisite WAN deployment with distributed call processing has many of the same requirements as a single site or a multisite WAN deployment with centralized call processing in terms of deploying Unified OM, Unified SM, Unified SSM, and Unified PM. Follow the best practices and recommendations from these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

- If only one Cisco Unified Network Management system is deployed to manage multiple Unified CM clusters, Cisco recommends deploying Unified OM, Unified SM, Unified SSM, and Unified PM along with the Unified CM cluster that has the highest call volume and the most endpoints.
- If multiple Cisco Unified Network Management systems are deployed, Cisco recommends utilizing a higher-level “manager of managers” to administer those multiple systems simultaneously.
- Cisco Monitor Manager (MM), Cisco Monitor Director, and Cisco netManager can be used to manage branch offices in which Cisco Unified Communications Manager Express (Unified CME) is deployed.

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 26-7](#) illustrates the deployment of Cisco Unified Network Management applications with clustering over the WAN.

Figure 26-7 Clustering over the WAN



191976



Note

There is no native high-availability or redundancy support for Unified SM, Unified SSM, or Unified PM with this model.

The following design characteristics and recommendations apply when deploying Unified OM, Unified SM, Unified SSM, and Unified PM with clustering over the WAN:

- Cisco recommends deploying Unified OM, Unified SM, Unified SSM, and Unified PM in the headquarter site where Unified CM publisher is located.
- Cisco recommends deploying a pair of Unified OMs. Deploy the active Unified OM in the headquarter site to manage all the sites under normal conditions. The warm-standby Unified OM should be located in the branch site and should have a longer polling interval. The warm-standby Unified OM will take over for the active server and provide redundancy support (shorten its polling interval) when the active Unified OM is unavailable. Additional WAN bandwidth should be provisioned for the SNMP polling messages of the warm-standby server.
- Cisco recommends deploying CVTQ-based voice quality monitoring to monitor overall voice quality in the network.
- Cisco recommends deploying the Cisco 1040 Sensor to monitor key IP phone devices, gateway devices, and application servers in the network and to investigate and troubleshoot voice quality issues.
- Each Unified OM can support a maximum 30,000 IP phones.

- Unified SM can support, concurrently, a maximum of 90,000 RTP streams per hour being monitored by the Cisco 1040 Sensor and 15,000 CVTQ-based calls per hour being monitored by Unified CM.
- Each Unified SSM can support a maximum of 30,000 IP phones.
- Each Unified PM can support a maximum of 30,000 IP phones.