CHAPTER 4

Discovering Devices

To manage devices using Prime Collaboration, you need to discover devices in your network. After adding device credentials, you can discover and manage all collaboration endpoints, multipoint switches, application managers, call processors, routers, and switches that are part of your network.

For a list of devices supported by Prime Collaboration, see *Supported Devices for Prime Collaboration Assurance*.

Note Prime Collaboration supports third party devices whose manageability depends on the MIB-II support.

You must perform discovery to:

- Add devices to Prime Collaboration database.
- Update or change IP addresses of devices managed by Prime Collaboration.

Any discovery involves three phases:

- Access-level discovery—Prime Collaboration does the following:
  - **a.** Checks whether the device can be pinged (ICMP). If the ICMP is not enabled on the device, the device is moved to the Unreachable state. See Device States, page 4-4 for information on how to disable the ICMP verification.
  - **b.** Gets all the defined credential profiles, based on the IP address. See Managing Device Credentials to understand how to define the credential profiles.
  - **c.** Checks whether the SNMP credentials match.
  - **d.** Identifies the device types.
  - **e.** Verifies all other mandatory device credentials, based on the device type. If the mandatory credentials are not defined, discovery fails.

    See Managing Device Credentials for information on required device credentials.
- Inventory discovery—Prime Collaboration polls MIB-II and other device MIBs to collect information on the device inventory, neighboring switches, and default gateway. It also verifies whether the polled device is supported in Prime Collaboration.
- Path trace discovery—Prime Collaboration verifies whether CDP is enabled on the device and discovers the topology, based on CDP. The links between the devices are computed using CDP and they are persisted in the Prime Collaboration database.

Device States

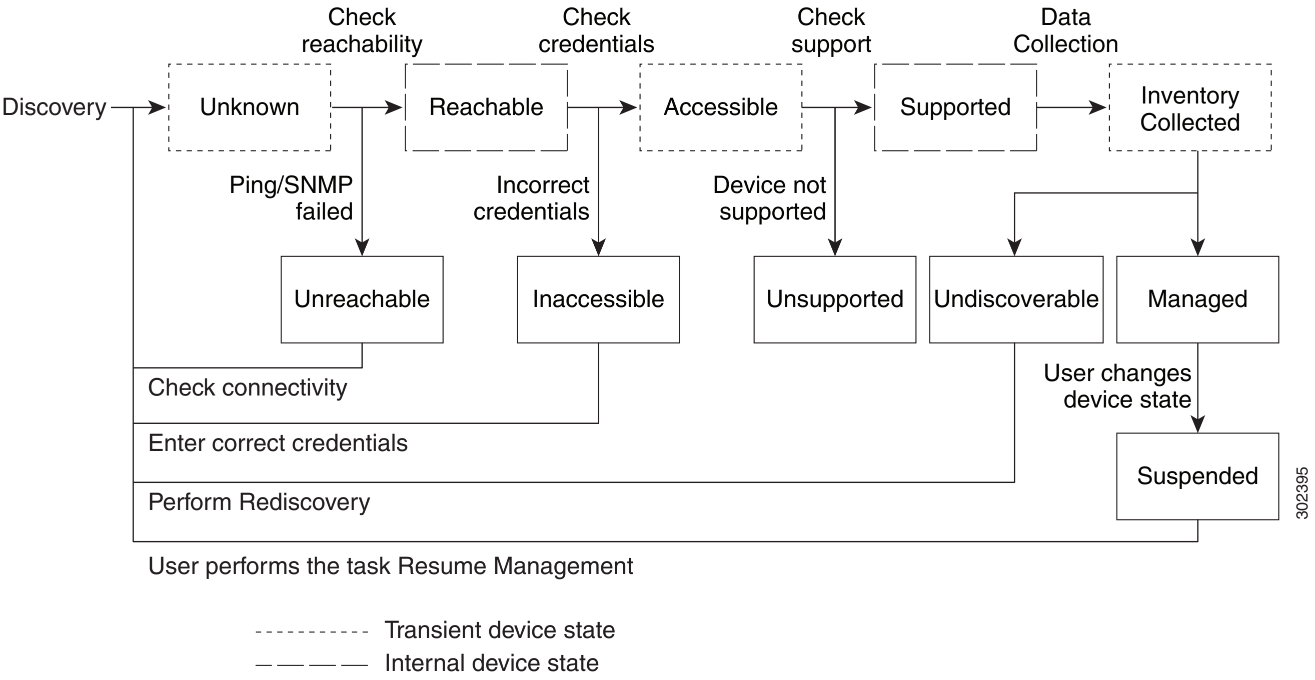
A device state indicates that Prime Collaboration is able to access the device and collect the inventory. The device state is updated only after performing either a discovery or an update inventory task.

Prime Collaboration displays the following device states:

- Unknown—This is the preliminary state, when the device is first added. This is a transient state.
- Unreachable—Prime Collaboration is unable to ping the device using ICMP, if the ICMP is not enabled on the device, the device is moved to the Unreachable state.
- Unsupported—Prime Collaboration compares the device with the device catalog. If the device does not match or the SysObjectID is not known, the device is moved to this state.
- Accessible—Prime Collaboration is able to access the device through all mandated credentials. This is part of the access-level discovery, which is an intermediate (transient) state during the device discovery.
- Inaccessible—Prime Collaboration is not able to access the device through any of the mandated credentials (see Managing Device Credentials). You must check the credentials and discover the devices.
- Deleted—The device is hidden from the Device Work Center. However, the device is in the Prime Collaboration database and can be discovered.
- Inventory Collected—Prime Collaboration is able to collect the required data using the mandated data collectors. This is part of the inventory discovery, which is an intermediate (transient) state during device discovery.
- Undiscoverable—Prime Collaboration is not able to collect the required data using the mandated data collectors.
  - CTS-Manager—Prime Collaboration must collect the endpoint data from CTS-Manager. If the data is not collected, CTS-Manager is moved to Undiscovered state. There is no mandated data collection for Cisco Unified CM, CTS, CTMS, and other network devices.
  - Connectivity issues can be caused by SNMP or HTTP/HTTPS timeout. Also, if you use HTTP/HTTPS to collect data, only one HTTP/HTTPS user can log in at a time. If Prime Collaboration faces any of these problems, the device state is moved to the Undiscoverable state. You must perform a rediscovery.
- Managed—Prime Collaboration has successfully imported the required device data to the inventory database. All session, endpoints, and inventory data are available for devices in this state. You can troubleshoot a device only if it is in this state.
- Suspended—User has suspended monitoring of the device. Session and endpoint data are not displayed for devices in this state. Periodic polling is also not performed for devices in this state. You cannot update inventory for these devices. To do so, you will need to perform Resume Management. See Suspending and Resuming Managed Devices, page 6-19 for details on suspended devices.

Figure 4-1 shows the device discovery lifecycle.

Figure 4-1 Device Discovery LifeCycle



Prime Collaboration discovers both layer 2 and layer 3 paths.

- For Cisco 500, 1000 and 3000 series TelePresence systems, Prime Collaboration discovers the first-hop router and switch. See Figure 4-2, Discovery Lifecycle for a CTS-Manager.

  The default hop count is 2 and is not configurable.

- For Cisco C and Ex series TelePresence systems, Prime Collaboration does not discover the first hop router and switch. See Figure 4-3,Discovery Lifecycle for a Cisco TMS.

The layer 3 path is discovered when a troubleshooting workflow is triggered either manually or automatically.

For further details on the Troubleshooting workflow, see Troubleshooting Sessions in the *Cisco Prime Collaboration 9.0 Network Monitoring, Reporting and Diagnostics Guide*.

See *Supported Devices for Prime Collaboration Assurance* for list of devices that are supported in Prime Collaboration.

Figure 4-2 shows the discovery lifecycle for a Cisco TelePresence Manager (CTS-Manager).

Figure 4-2 Discovery Lifecycle for CTS-Manager

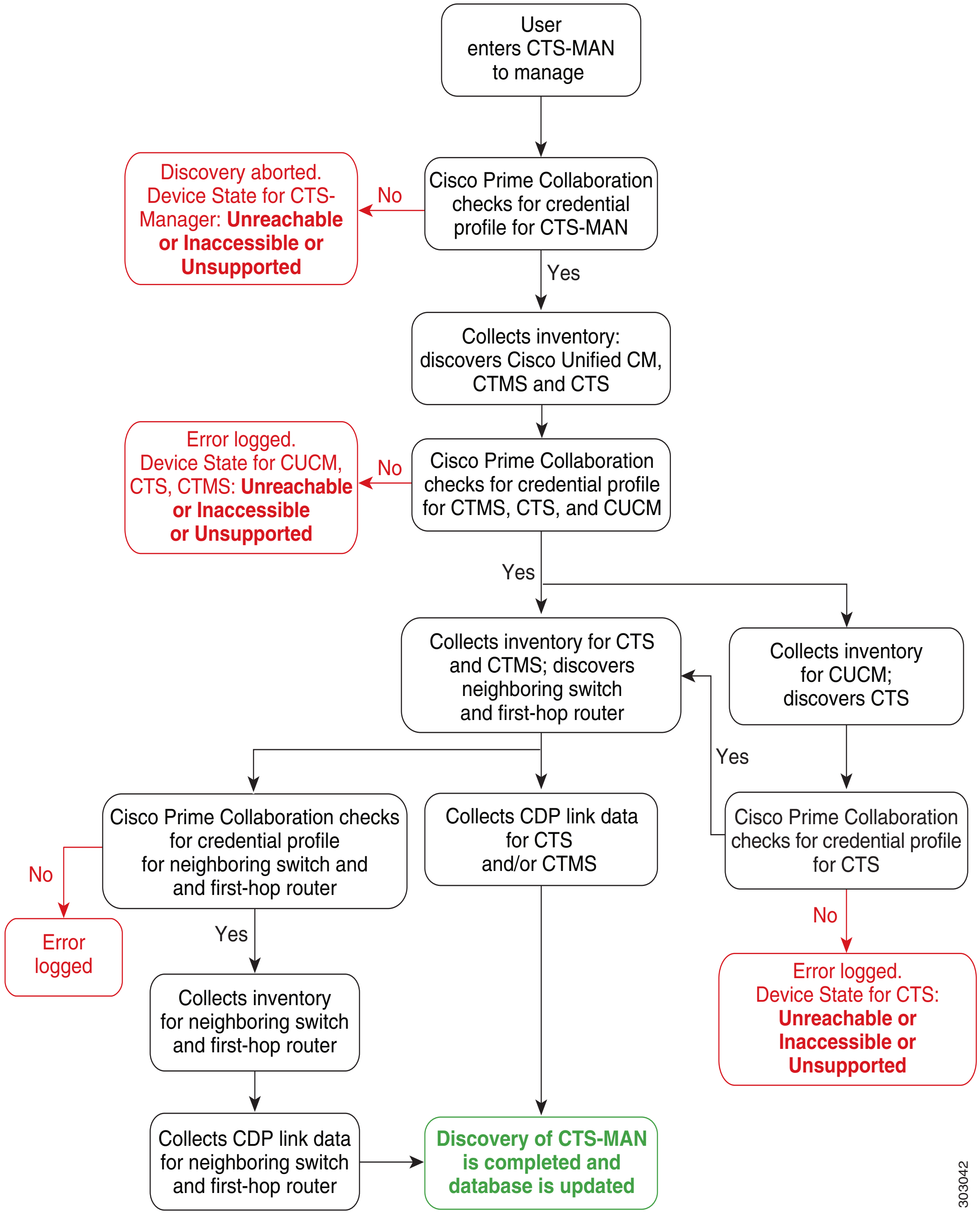
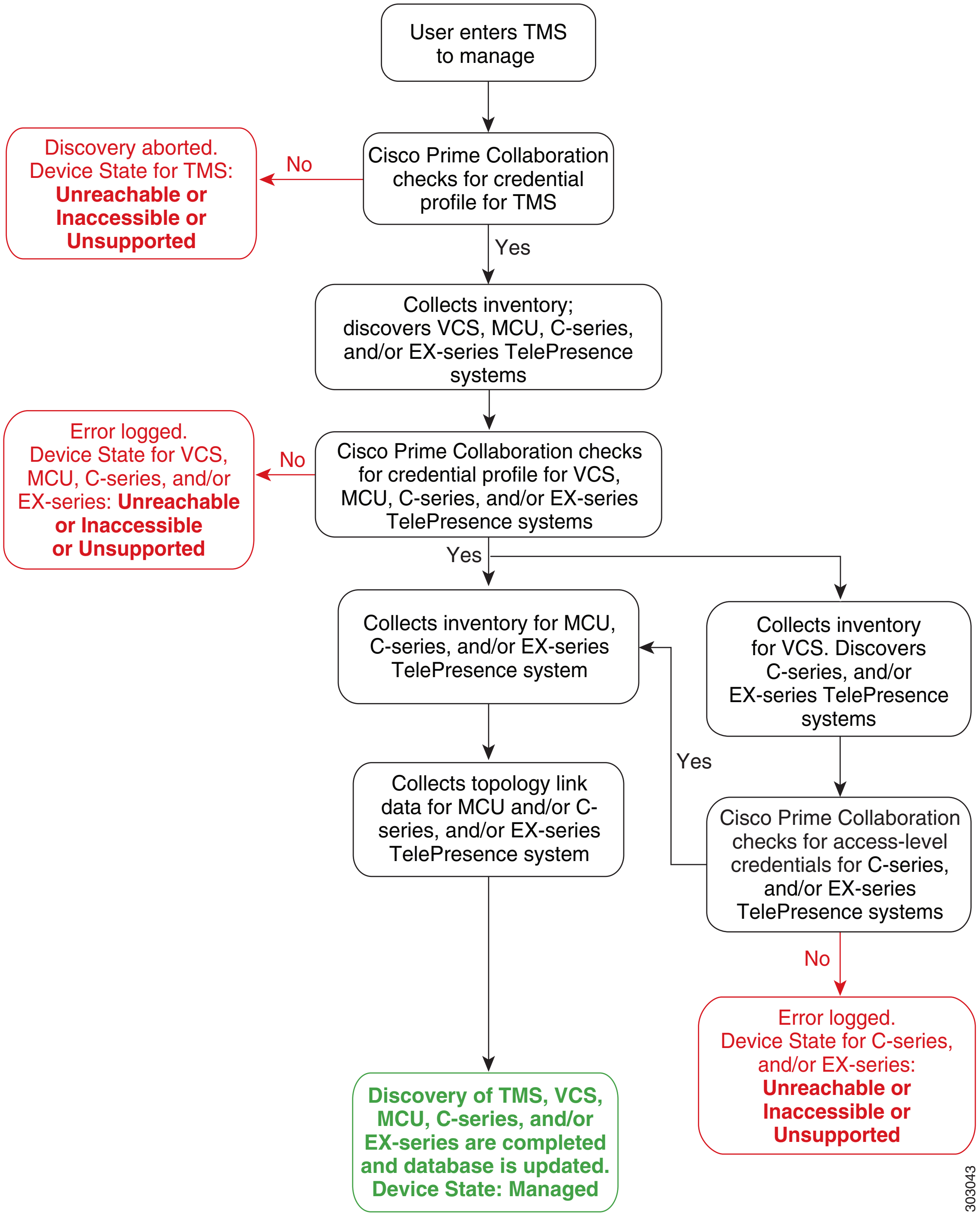

User enters CTS-MAN to manage
Cisco Prime Collaboration checks for credential profile for CTS-MAN
No
Discovery aborted. Device State for CTS-Manager: Unreachable or Inaccessible or Unsupported
Yes
Collects inventory: discovers Cisco Unified CM, CTMS and CTS
Cisco Prime Collaboration checks for credential profile for CTMS, CTS, and CUCM
No
Error logged. Device State for CUCM, CTS, CTMS: Unreachable or Inaccessible or Unsupported
Yes
Collects inventory for CTS and CTMS; discovers neighboring switch and first-hop router
Collects inventory for CUCM; discovers CTS
Yes
Cisco Prime Collaboration checks for credential profile for neighboring switch and and first-hop router
No
Error logged
Collects CDP link data for CTS and/or CTMS
Cisco Prime Collaboration checks for credential profile for CTS
No
Error logged. Device State for CTS: Unreachable or Inaccessible or Unsupported
Yes
Collects inventory for neighboring switch and first-hop router
Collects CDP link data for neighboring switch and first-hop router
Discovery of CTS-MAN is completed and database is updated
303042

Figure 4-3 shows the discovery lifecycle for a Cisco TelePresence Management System (Cisco TMS).

Figure 4-3 Discovery Life Cycle for a TMS


User enters TMS to manage
Cisco Prime Collaboration checks for credential profile for TMS
No
Discovery aborted. Device State for TMS: Unreachable or Inaccessible or Unsupported
Yes
Collects inventory; discovers VCS, MCU, C-series, and/or EX-series TelePresence systems
Cisco Prime Collaboration checks for credential profile for VCS, MCU, C-series, and/or EX-series TelePresence systems
No
Error logged. Device State for VCS, MCU, C-series, and/or EX-series: Unreachable or Inaccessible or Unsupported
Yes
Collects inventory for MCU, C-series, and/or EX-series TelePresence system
Collects inventory for VCS. Discovers C-series, and/or EX-series TelePresence systems
Yes
Collects topology link data for MCU and/or C-series, and/or EX-series TelePresence system
Cisco Prime Collaboration checks for access-level credentials for C-series, and/or EX-series TelePresence systems
No
Error logged. Device State for C-series, and/or EX-series: Unreachable or Inaccessible or Unsupported
Discovery of TMS, VCS, MCU, C-series, and/or EX-series are completed and database is updated. Device State: Managed
303043

Device Prerequisites

Note the following when managing devices:

- If Cisco Discovery Protocol (CDP) is not enabled on a media server (either it is disabled or not responding), Prime Collaboration will not discover the device correctly and the device will be moved to the Unsupported state.
- If DNS is configured on a device, ensure that Prime Collaboration can resolve the DNS name for that device. Check the DNS Server configuration to make sure it is correct. This is critical for Cisco Unified CM, Unified Presence Server, and Unity Connection devices, since without DNS resolution certain monitoring features do not work. See the *Cisco Prime Collaboration 9.0 Administration Guide*.
- If you have installed a licensed version of Prime Collaboration, it is mandatory to configure the CTS-Manager Reporting API. If this feature is not configured on the CTS-Manager 1.7, 1.8, or 1.9, Prime Collaboration will not manage the CTS-Manager.
- If you are using Cisco TMS 13.0 or 13.1, it is mandatory to configure the Cisco TMS Booking API feature. If this feature is not configured, the sessions will not be monitored.
- For Cisco TMS 13.2 and above, the Cisco TMS Booking API feature need not be configured.
- If the Cisco VCS Expressway is configured within the DMZ, Prime Collaboration should be able to access the Cisco VCS Expressway through SNMP. If it cannot, then this device is moved to the Inaccessible state.
- You can also discover the devices (endpoints, TelePresence server, and so on) individually, except for the Cisco Unified IP Phone 8900 and 9900 series, Cisco Cius, and Cisco TelePresence Movi endpoints. These endpoints are discovered only with the discovery of the call processor with which they are registered.

Note For discovery of Cisco Cius and Cisco Unified IP Phone 8900 and 9900 series, you must enable the HTTP interface so these devices appear in the inventory table.

If you have Cisco MSE Supervisor, ensure that it is registered with the Cisco TMS.

You must ensure that the device credentials that you have entered are correct. During the discovery process, based on the device that you want to discover, Prime Collaboration connects to the device using CLI, HTTP/HTTPS, or SNMP. CDP must be enabled on all CTS endpoints, CTMS, and network devices (routers and switches).

Device Discovery Methods

Cisco Prime Collaboration involves four discovery methods. Table 4-1 lists these discovery methods.

Table 4-1 Device Discovery Method

Discovery Method	Description	Information
Logical Discovery	• Discovers management applications, conferencing devices, and call processors such as CTS-Manager, Cisco TMS, Cisco VCS, and Cisco Unified CM. • All endpoints and infrastructure devices *registered* with CTS-Manager, Cisco TMS, Cisco Unified CM, and Cisco VCS are discovered automatically during logical discovery. – Logical discovery of CTS-Manager discovers Cisco TMS, Cisco Unified CM, CTS, Cisco Cius, IP phones, routers, and switches. – Logical discovery of Cisco TMS discovers VCS, codec, Cisco MCU, TPS, Cisco IP Video Phone E20, and Cisco MXP Series. • To discover clusters using logical discovery, you must discover the publisher of the cluster, which will automatically discover its subscribers and all the endpoints and infrastructure devices registered with both publisher and subscribers. – Logical discovery of the Cisco Unified CM publisher discovers other Cisco Unified CMs (subscribers) in the network, Cisco Unity, Cisco MGCP Voice Gateways, H.323 Voice Gateways, Gatekeepers, CTI applications.	• Endpoints and infrastructure devices that are *not registered* with any of the management applications, conferencing devices, or call processors cannot be discovered using logical discovery. Use ping sweep or direct discovery to discover these devices. • For more information on cluster discovery, see Discovering Devices.
Cisco Discovery Protocol (CDP)	• Discovers devices independently of media and protocol used. This protocol runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. • This discovery method queries the CDP Neighbor Table to find neighboring devices. When CDP is enabled, discovery queries the CDP cache on each seed device (and its peers) via SNMP. After CDP discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by CDP discovery, then all endpoints and infrastructure devices registered with it are also discovered.	• CDP must be enabled on the devices to perform CDP discovery.

Table 4-1 Device Discovery Method (continued)

Discovery Method	Description	Information
Ping Sweep	• Discovers devices within a range of IP addresses from a specified combination of IP address and subnet mask. • This method pings each IP address in the range to check the reachability of devices. If a device is reachable, you must specify a list of subnets and network masks to be pinged. After ping sweep discovery, a logical discovery is performed automatically. That is, if a call processor or a management device is discovered by ping sweep discovery, then all endpoints and infrastructure devices registered with it are also discovered.	• Ping Sweep discovery does not require seed devices. Instead, you must specify a list of subnets and network masks to be pinged. • Ping sweep discovery may take longer than usual to discover devices if the IP ranges are large. • You must create an "Any" credential profile for ping sweep and CDP discovery.
Direct or None	• Discovers the device directly using the IP address. • You can use this method to discover individual devices in your network.	• For example, if the discovery of a device fails because of incorrect credentials during a scheduled discovery, then you can discover the failed device alone using the direct discovery method.

Note You cannot run both Ping Sweep and CDP discovery simultaneously in your network.

Discovery depends on the type of network deployed. For recommendations on which discovery to perform, see Recommendations for Device Discovery, page 4-10.

You must add credential profiles before discovering devices. See Adding and Copying Device Credentials, page 2-1 for more information.

Recommendations for Device Discovery

These recommendations will help you decide which discovery method to use for your network.

- If you have management applications and call processors such as CTS-Manager, Cisco TMS, Cisco Unified CM, or Cisco VCS deployed in your network, you can discover these devices first using logical discovery. All endpoints registered with these devices are discovered when you discover the application managers and call processors.
- If you want to discover just the call processor and not the devices registered to the call processor, then you can use the direct device discovery method.
- If no call processors are deployed, or if no devices are registered to call processors, use ping sweep discovery. This method discovers all new infrastructure devices, new network devices, and new locations of devices in the target network. You must provide a list of subnet and network masks of

the target network. During a scheduled ping sweep discovery, all devices in the network are identified and matched with their credential profiles. If a new device is discovered, it is added to the inventory.

- If you need to discover Cisco-manufactured equipment, use CDP discovery method.
- To discover only a specific device, use direct device discovery.
- During a scheduled discovery, if discovery of a single device fails because the device is in a suspended or inaccessible state, or you have updated the device credentials, use the direct device discovery.
- After discovering Cisco Unified CM, if you have registered any new endpoints, you must rediscover CUCM Publisher node to add them to Cisco Prime Collaboration. For Cisco VCS, the newly registered endpoints are automatically discovered.
- SIP and SRST devices cannot be discovered using logical discovery. You must add these devices manually, or perform direct discovery.
- If you have both voice and video endpoints deployed in your network, ensure that you do not discover all clusters in your network at the same time, as discovery could take a long time.
- If HTTP is used to retrieve device details, HTTP firewall should be disabled.

To periodically update inventory, and synchronize the inventory with the Prime Collaboration database, you must perform inventory update. For more information, see Updating and Collecting Inventory Details, page 6-13.

After discovery, if you have changed any configuration details, you must rediscover devices. For more information, see Rediscovering Devices, page 4-18.

Additional Notes:

- If a managed device is removed from the network, it will continue to be in the Managed state until the next inventory collection occurs, even though the device is unreachable. If a device is unreachable, an Unreachable event appears that contains event information for this device appears.
- Configuration changes on a device are discovered by Cisco Prime Collaboration only during the inventory collection process. Therefore any changes to a device’s configuration will not be shown by Cisco Prime Collaboration until the next inventory collection after the configuration change.
- When you add devices, the HTTP (and HTTPS) port numbers are optional. These settings are automatically detected.
- When you add devices that have multiple interfaces and HTTP administrative access, you must manage the devices in Prime Collaboration using the same interface on which you have enabled HTTP administrative access.
- To enable Prime Collaboration to provide the correct phone count for the Cisco Unified CM Express and Cisco Unity Express (CUE), you must use the following configuration:

  ```
  ephone 8
  mac-address 001A.E2BC.3EFB
  type 7945
  ```

  where type is equal to the phone model type. If you are unsure of your model type, see Cisco.com for details on all phone model types, or enter *type?*. For information on how phone counts are displayed, see the Inventory Summary slider windowin the Device Work Center page.

- If a UC500 Series router is running Cisco Unified CM Express, configure "type" under ephone config for each phone so that the cmeEphoneModel MIB variable of CISCO-CME_MIB will return the correct phone model. This enables Prime Collaboration to discover the phones registered with Cisco Unified CM Express.
- For a Cisco Unity Express that is attached to a Cisco Unified CM Express to display in the Service Level View, you must use the following configuration:

  ```
  dial-peer voice 2999 voip <where voip tag 2999 must be different from voicemail>
  destination-pattern 2105 <prefix must be the full E.164 of configured voicemail 2105>
  session protocol sipv2
  session target ipv4:10.10.1.121
  dtmf-relay sip-notify
  codec g711ulaw
  no vad
  !
  !
  telephony-service
  voicemail 2105
  ```

  where the dial-peer VoIP tag, 2999, is not equal to the voice mail number, and the destination-pattern tag, 2105, is equal to the voice mail number. This will allow Unity Express to display properly in the Service Level View.
- Cisco Prime Collaboration manages a device only when the device's management state is set to True. A device with a management state set to False is called a suspended device. Prime Collaboration stops polling the device but may still receive device data, such as CDR records. You can also selectively unmanage device components.
- For information on how many devices Prime Collaboration can manage, see the *Cisco Prime Collaboration 9.0 Quick Start Guide*. If the Cisco Prime Collaboration inventory exceeds your device limit, you will see a warning message. For more information, see the *Cisco Prime Collaboration 9.0 Administration Guide*.
- Firewall devices are not supported in Cisco Prime Collaboration.
- Prime Collaboration supports Cisco TelePresence Conductor XC 1.2 in the standalone model. The cluster model is not supported.

Adding Devices

You can add devices to the Prime Collaboration database by performing discovery.

You must perform discovery:

- When you want to add new devices to the Prime Collaboration database.
- When you have changed the IP address of the devices.

If the IP address of a DHCP-enabled endpoint registered to Cisco Unified CM changes, Prime Collaboration may not be able to automatically discover this endpoint. This is applicable to all Cisco TelePresence systems registered with Cisco Unified CM.

The endpoints registered with Cisco VCS are discovered automatically when the IP address is changed. Newly registered endpoints are also discovered automatically.

You must rediscover the following:

- The endpoints, by providing the new IP address or hostname.
- The Cisco Unified CM instance with which the endpoint is registered.

- The CTS-Manager with which the endpoint is registered.

If the IP address changes for network devices and infrastructure devices (such as CTS-Manager, Cisco Unified CM, CTMS, Cisco MCU, Cisco VCS, Cisco TS, and so on), you must discover these devices by providing the new IP address or hostname.

You can either discover devices immediately or schedule a discovery job.

Note A discovery job, once started, cannot be stopped or canceled.

To discover devices:

Step 1 Choose **Operate** > **Device Work Center**.

Step 2 In the Device Work Center page, click **Discover Devices**.

Step 3 Enter the job name, and check the **Enable device accessibility verification during device discovery** check box.

Prime Collaboration verifies device accessibility using SNMP, CLI, HTTP (HTTPS), and JTAPI.

Step 4 Select a discovery method. For information on the best discovery option to use, see Recommendations for Device Discovery, page 4-10.

Step 5 Enter IP address or hostname of the device.

For Logical Discovery, Cisco Discovery Protocol and Direct Discovery, you can enter multiple IP addresses or hostnames using one of the supported delimiters: comma, colon, pipe, or blank space.

For Ping Sweep specify a comma-separated list of IP address ranges using the /netmask specification. For example, use 172.20.57.1/24 to specify a ping sweep range starting from 172.20.57.1 and ending at 172.20.57.255.

If you want to discover CTS-Manager or TMS cluster, you must enter the IP address of Primary, Secondary, Hot Standby, and the Load-Balancer servers as mentioned in the Manager Cluster page (**Device WorkCenter > Manage CTS-MAN/TMS Clusters**).

Step 6 You can either schedule a periodic discovery job or run the discovery job immediately. To run the job immediately, go to Step 9.

Step 7 (Optional) Enter the Filter and Advanced Filter details (available only for logical, CDP and ping sweep discovery methods). You can use wildcard to enter the IP address and DNS information that you may want to include or exclude. See Table 4-2 for field descriptions.

Step 8 Enter scheduling details to schedule a discovery job.

- Start Time—Click **Start Time** to enter the start date and time in the yyyy/MM/dd and hh:mm AM/PM formats, respectively.
- Click the date picker if you want to select the start date and time from the calendar. The time displayed is the client browser time. The scheduled periodic job runs at this specified time.
- Recurrence—Click **None**, **Hourly**, **Daily**, **Weekly**, or **Monthly** to specify the job period.
- Settings—Specify the details of the job period.
- End Time—If you do not want to specify an end date/time, click **No End Date/Time**. Click *Every number of* **Times** to set the number of times you want the job to end in the specified period. Enter the end date and time in the *yyyy/MM/dd* and *hh:mm* AM/PM formats, respectively.

Step 9 Click **Run Now** to immediately run the discovery job, or click **Schedule** to schedule a periodic discovery job to run at a later time.

A dialog box appears with the Discovery Job status. You can click the Job Progress Details link which will take you to the **Job Management** page. See Verifying Discovery Status, page 4-19 for more information.

Table 4-2 describes the filters that are available when you run discovery.

Table 4-2 Discovery Filters

Filter	Description
IP Address	Enter comma-separated IP addresses or IP address ranges for devices that you want to include or exclude. Use wildcards when specifying the IP address range. An asterisk (*) denotes the octet range of 1-255. Also, the octet range can be constrained using the [xxx-yyy] notation. For example: • To include all devices in the 172.20.57/24 subnet, enter an include filter of 172.20.57.*. • To exclude devices in the IP address range of 172.20.57.224 to 172.20.57.255 enter an exclude filter of 172.20.57.[224-255]. Both types of wildcards can be used in the same range specification; for example, 172.20.[55-57].*. If both include and exclude filters are specified, the exclude filter is applied before the include filter. After a filter is applied to an auto-discovered device, no other filter criterion will be applied to the device. If a device has multiple IP addresses, the device will be processed for auto-discovery as long as it has one IP address that satisfies the include filter.
Advanced Filter	

Table 4-2 Discovery Filters (continued)

Filter	Description
DNS Domain	Enter comma-separated DNS domain names for devices that you want to include or exclude. An asterisk (*) matches any combination of mixed uppercase and lowercase alphanumeric characters, along with the hyphen (-) and underscore (_) characters, of an arbitrary length. A question mark (?) matches any of the following: • A single alphanumeric character • A hyphen • An underscore character For example*.*cisco.com* matches any DNS name ending with *.cisco.com. *.?abc.com* matches any DNS name ending with *.aabc.com*, or *.babc.com*, etc.
Sys Location	Available only for CDP and ping sweep discovery methods. Enter comma-separated strings that will match the string value stored in the sysLocation OID in MIB-II, for devices that you want to include or exclude. An asterisk (*) matches, up to an arbitrary length, any alphanumeric characters, hyphen (-), underscore (_), and, white space (spaces and tabs). A question mark (?) wildcard matches a single occurrence of any of the above characters. For example, a SysLocation filter of San * will match all SysLocation strings starting with San Francisco, San Jose, etc.

Cisco VCS Cluster

Prime Collaboration supports Cisco VCS clusters. You must ensure that the cluster names are unique. All the endpoints that need to be managed in Prime Collaboration should be registered in the Cisco VCS master.

Discovering Cisco Unified CM Clusters

Prime Collaboration supports Cisco Unified CM clusters. You must ensure that the cluster IDs are unique.

You must ensure that the access control list in Cisco Unified CM contains all endpoints that need to be managed. If the Cisco Unified CM SNMP user configuration includes the use of the access control list, you must enter the Prime Collaboration server IP address on all Cisco Unified CM nodes in the cluster.

Prime Collaboration must discover and manage only the Cisco Unified CM publisher to manage a cluster. All subscribers must be discovered only through the publisher. You must not discover the subscribers directly.

Prime Collaboration must manage the publisher to monitor a cluster. The computer telephony integration (CTI) service must be running on all subscribers.

Note The JTAPI credential is optional for Cisco Unified CM clusters. However, the SNMP and HTTP credentials are mandatory for Cisco Unified CM publishers and subscribers.

You can schedule a Cisco Unified CM cluster discovery using Cluster Data Discovery. You can discover only phones registered with Cisco Unified CM clusters in this discovery. To discover video endpoints, you need to discover clusters using Adding Devices, page 4-12.

Cluster Data Discovery Settings

Cluster data discovery is performed by the Common Devices Table (CDT) module. This allows Prime Collaboration to consolidate the inventory and the device registration information it collects from Unified CMs (Unified CM). It collects two different categories of information from Unified CMs:

- Cluster configuration data including Redundancy group, Devicepool, Location, Region, RouteList, RouteGroup, RoutePattern, Partition, and so on. This also includes the entities provisioned in the cluster such as phones, voice mail endpoints, media resources, gateways, and trunks.
- Registration information—Registration information corresponds to all the entities which register with the Unified CM cluster. This includes Device IP, Registration status, the Unified CM server to which the entity is registered currently, the latest registration/unregistration timestamp, and the status reason.

  Registration information can be configured using a configuration file. This information is collected from all the subscriber nodes in the clusters to which the entities like phones or gateways register.

For this data collection to occur successfully it requires:

- Cisco RIS Data Collector to be running in 7.x versions of Unified CM.
- Cisco SOAP - CDRonDemand Service to be running in other versions of Unified CM.

The data collected from the Unified CM cluster is used in other modules such as the Diagnostics View, Phone Inventory, Service Level View, and Voice Health Monitor (VHM).

Prerequisites to Running Cluster Device Discovery

Ensure the following prerequisites for data collection are completed before using cluster device discovery.

- Data is collected from Publisher/First node through AXL. Therefore, the publisher should be in fully in monitored state with proper HTTP credentials entered and the AXL Web Service should be running in the publisher.
- AXL is not supported in Unified CM versions prior to 4.x. These clusters cannot be monitored.
- If the Unified CM publisher is configured using name in the CUCM section/System Server section of Prime Collaboration Administration, then this name must be resolvable through DNS from the Prime Collaboration server. Otherwise, an entry must be configured for this name in the hosts files for the data collection to proceed further.
- Any changes in the registration information are updated through processing the relevant syslogs from the Cisco Unified CM. For Prime Collaboration to be able to receive syslogs and process configurations required in the Unified CM, you must perform the steps in Syslog Receivers section.

  Syslog processing can detect the following for the entities registered to the Cisco Unified CM cluster:

  - Any registration changes on entities such as phone, voice mail endpoint, gateways, and so on.

- Any new phones provisioned in the cluster are detected and updated to the inventory.

Other devices may also require configuring syslogs from within the device. For details on the device configurations required, see Syslog Receivers section in the *Setting Up Devices for Prime Collaboration*.

Scheduling Between Discoveries

If any of the following changes occur on the cluster configuration before the scheduled periodic data collection and you want these changes to appear in Prime Collaboration immediately, you must use the **Run Now** option to ensure the following types of data are collected:

- New device pools, location, region, redundancy group, Route List, Route Group, Route pattern or Partition added, deleted or modified in the cluster.
- Changes in membership of any end point to the device pool or association of any end point to the redundancy group.
- New subscriber added to or deleted from the Unified CM cluster.
- Changes in membership of any subscriber to the redundancy group.
- Changes in membership of any gateway to Route group or Route Group to Route List.

This option triggers data collection and synchronizes all the clusters monitored in Prime Collaboration.

If changes are limited to a specific cluster, the publisher of the cluster can be rediscovered by using **Operate > Device Work Center > Rediscover**.

Scheduling Cluster Data Discovery

Prime Collaboration collects cluster configuration from the Cisco Unified CM once a day as well as at startup. This periodic discovery data collection is done by default at midnight daily. You can change this default schedule using the Cluster Device Discovery.

Note

- You can schedule only Cisco Unified CM cluster discovery using Cluster Data Discovery.
- Only voice endpoints registered to CUCM are discovered. TelePresence endpoints are not discovered.

When you choose **Administration > System Setup > Assurance Setup > Cluster Data Discovery Settings**, you can view cluster device discovery status or set the schedule to run a discovery.

To schedule or view cluster device discovery:

Step 1 Choose **Administration > System Setup > Assurance Setup > Cluster Data Discovery Settings**.

The Cluster Device Discovery window displays the following:

- Discovery Status—Displays the status of the discovery process using any of the following categories:
  - In progress—When you start SEGServer for the first time or restart it, discovery takes place automatically and the status appears as `In Progress`.
  - Completed—The discovery process is complete.
  - Not available. Try after some time—Appears when you start SEGServer for the first time, or restart it, and the discovery process has not yet begun.

- Last Discovery Start Time—Displays the start time of the last discovery.
- Last Discovery End Time—Displays the end time of the last discovery.
- Device Schedule using the hour and minute set for the discovery reoccurrence.

Step 2 Click **Apply** to set the discovery schedule for a future discovery, or **Run Now** to run the cluster discovery immediately.

Rediscovering Devices

You can rediscover devices that have already been discovered. The credentials previously entered are already available in the Prime Collaboration database, and the system updates the new changes. Devices in any state can be rediscovered.

To rediscover a device use the **Rediscover** button on the Inventory table.

Perform rediscovery when:

- A deleted device must be rediscovered.
- There are changes in the first hop router configuration, and for software image updates.
- There are changes to the credentials, location, time zone, and device configurations such as IP address or hostname, SIP URI, H.323 gatekeeper address, and so on.

Note Accessibility information is not checked during rediscovery.

The workflow for rediscovery is the same as for discovery. See Figure 4-1 for details.

Rediscovering Deleted Devices

To rediscover the devices listed in the Current Inventory table, you can use the **Rediscover** button available in the Current Inventory pane. You can select a single device and perform the rediscovery.

To rediscover deleted devices:

Step 1 Choose **Operate > Device Work Center**.

Step 2 From the Device Work Center page, filter the devices in the Deleted state from the Current Inventory table.

You can use the quick filter Deleted to get the list of devices in this state.

Step 3 Choose the devices you want to rediscover, and click **Rediscover**.

A message appears, `Are you sure you want to Rediscover the selected devices?`

Step 4 Click **OK.**

A message appears, `Selected devices Rediscovered successfully.`

You can check the progress and the status of the job, using the **Discovery Jobs** button on the **Device Work Center** page. The Job Management page appears with the list of discovery jobs. For more information, see Verifying Discovery Status, page 4-19.

Note When you rediscover VCS, deleted Cisco Jabber video will be moved to Managed state if it is accessible.

Verifying Discovery Status

The status of all discovery jobs are displayed in the Job Management page. After running discovery, a dialog box appears with the Job Progress Details link to view the status of discovery in the Job Management page. You can also choose **Operate > Device Work Center > Discovery Jobs** to navigate to the Job Management page.

The time taken to complete a discovery job depends on your network. After the discovery is complete, the details appear on the Current Inventory table.

To verify the discovery was successful:

Step 1 Choose **Operate** > **Device Work Center** > **Discovery Jobs**.

Step 2 From the Job Management page, select the discovery job for which you want to view the details.

The status of discovery, and all the devices discovered during discovery appear in the pane below the Job Management table.

Step 3 The Job details pane has the Job Instance Result popup next to the Job ID. This lists the details about the devices that are discovered.

There may be devices that are not discovered because of incorrect credentials. Verify the credentials for these devices (see Verifying Device Credentials, page 2-6) and run the discovery again.

If the CTS-Manager discovery has failed with the error `UNDISCOVERABLE Exception:: null`, perform the discovery again. This issue occurs because multiple users may be accessing CTS-Manager at the same time.

If you are discovering the same devices more than once, use the rediscover option. For more information see Rediscovering Devices, page 4-18.

Importing Device List and Credentials

You can import device lists, device properties or attributes and device credentials from Cisco Unified Operation Manager to Prime Collaboration using the Import feature. You can also import an exported list of devices and credentials from Prime Collaboration.

To import device information from a file:

Step 1 Choose **Operate** > **Device Work Center**.

Step 2 Click **Import**.

Step 3 In the Import dialog box, enter the Device List and Credentials file name.

Or

Browse the file system and enter the file using the Browse option. Only XML file format is supported.

Step 4 Click **Import**.

A message appears that the import job has been scheduled successfully, if you have scheduled an import job.

Credential Profiles are not created for the imported list of devices and credentials. After import, device discovery is triggered automatically using the credentials available in the import file. If any of the imported device credentials are incorrect, then the device may not be in Managed state.

After discovery, the imported devices appear in the inventory. Other device details, physical information, access information are displayed in the respective panes below the inventory table.

Exporting Device List and Credentials

You can export device lists, device properties or attributes and device credentials into a file. You can view the list of attributes that can be exported and edit the Export Format file to specify the credentials you need to export.

To export device list and credentials:

Step 1 Choose **Operate > Device Work Center > Export**.

The Export dialog box appears. You have options to export device list and credentials, and device inventory.

Step 2 Select Device list and Credentials, and enter a name for the output file.

Any device in Managed state in the inventory will be exported. Only XML file format is supported.

Step 3 Click **Export**.

A dialog box appears asking you to either open or save the file. Click **Open** to view the information, or click **Save** to save the .xml file on your local system.