



CHAPTER 3

CWVM Device Management

CWVM has a distributed architecture, allowing system changes to be shared among network elements within CWVM. For example, if a gateway, group, Cisco UBE gatekeeper, or Cisco UBE directory gatekeeper is added, modified, moved, or deleted, all associated clients logged into CWVM are notified.

The following topics are associated with CWVM device management:

- [Groups, page 3-1](#)
- [Cisco UBE Gatekeepers, page 3-3](#)
- [Gateways, page 3-21](#)
- [CME Routers, page 3-34](#)
- [SRST Routers, page 3-39](#)
- [Batch Add Files, page 3-43](#)
- [Synchronizing Devices, page 3-45](#)
- [Automating Tasks, page 3-46](#)

Groups

You create groups in CWVM to manage gateways that are not managed by a Cisco UBE gatekeeper. A group is a logical partition that contains gateways that interact with each other in a network. Groups must be created to manage gateways in VoFR/VoATM networks, because these networks do not use Cisco UBE gatekeepers. Groups must also be created in VoIP networks that contain gateways that are not managed by a Cisco UBE gatekeeper. When you add a gateway to a group and make changes to the phone number on its voice port, CWVM automatically propagates dial plan information among all gateways in the group.

See the following topics for more information about working with groups:

- [Creating a Group, page 3-2](#)
- [Modifying a Group, page 3-2](#)
- [Moving a Group, page 3-2](#)
- [Deleting a Group, page 3-3](#)

Creating a Group

Procedure

- Step 1** From the tree view, right-click the network or CWVM server to which you want to add the group. A popup menu appears.
- Step 2** Select **Add Group...** The Add Group dialog box appears.
- Step 3** Enter a group name in the Group Name field.
- Step 4** Enter a group description in the Group Description field.
- Step 5** Click **Finish**. The group appears in the tree.



Note

You can add a number of groups at the same time by importing a batch add file. For more information, see [Batch Add Files, page 3-43](#).

Related Topics

- [Groups, page 3-1](#)
- [Modifying a Group, page 3-2](#)
- [Deleting a Group, page 3-3](#)

Modifying a Group

Procedure

- Step 1** From the tree view, right-click the group that you want to modify. A popup menu appears.
- Step 2** Select **Modify...** The Modify Group window appears.
- Step 3** Modify the group name or description.
- Step 4** Click **Finish**. The group is modified.
-

Related Topics

- [Groups, page 3-1](#)
- [Creating a Group, page 3-2](#)
- [Deleting a Group, page 3-3](#)

Moving a Group

You can move groups between networks under a single CWVM server in a selected network tab view.

Procedure

- Step 1** Select the VoIP or VoATM/FR view.
- Step 2** From the tree, click the group you want to move.
- Step 3** Drag and drop the group to the place where you want it moved (within the selected tab view).

**Note**

If you are performing this task in the VoIP view, underlying gateways are updated only in the VoIP view. You should later select the VoATM/FR view and move the gateways to the new network.

Deleting a Group

If a group no longer contains any gateways, you might want to delete it from CWVM. You can delete only groups that do not contain routers.

Procedure

- Step 1** From the tree view, right-click the group you want to delete. A popup menu appears.
- Step 2** Select **Delete**.
- Step 3** Click **Yes** to confirm the deletion of the group. The group is deleted from the tree view.
-

Related Topics

- [Groups, page 3-1](#)
- [Creating a Group, page 3-2](#)
- [Modifying a Group, page 3-2](#)

Cisco UBE Gatekeepers

Cisco UBE gatekeepers are used only in VoIP networks. When added to CWVM, they appear only in the VoIP view. When adding a Cisco UBE gatekeeper to CWVM, you must know its IP address or DNS name and its Enable and Telnet passwords. The Cisco UBE gatekeeper must also be running the appropriate Cisco IOS gatekeeper software.

CWVM can have different levels of Cisco UBE gatekeepers. Parent Cisco UBE gatekeepers can help expedite call resolution. These parent Cisco UBE gatekeepers are called Cisco UBE directory gatekeepers. Cisco UBE directory gatekeepers know only about the Cisco UBE gatekeepers that they manage or other associated Cisco UBE directory gatekeepers. Cisco UBE directory gatekeepers do not manage individual gateways.

See the following topics for more information on working with Cisco UBE gatekeepers:

- [Adding a Cisco UBE Gatekeeper or Cisco UBE Directory Gatekeeper, page 3-4](#)
- [Modifying a Cisco UBE Gatekeeper, page 3-5](#)

- [Moving a Cisco UBE Gatekeeper, page 3-6](#)
- [Deleting a Cisco UBE Gatekeeper, page 3-6](#)
- [Converting a Cisco UBE Gatekeeper to a Cisco UBE Directory Gatekeeper, page 3-7](#)
- [Converting a Cisco UBE Directory Gatekeeper to a Cisco UBE Gatekeeper, page 3-7](#)
- [Configuring a Cisco UBE Gatekeeper, page 3-8](#)
- [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#)
- [Managing Local Zones, page 3-11](#)
- [Managing Remote Zones, page 3-13](#)
- [Managing Zone Prefixes, page 3-15](#)
- [Managing Technology Prefixes, page 3-18](#)
- [Verifying a Phone Number Under a Cisco UBE Gatekeeper, page 3-20](#)

Adding a Cisco UBE Gatekeeper or Cisco UBE Directory Gatekeeper

When you add a Cisco UBE gatekeeper to CWVM, you must know its IP address or DNS name and its Enable and Telnnet passwords. CWVM searches the Cisco UBE gatekeeper for such configurations as zone, bandwidth, and technology prefix. CWVM saves this information in its database. You can propagate zone information between top level Cisco UBE gatekeepers and Cisco UBE directory gatekeepers.

Before you add a Cisco UBE gatekeeper under a Cisco UBE directory gatekeeper, you must configure the Cisco UBE directory gatekeeper's remote zone and zone prefixes to cover zone prefixes that its children will manage. If a Cisco UBE directory gatekeeper's remote zone prefixes do not cover the child Cisco UBE gatekeeper's zone prefix, CWVM does not allow you to add the child Cisco UBE gatekeeper. See [Configuring a Cisco UBE Gatekeeper, page 3-8](#), for more information on how to configure a Cisco UBE gatekeeper.

CWVM also allows you to add backup Cisco UBE gatekeepers or backup Cisco UBE directory gatekeepers to the system. See the following procedure for details.



Note

You cannot add gateways to Cisco UBE directory gatekeepers.

Procedure

- Step 1** Select the VoIP view.
- Step 2** From the tree, right-click the network or CWVM server to which you want to add the new Cisco UBE gatekeeper. A popup menu appears.
- Step 3** Select **Add Cisco UBE Gatekeeper...** (when adding a Cisco UBE gatekeeper) or **Add Cisco UBE Directory GK...** (when adding a Cisco UBE directory gatekeeper).
- Step 4** Enter the following values for the Cisco UBE gatekeeper:
 - IP address of device
 - IP address of an HSRP backup Cisco UBE gatekeeper, if applicable.
 - Community string read
 - Community string write

- Login username

Step 5 Enter the following passwords for the Cisco UBE gatekeeper:

- Telnet
- Enable



Note The device should have “>” at the end of a login prompt and “#” at the end of an enable prompt. For example: `router>` and `router#`.

Step 6 Click **Finish**. The Cisco UBE gatekeeper is added to the tree. In addition, a dialog box that lists the commands delivered to the device is displayed.



Note You can add a two or more Cisco UBE gatekeepers or Cisco UBE directory gatekeepers at the same time by importing a batch add file. For more information, see [Batch Add Files, page 3-43](#).

Modifying a Cisco UBE Gatekeeper

You can modify a Cisco UBE gatekeeper in CWVM to change its credentials, HSRP Cisco UBE gatekeeper, or HSRP Cisco UBE directory gatekeeper. For example, you can use CWVM to modify the password. Information is updated in the CWVM database.



Note Because CWVM supports a wide variety of Cisco routers, only basic information about Cisco UBE gatekeepers is provided in this document. For detailed information, refer to the documentation provided with your Cisco router.

Procedure

Step 1 Select the VoIP view.

Step 2 From the tree, right-click the Cisco UBE gatekeeper you want to modify. A popup menu appears.

Step 3 Select **Modify...**

Step 4 Modify either or both of the following:

- IP address of an HSRP backup Cisco UBE gatekeeper, if applicable. Refer to the device’s documentation for information on how to configure a device as an HSRP backup Cisco UBE gatekeeper.



Note From this point on, any CLI configurations or changes to the primary Cisco UBE gatekeeper are not updated in the backup Cisco UBE gatekeeper.

- Login username

- Step 5** Click **Change Credentials** to modify community strings and the Enable and Telnet passwords:
- Enter the old community strings, Enable password, and Telnet password in the Old field.
 - Enter the new community strings, Enable password, and Telnet password once in the New field.
 - Enter the new community strings, Enable password, and Telnet password a second time in the Confirm field to confirm that you have typed them correctly.
 - Click **OK**.



Note CWVM will change the credentials only in the database and not on the actual device.

- Step 6** Click **Finish**. The Cisco UBE gatekeeper is modified.

Related Topics

- [Moving a Cisco UBE Gatekeeper, page 3-6](#)
- [Configuring a Cisco UBE Gatekeeper, page 3-8](#)
- [Managing Zone Prefixes, page 3-15](#)
- [Managing Technology Prefixes, page 3-18](#)
- [Managing Local Zones, page 3-11](#)
- [Managing Remote Zones, page 3-13](#)

Moving a Cisco UBE Gatekeeper

You can move top-level Cisco UBE gatekeepers or Cisco UBE directory gatekeepers from one network to another network under a single CWVM server. See also [Moving a Gateway, page 3-32](#).

Procedure

- Step 1** Select the VoIP view.
- Step 2** From the tree, click the Cisco UBE gatekeeper you want to move.
- Step 3** Drag and drop the Cisco UBE gatekeeper to where you want it moved (within the VoIP view).



Note Underlying gateways are updated only in the VoIP view. You should later select the VoATM/FR tab view and move the gateways to the new network.

Deleting a Cisco UBE Gatekeeper

If you are no longer using a Cisco UBE gatekeeper in your network, you might want to delete it from CWVM. Before deleting it, make sure it no longer controls any gateways. Before deleting a Cisco UBE directory gatekeeper, make sure it no longer controls any Cisco UBE gatekeepers. You must delete all Cisco UBE gatekeeper children first.



Note When a Cisco UBE gatekeeper is deleted, any associated backup Cisco UBE gatekeepers or Cisco UBE directory gatekeepers are also deleted.

Procedure

- Step 1** Select the VoIP view.
 - Step 2** From the tree, right-click the Cisco UBE gatekeeper you want to delete. A popup menu appears.
 - Step 3** Select **Delete....**
 - Step 4** Click **OK** to confirm the deletion of the Cisco UBE gatekeeper. The Cisco UBE gatekeeper is deleted from the tree.
-

Converting a Cisco UBE Gatekeeper to a Cisco UBE Directory Gatekeeper

This procedure converts a Cisco UBE gatekeeper to a Cisco UBE directory gatekeeper, which enables location requests (LRQs) to be forwarded to the device. Before converting a Cisco UBE gatekeeper to a Cisco UBE directory gatekeeper, make sure there are no gateways under its control.

Procedure

- Step 1** Select the VoIP view.
 - Step 2** From the tree, right-click the Cisco UBE gatekeeper you want to convert to a Cisco UBE directory gatekeeper. A popup menu appears.
 - Step 3** Select **Convert to Cisco UBE Directory Gatekeeper....** A dialog box appears, asking if you are sure you want to convert this Cisco UBE gatekeeper to a Cisco UBE directory gatekeeper.
 - Step 4** Click **Yes**. The Cisco UBE gatekeeper is now a Cisco UBE directory gatekeeper.
-

Converting a Cisco UBE Directory Gatekeeper to a Cisco UBE Gatekeeper



Note CWVM does not remove the LRQ forwarding command from the device when CWVM converts a Cisco UBE directory gatekeeper to a Cisco UBE gatekeeper.

Procedure

- Step 1** Select VoIP view.
- Step 2** From the tree, right-click the Cisco UBE directory gatekeeper you want to convert to a Cisco UBE gatekeeper. A popup menu appears.
- Step 3** Select **Convert to Cisco UBE Gatekeeper....** A dialog box appears, asking if you are sure you want to convert this Cisco UBE directory gatekeeper to a Cisco UBE gatekeeper.

Step 4 Click **Yes**. The Cisco UBE directory gatekeeper is now a Cisco UBE gatekeeper.

Configuring a Cisco UBE Gatekeeper

Follow this procedure to do any of the following:

- Enable or disable automatic repeat request (ARQ) or LRQ reject unknown prefixes
- Enable or disable ARQ or LRQ reject low resources
- Enable or disable LRQ reject unknown circuits or (location reject) LRJ immediate-advance
- Configure ARQ hop off zone
- Configure bandwidth
- Configure zones and technology prefixes

If you are working with a Cisco UBE directory gatekeeper, you can also use this procedure to:

- Enable the LRQ time-to-live
- Configure the allowable LRQ hop count




Note

By design, the Cisco UBE gatekeeper configuration window is populated with the information listed in a device's running configuration (obtained by entering the `sh run` command). As a result, if the default values for any of the available options are not provided in the running configuration, these values will not appear in the Cisco UBE gatekeeper configuration window.

Procedure

- Step 1** Select the VoIP view.
- Step 2** From the tree, right-click the Cisco UBE gatekeeper for which you want to configure options. A popup menu appears.
- Step 3** Select **Configure....** The Configuration for Cisco UBE Gatekeeper window appears with the **General** tab active.
- Step 4** Perform the desired action.

Field	Description	Action
ARQ Reject Unknown Prefix	Default is disabled. When a zone prefix match is not found, the default behavior is to attempt to use a local zone for the hop off (instead of failing the call). If enabled, an admission reject (ARJ) message is returned to the originating gateway and the call is routed through an alternate dial peer.	Select Enable or Disable.
ARQ Reject Resource Low	Default is disabled. If this is enabled, an ARJ message is returned to the originating gateway when destination resources are low.	Select Enable or Disable.

Field	Description	Action
ARQ Hopoff Zone	Forces the access Cisco UBE gatekeeper to send LRQ messages to remote zones or clusters to resolve the called number, even though the routing information for the called number is already known.	<p>Enter valid remote zones or clusters. Use the semicolon (;) as a delimiter when entering multiple values. The following are examples of valid values:</p> <ul style="list-style-type: none"> <i>zone1</i> <i>zone1;zone2;zone3</i> <p> Caution The values specified in this field are saved only after the previous values are deleted using the no arq hopoff command. Make sure you enter valid remote zones/clusters. Otherwise, the values previously set for this field will be discarded.</p>
LRQ Reject Unknown Prefix	Default is disabled. When a hop off zone is not found (that is, when a zone prefix is not matched), the default behavior is to attempt to service the request using a local zone. If enabled, a location reject (LRJ) is returned to the originating gateway.	Select Enable or Disable.
LRQ Reject Resource Low	Default is disabled. If this is enabled, a Cisco UBE gatekeeper notifies a sending Cisco UBE gatekeeper on receipt of an LRQ message that indicates no terminating endpoints are available.	Select Enable or Disable.
LRQ Reject Unknown Circuit	Default is disabled. If this is enabled, a Cisco UBE gatekeeper rejects an LRQ message that contains an unknown destination circuit.	Select Enable or Disable.
LRQ LRJ Immediate-Advance	Default is disabled. If this is enabled, a Cisco UBE gatekeeper sends a sequential LRQ message to the next zone immediately after it receives an LRJ message from a Cisco UBE gatekeeper in the current zone.	Select Enable or Disable.
LRQ Add Time-to-live	Default is disabled. If this is enabled, a Cisco UBE directory gatekeeper forwards LRQs to other Cisco UBE gatekeepers and returns the highest priority and lowest cost gateway information to the requesting endpoint.	Select Enable or Disable.
LRQ Hop Count	Specifies the maximum number of hops for LRQ forwarding among Cisco UBE directory gatekeepers in the Cisco UBE gatekeeper group.	Enter a valid maximum hop count (from 1 to 10).

Field	Description	Action
BandWidth Management	Determines amount of bandwidth allocated for total, interzone, per session, and remote maximum bandwidth usage for Cisco UBE gatekeeper.	<p>Enter bandwidth values.</p> <p>To enable a destination zone bandwidth check before responding to an ARQ message, select the Check Bandwidth check box.</p> <p>Note To allocate different values for individual local zones, see Adding a Local Zone, page 3-11.</p>
Extra Commands	Runs Cisco UBE gatekeeper commands that are not available through CWVM. Also lists Cisco UBE gatekeeper commands that are not supported by CWVM.	<p>Enter the CLI command. For example:</p> <pre>zone subnet gkName 172.20.118.1 255.255.255.0 enable</pre> <p>Note CWVM does not validate these commands.</p>

Step 5 Click **Finish**.

To configure local zones, remote zones, zone prefixes, and technology prefixes for a Cisco UBE gatekeeper, see the following topics:

- [Managing Local Zones, page 3-11](#)
- [Managing Remote Zones, page 3-13](#)
- [Managing Zone Prefixes, page 3-15](#)
- [Managing Technology Prefixes, page 3-18](#)

Interpreting Cisco UBE Gatekeeper Configuration Options

When you reconfigure a Cisco UBE gatekeeper or Cisco UBE directory gatekeeper, CWVM displays the following:

- A list of devices that will be unregistered—Select Yes or No to proceed with the operation.
- An option of whether or not you want to propagate any zone information changes—Select Yes or No. If you select Yes, the information is propagated only to other top level Cisco UBE gatekeepers.
- An option to schedule the operation—Select Schedule to have the operation perform at a later time, or select Do NOW to perform the operation immediately.

**Note**

When zones and zone prefixes are deleted, the Unregistered Devices window appears. This window shows a list of Cisco UBE gatekeepers or gateways (depending on whether a Cisco UBE directory gatekeeper or a Cisco UBE gatekeeper was configured) followed by a list of zones or zone prefixes that were deleted. Upon clicking Yes, you are given the option to propagate the zone information to top level Cisco UBE gatekeepers at a later scheduled time.

Managing Local Zones

Local zones are logical groups of gateways that are registered locally to a Cisco UBE gatekeeper.

See the following to configure a local zone:

- [Adding a Local Zone](#)
- [Modifying a Local Zone](#)
- [Deleting a Local Zone](#)

**Tip**

If you want to manage zones using only Cisco UBE gatekeepers (without using Cisco UBE directory gatekeepers), you can establish remote zones between Cisco UBE gatekeepers. All local zones for one Cisco UBE gatekeeper are represented by one remote zone in a remote Cisco UBE gatekeeper. All zone prefixes assigned to a Cisco UBE gatekeeper, regardless of what local zone they are in, are created under the same remote zone in a remote Cisco UBE gatekeeper. For example, if GatekeeperAA has two local zones (localZone1 and localZone2), then remote GatekeeperB creates remoteZoneAA that contains all zone prefixes belonging to localZone1 and localZone2.

Related Topics

- [Configuring a Cisco UBE Gatekeeper, page 3-8](#)
- [Managing Remote Zones, page 3-13](#)
- [Managing Zone Prefixes, page 3-15](#)
- [Managing Technology Prefixes, page 3-18](#)

Adding a Local Zone

Procedure

- Step 1** Select the VoIP view.
- Step 2** From the tree view, right-click the Cisco UBE gatekeeper to which you want to add a local zone. A popup menu appears.
- Step 3** Select **Configure...**. The Configuration for Cisco UBE Gatekeeper window appears.
- Step 4** Click the **Local Zones** tab.
- Step 5** Click the **Add** button.
- Step 6** Enter the following information:
 - Name of zone
 - Zone domain
 - IP address of Registration, Admission, and Status Protocol (RAS) port (CWVM detects the existing RAS IP address. If you want to change it to another interface IP address, select one from the drop-down list.)

**Note**

If you are configuring an HSRP backup Cisco UBE gatekeeper, then choose the RAS IP address as the standby IP address.

- Maximum bandwidth usage for this zone
- Interzone bandwidth usage
- Session bandwidth

Step 7 Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.

Related Topics

- [Managing Local Zones, page 3-11](#)
- [Modifying a Local Zone, page 3-12](#)
- [Deleting a Local Zone, page 3-12](#)

Modifying a Local Zone

Procedure

- Step 1** From the tree view, right-click the Cisco UBE gatekeeper that you want to modify. A popup menu appears.
- Step 2** Select **Configure....** The Configuration for Cisco UBE Gatekeeper window appears.
- Step 3** Click the **Local Zones** tab.
- Step 4** Select the local zone that you want modified and modify the information in each field.



Note Any modifications to the zone name will remove any previous prefixes associated with the zone.

Step 5 Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.

Related Topics

- [Managing Local Zones, page 3-11](#)
- [Adding a Local Zone, page 3-11](#)
- [Deleting a Local Zone, page 3-12](#)

Deleting a Local Zone

Before deleting a local zone, be sure its end points are not active and that the Cisco UBE gatekeeper is shut down.

Procedure

- Step 1** Select VoIP view.
- Step 2** From the tree view, right-click the Cisco UBE gatekeeper you want to modify. A popup menu appears.
- Step 3** Select **Configure....** The Configuration for Cisco UBE Gatekeeper window appears.

- Step 4** Click the **Local Zones** tab.
- Step 5** Select the local zone to be deleted.
- Step 6** Click the **Delete** button. If prompted, click **Yes** to confirm deletion.
- Step 7** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.

**Note**

Bring the Cisco UBE gatekeeper up again after this procedure is completed.

Related Topics

- [Managing Local Zones, page 3-11](#)
- [Adding a Local Zone, page 3-11](#)
- [Modifying a Local Zone, page 3-12](#)

Managing Remote Zones

Remote zones gateway groupings not registered locally to a Cisco UBE gatekeeper. For example, a dialed number is received through GatekeeperA. GatekeeperA checks to see if that number is registered locally (in its local zone). If not, the number is considered in a remote zone and forwarded to GatekeeperB, which has that number registered to its local zone.

Follow these procedures to manage remote zones:

- [Adding a Remote Zone, page 3-13](#)
- [Modifying a Remote Zone, page 3-14](#)
- [Deleting a Remote Zone, page 3-15](#)

Related Topics

- [Configuring a Cisco UBE Gatekeeper, page 3-8](#)
- [Managing Local Zones, page 3-11](#)
- [Managing Zone Prefixes, page 3-15](#)
- [Managing Technology Prefixes, page 3-18](#)

Adding a Remote Zone

Procedure

- Step 1** Select the VoIP view.
- Step 2** From the tree view, right-click the Cisco UBE gatekeeper you want to modify. A popup menu appears.
- Step 3** Select **Configure...**. The Configuration for Cisco UBE Gatekeeper window appears.
- Step 4** Click the **Remote Zones** tab.
- Step 5** Click **Add**.

- Step 6** Enter the following information:
- Name of zone
 - Zone domain
 - IP address and port number of RAS
 - Cost
 - Priority
 - ID of the circuit to be associated with the remote zone.
- Step 7** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.
-

Related Topics

- [Managing Remote Zones, page 3-13](#)
- [Modifying a Remote Zone, page 3-14](#)
- [Deleting a Remote Zone, page 3-15](#)

Modifying a Remote Zone

Procedure

-
- Step 1** Select VoIP view.
- Step 2** From the tree view, right-click the Cisco UBE gatekeeper that you want to modify. A popup menu appears.
- Step 3** Select **Configure....** The Configuration for Cisco UBE Gatekeeper window appears.
- Step 4** Click the **Remote Zones** tab.
- Step 5** Select the remote zone you want to modify, and modify the information in each field.



Note Any modifications to the zone name will remove any previous prefixes associated with the zone.

- Step 6** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.
-

Related Topics

- [Managing Remote Zones, page 3-13](#)
- [Adding a Remote Zone, page 3-13](#)
- [Deleting a Remote Zone, page 3-15](#)

Deleting a Remote Zone

Procedure

- Step 1** Select VoIP view.
- Step 2** From the tree view, right-click the Cisco UBE gatekeeper that you want to modify. A popup menu appears.
- Step 3** Select **Configure...**. The Configuration for Cisco UBE Gatekeeper window appears.
- Step 4** Click the **Remote Zones** tab
- Step 5** Select the remote zone you want to delete.
- Step 6** Click the **Delete** button. If prompted, click **Yes** to confirm deletion.
- Step 7** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.
-

Related Topics

- [Managing Remote Zones, page 3-13](#)
- [Adding a Remote Zone, page 3-13](#)
- [Modifying a Remote Zone, page 3-14](#)

Managing Zone Prefixes

Zone prefixes allow calls to be routed correctly and expediently. A zone prefix identifies the addresses to be serviced by a given Cisco UBE gatekeeper. Zone prefixes are typically area codes and serve the same purpose as the domain names in the H.323-ID address space.

See the following to configure zone prefixes:

- [Adding a Zone Prefix, page 3-15](#)
- [Assigning a Zone Prefix to a Local Zone, page 3-16](#)
- [Assigning a Zone Prefix to a Remote Zone, page 3-17](#)
- [Deleting a Zone Prefix, page 3-18](#)

Related Topics

- [Configuring a Cisco UBE Gatekeeper, page 3-8](#)
- [Managing Local Zones, page 3-11](#)
- [Managing Remote Zones, page 3-13](#)
- [Managing Technology Prefixes, page 3-18](#)

Adding a Zone Prefix

When you add a zone prefix to a child Cisco UBE gatekeeper or Cisco UBE directory gatekeeper, CWVM verifies the prefix and makes sure it is within the range that its parent Cisco UBE directory gatekeeper allows.

Procedure

- Step 1** Select the VoIP view.
 - Step 2** From the tree view, right-click the Cisco UBE gatekeeper you want to modify. A popup menu appears.
 - Step 3** Select **Configure....** The Configuration for Cisco UBE Gatekeeper window appears.
 - Step 4** Click the **Zone Prefixes** tab.
 - Step 5** Click the **Add** button.
 - Step 6** Enter a zone prefix.
 - Step 7** Select the Blast option, if applicable.
 - Step 8** Assign the newly added zone prefix to a local or remote zone. See [Assigning a Zone Prefix to a Local Zone, page 3-16](#) and [Assigning a Zone Prefix to a Remote Zone, page 3-17](#), for more details.
 - Step 9** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.
-

Related Topics

- [Managing Zone Prefixes, page 3-15](#)
- [Assigning a Zone Prefix to a Local Zone, page 3-16](#)
- [Assigning a Zone Prefix to a Remote Zone, page 3-17](#)
- [Deleting a Zone Prefix, page 3-18](#)

Assigning a Zone Prefix to a Local Zone

Procedure

- Step 1** Select the VoIP view.
 - Step 2** From the tree view, right-click the Cisco UBE gatekeeper for which you want to configure the zone prefix. A popup menu appears.
 - Step 3** Select **Configure....** The Configuration for Cisco UBE Gatekeeper window appears.
 - Step 4** Click the **Zone Prefixes** tab.
 - Step 5** Select the zone prefix you want to assign to a local zone.
 - Step 6** Click the **Local Zone** button. The Local Zone Selection window appears.
 - Step 7** Select and define options. See [Local Zone Selection Options, page 3-17](#), for more information.
 - Step 8** Click **OK**.
 - Step 9** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.
-

Related Topics

- [Managing Zone Prefixes, page 3-15](#)
- [Adding a Zone Prefix, page 3-15](#)

- [Assigning a Zone Prefix to a Remote Zone, page 3-17](#)
- [Deleting a Zone Prefix, page 3-18](#)

Local Zone Selection Options

The Local Zone Selection Options window appears when you assign a zone prefix to a local zone.

-
- Step 1** From the drop-down list of zones, select the local zone to which you want to assign the zone prefix.
- Step 2** Enter the default priority number if you want to assign a default priority to all gateways in this local zone.



Note This option is available only on certain Cisco IOS versions.

- Step 3** Click the **Add** button to enter additional priority to individual gateways.
- Step 4** Enter Priority number and gateway IDs.
- Step 5** Click **OK**. The Local Zone Selection options are applied.
-

Assigning a Zone Prefix to a Remote Zone

Procedure

- Step 1** Select the VoIP view.
- Step 2** From the tree view, right-click the Cisco UBE gatekeeper for which you want to configure the zone prefix. A popup menu appears.
- Step 3** Select **Configure...**. The Configuration for Cisco UBE Gatekeeper window appears.
- Step 4** Click the **Zone Prefixes** tab.
- Step 5** Select the zone prefix you want to assign to a remote zone.
- Step 6** Click the **Remote Zone** button. The Remote Zone Selection window appears.
- Step 7** From the list of remote zones available, use the left and right arrows to assign this prefix to a remote zone.
- Step 8** Click **OK**.
- Step 9** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.
-

Related Topics

- [Managing Zone Prefixes, page 3-15](#)
- [Adding a Zone Prefix, page 3-15](#)
- [Assigning a Zone Prefix to a Local Zone, page 3-16](#)
- [Deleting a Zone Prefix, page 3-18](#)

Deleting a Zone Prefix

Procedure

- Step 1** Select the VoIP view.
- Step 2** From the tree view, right-click the Cisco UBE gatekeeper for which you want to delete the zone prefix. A popup menu appears.
- Step 3** Select **Configure....** The Configuration for Cisco UBE Gatekeeper window appears.
- Step 4** Click the **Zone Prefixes** tab.
- Step 5** Select the zone prefix you want to delete.
- Step 6** Click the **Delete** button.
- Step 7** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.
-

Related Topics

- [Managing Zone Prefixes, page 3-15](#)
- [Adding a Zone Prefix, page 3-15](#)
- [Assigning a Zone Prefix to a Local Zone, page 3-16](#)
- [Assigning a Zone Prefix to a Remote Zone, page 3-17](#)

Managing Technology Prefixes

Technology prefixes determine the type of services a gateway can provide. These services include voice mail gateways, gateway priority assignment, and hop off options. For example, voice gateways may register with technology prefix “1xx,” H.320 gateways with “2xx,” voice mail gateways with “3xx,” and so on.

See the following topics to configure technology prefixes:

- [Adding a Technology Prefix, page 3-18](#)
- [Deleting a Technology Prefix, page 3-20](#)

Related Topics

- [Configuring a Cisco UBE Gatekeeper, page 3-8](#)
- [Managing Local Zones, page 3-11](#)
- [Managing Remote Zones, page 3-13](#)
- [Managing Zone Prefixes, page 3-15](#)

Adding a Technology Prefix

Procedure

- Step 1** Select the VoIP view.

- Step 2** From the tree view, right-click the Cisco UBE gatekeeper to which you want to add a technology prefix. A popup menu appears.
 - Step 3** Select **Configure...**. The Configuration for Cisco UBE Gatekeeper window appears.
 - Step 4** Click the **Tech Prefixes** tab.
 - Step 5** Click the **Add** button.
 - Step 6** Enter a technology prefix. You can enter up to 13 characters.
 - Step 7** Select the default option, if applicable. You can define a gw-type (for example, 1#*) to be used as default tech prefix. It is used if there is no technology prefix specified in the called number.
 - Step 8** Click the **Hop Off** button and define options, if applicable. See [Hop Off Zones, page 3-19](#).
 - Step 9** Click the **Gateways** button and define options. See [Gateway Selection, page 3-19](#).
 - Step 10** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.
-

Hop Off Zones

The Hop Off Zone window appears when you add or modify technology prefixes.

Procedure

- Step 1** Select either sequential or blast for the type of LRQ, if applicable.
 - Step 2** From the list of available local and remote zones, use the left and right arrows to choose which zones are assigned as hop off zones.
 - Step 3** Click **OK**. The Hop Off Zones window closes.
-

Related Topics

- [Managing Technology Prefixes, page 3-18](#)
- [Adding a Local Zone, page 3-11](#)

Gateway Selection

The Gateway Selection window appears when you add or modify technology prefixes. Use this procedure to assign technology prefixes to a gateway.

Procedure

- Step 1** Click **Add**.
- Step 2** Enter the Gateway IP address.



Note The gateway IP address you enter does not have to be a gateway that has been defined in CWVM.

- Step 3** Enter the port number (optional). If no port number is entered, CWVM adds it for you.
- Step 4** Click **OK**. The Gateway Selection window closes.
-

Use this procedure to remove technology prefixes from a gateway.

Procedure

- Step 1** Select the gateway for which you want to remove the technology prefix.
- Step 2** Click **Delete**.
- Step 3** Click **OK**. The technology prefix is no longer assigned to the gateway.
-

Related Topics

- [Managing Technology Prefixes, page 3-18](#)
- [Adding a Local Zone, page 3-11](#)

Deleting a Technology Prefix

Procedure

- Step 1** Select the VoIP view.
- Step 2** From the tree view, right-click the Cisco UBE gatekeeper to which you want to add a technology prefix. A popup menu appears.
- Step 3** Select **Configure....** The Configuration for Cisco UBE Gatekeeper window appears.
- Step 4** Click the **Tech Prefixes** tab.
- Step 5** Select the technology prefix you want to delete.
- Step 6** Click the **Delete** button.
- Step 7** Click **Finish**. If the Configuration Options window appears, see [Interpreting Cisco UBE Gatekeeper Configuration Options, page 3-10](#), for more information.
-

Verifying a Phone Number Under a Cisco UBE Gatekeeper

Procedure

- Step 1** Select the VoIP view.
- Step 2** From the tree view, right-click the Cisco UBE gatekeeper for which you want to verify a phone number. A popup menu appears.

- Step 3** Select **Verify Phone Number**. The Verify Phones Under Cisco UBE Gatekeeper window appears with prefix and gateway number verification.
-

Related Topics

- [Managing Technology Prefixes, page 3-18](#)
- [Adding a Technology Prefix, page 3-18](#)

Gateways

CWVM manages gateways enabled for combinations of VoIP and VoFR/VoATM networks. Groups must always be created to manage gateways in VoFR/VoATM networks because these networks do not use Cisco UBE gatekeepers. Groups must also be created in VoIP networks that contain gateways that are not managed by a Cisco UBE gatekeeper.

See the following topics for more information about working with gateways:

- [Preparing a Gateway for CWVM, page 3-21](#)
- [Adding a Gateway to a Cisco UBE Gatekeeper, page 3-23](#)
- [Adding a Gateway in CWVM, page 3-24](#)
- [Cloning Gateway Information, page 3-25](#)
- [Searching for a Gateway, page 3-25](#)
- [Modifying a Gateway, page 3-26](#)
- [Configuring SIP User Agent, page 3-27](#)
- [Monitoring DSP Status, page 3-31](#)
- [Viewing Gateway Resource Information, page 3-31](#)
- [Deleting a Gateway, page 3-32](#)
- [Moving a Gateway, page 3-32](#)
- [Saving a Running Configuration to NVRAM, page 3-33](#)
- [Backing up and Restoring Gateway Configuration, page 3-34](#)

Preparing a Gateway for CWVM

Before you can add a gateway to CWVM, Telnet and SNMP must be enabled on the router. Because Telnet is used to communicate with the gateway, Session Timeout must be configured to a nonzero value for all vty lines.

To enable SNMP:

```
Router(config)# snmp-server community public RW
```

To configure Enable or Secret Password:

```
Router(config)# enable password lab
```

Line password in the line configuration set to enable Telnet:

```
Router(config)# line vty 0 4
```

```
Router(config)# password lab
```

To configure Session Timeout for all vty lines:

```
Router# config term
Router(config)# line vty 0 4
Router(config-line)# session-timeout 10
```

When adding a gateway to CWVM, you must know the IP address or DNS name and any passwords the gateway has. CWVM searches the gateway, automatically detects the type of voice interfaces enabled on it, and places it in the appropriate views and in the All Gateways view.

**Note**

Because CWVM supports a wide variety of Cisco routers, only basic information about gateways is provided in this document. For detailed information about routers, refer to the documentation provided with your Cisco router.

Related Topic

- [Adding a Gateway to a Cisco UBE Gatekeeper, page 3-23](#)

Adding a Gateway to a Cisco UBE Gatekeeper

Before adding a gateway to a Cisco UBE gatekeeper (or moving a gateway to a new Cisco UBE gatekeeper) using CWVM, you must configure both devices through the CLI.



Caution

When you configure a gateway to be moved to a new Cisco UBE gatekeeper using the CLI, you must also move the gateway to the new Cisco UBE gatekeeper in CWVM (see [Moving a Gateway, page 3-32](#)). If you do not move the gateway to the new Cisco UBE gatekeeper within CWVM, any associated gateways in the originating Cisco UBE gatekeeper will propagate incorrect dial peer information to this gateway as well as receive incorrect dial peer information from the gateway. This might cause calls to be routed incorrectly.

In this example, the following parameters are assigned.

Parameter	Assignment
Gateway IP Address	172.20.118.12
Gateway Alias	gw12-sj
Cisco UBE Gatekeeper IP Address	172.20.118.7 1718
Cisco UBE Gatekeeper Port Number	1718
Cisco UBE Gatekeeper Alias	gk7-sj

The following is an example of how you would configure this gateway:

```
interface Ethernet0
! IP address of the gateway
ip address 172.20.118.12 255.255.255.192
! Identifies that this is a VoIP gateway
h323-gateway voip interface
! Defines name and location of Cisco UBE Gatekeeper
h323-gateway voip id gk7-sj ipaddr 172.20.118.7 1718
! Defines name and location of gateway
h323-gateway voip h323-id gw12-sj
! Enabling the gateway command
conf t
conf#gateway
conf-gateway#end
```

The following is an example of how you would configure the Cisco UBE gatekeeper for the previous gateway:

```
gatekeeper
! Create local zone - has gateway alias and domain name
zone local gk7-sj cisco.com
! Add prefix to Cisco UBE gatekeeper zone list and set priority to 10
zone prefix gk7-sj 408* gw-priority 10 gw12-sj
! Verify gateway
show gatekeeper zone status
```



Related Topic

- [Adding a Gateway in CWVM, page 3-24](#)

Adding a Gateway in CWVM

You can add a gateway to a group or Cisco UBE gatekeeper in CWVM. If you are adding a gateway to a Cisco UBE gatekeeper, you must configure both devices outside of CWVM first. See [Adding a Gateway to a Cisco UBE Gatekeeper, page 3-23](#), for more information. In VoFR/VoATM networks, you can add gateways to groups only. In VoIP networks, you add gateways to groups or Cisco UBE gatekeepers, depending on the network configuration. Verify that you have prepared the gateway before adding it in CWVM. See [Preparing a Gateway for CWVM, page 3-21](#), for more information.

Procedure

-
- Step 1** From the tree view, right-click the group or Cisco UBE gatekeeper to which you want to add the gateway. A popup menu appears.
- Step 2** Select **Add Gateway...** The Add Gateway window appears.
- Step 3** Enter the following values for the gateway:
- IP address or DNS name
 - Community string read and write
 - Login username
- Step 4** Enter the following passwords for the gateway:
- Login or Telnet
 - Enable
-  **Note** The device should have “>” at the end of a login prompt and “#” at the end of an enable prompt. For example: `router>` and `router#`.
-
- Step 5** Select **CWVM to Poll** if you want to have CWVM poll the router.
- Step 6** Select **Forward Traps to CWVM** if you want to have CWVM monitor traps on the gateway.
-  **Note** If you configure a gateway manually (outside of the CWVM application) to send traps to CWVM, CWVM may receive traps even if this option is not selected. However, CWVM will accept those traps only if the gateway has been added in CWVM.
-
- Step 7** Select the gateway time zone from the drop-down list.
- Step 8** Click **Finish**. The Add Gateway window appears.
- Step 9** Click **OK**. The Change Network Type window appears.
- Step 10** Select the types of voice-network dial peers with which you want to associate the gateway.
- Step 11** Read the information displayed about the gateway. If applicable, select whether you want to add the gateway to a group or Cisco UBE gatekeeper.
- Step 12** Click **OK** to add the device only as a Voice Gateway.
- Step 13** Click **Choose Capabilities**. The Choose VoIP Capabilities to Be Managed window appears.

- Step 14** Select the VoIP capabilities to be managed for this device.
- Step 15** Click **OK**. The Change Network Type window appears again. Click **OK** to complete the operation.



Note You can multiple gateways at one time by importing a batch add file. See [Batch Add Files, page 3-43](#).

Cloning Gateway Information

Cloning creates a copy of the selected gateway's passwords, community strings, terminals servers, poller and trap options, and login ID. After cloning a gateway, you need to change only the IP address or DNS name of the new gateway.

Procedure

- Step 1** From the tree view, right-click a group or Cisco UBE gatekeeper that contains the gateway you want to clone. A popup menu appears.
- Step 2** Select **Clone Gateway....** The Clone Gateway window appears.
- Step 3** In **Device Address**, enter the IP address of the new gateway.
- Step 4** Click **Finish**. The Add Gateway Completed window appears.
- Step 5** Click **OK**. The Change Network Type window appears.
- Step 6** Select the types of voice-network dial peers with which you want to associate the gateway.
- Step 7** Read the information displayed about the gateway. If applicable, select whether you want to add the gateway to a group or Cisco UBE gatekeeper.
- Step 8** Click **Choose Capabilities**. The Choose VoIP Capabilities to Be Managed window appears.
- Step 9** Select the VoIP capabilities to be managed for this device.
- Step 10** Click **OK**. The Change Network Type window appears again. Click **OK** to complete the operation.

Searching for a Gateway

When you have many gateways displayed in the tree, it can become difficult to find a specific gateway. CWVM enables you to locate a specific gateway easily.

Procedure

- Step 1** From the tree view, right-click the server (or network, if you are in the CWVM tree view). A popup menu appears.
- Step 2** Select **Search Gateway....** The Search Gateway window appears.

- Step 3** Enter the IP address of the gateway you need to locate:
- Click **VoIP** or **VoFR/ATM** to search your current tab view. The gateway is highlighted in the tree.
 - Click **All Gateways** to search the All Gateways tab view. The gateway is highlighted in the tree. If you started this procedure in the All Gateways view, only this button will be highlighted.
- Step 4** Click **Finish**. The Search Gateway window closes.
-

Modifying a Gateway

CWVM gives you the ability to change specific parameters on a gateway that you have added to CWVM.



Note

Because CWVM supports a wide variety of Cisco routers, only basic information about routers is provided in this document. For detailed information about routers, refer to the documentation provided with your Cisco router.

Procedure

- Step 1** From the tree view, right-click the gateway that you want to modify. A popup menu appears.
- Step 2** Select **Modify...**
- Step 3** Enter a new login username, if applicable.
- Step 4** Click **CWVM to Poll** to have CWVM poll the router.
- Step 5** Click **Forward Traps to CWVM** to have CWVM monitor traps on the router.



Note

If a gateway is configured outside of CWVM to send traps to CWVM, CWVM may receive traps even if this option is not selected. However, CWVM will accept those traps only if the gateway has been added to CWVM.

- Step 6** Click the types of traps you want to enabled.



Note

Call information type traps (dialCtlPeerCallInformation and dialCtlPeerCallSetup) are generated for each call. If CWVM is configured to receive these traps, you may experience severe performance issues on the CWVM server.

- Step 7** Set the poll interval.
- Step 8** Set the gateway time zone.
- Step 9** Click **Change Credentials** to modify community strings and the Enable and Telnet passwords.
- Enter the old community strings, Enable password, and Telnet password in the first field.
 - Enter the new community strings, Enable password, and Telnet password twice to confirm that you have typed them in correctly.
 - Click **OK**. The changes are captured in memory. They are not saved in the database until you click **OK**. If you click **Cancel**, only credential changes are canceled.



Note CWVM will change the credentials only in its database and not on the actual device.

- Step 10** Click **Change Network Type** to modify the network types found on the gateway. The Change Network Type window appears:
- Select the types of voice-network dial peers (VoIP, VoATM, or VoFR) with which you want to associate the gateway.
 - Read the information displayed about the gateway. If applicable, select whether you want to add the gateway to a group or Cisco UBE gatekeeper.
 - Click **OK** to save the network type changes. The Choose VoIP Capabilities to Be Managed window appears. If you click **Cancel**, only network type changes are canceled.
- Step 11** Click **Choose Capabilities** to modify the capabilities found on the gateway. The Choose VoIP Capabilities to Be Managed window appears:
- As applicable, select Voice Gateway, Cisco Communications Manager Express, or SRST Gateway capabilities. Note that CME and SRST options are enabled only if they are enabled on the device.
 - Click **OK** to save the capability changes. The Modify Gateway window reappears.
- Step 12** Click **Finish**. The gateway is modified.



Note If you changes both the credentials and network type and then click **Cancel**, only the network changes are canceled.

Configuring SIP User Agent

You must have SIP user agent configuration commands enabled on the device before configuring the device through CWVM. To do this, enter the sip-ua command using the CLI on the device.



Note CWVM supports SIP-enabled devices using Cisco IOS version 12.1.3t or later.

By design, the SIP user agent configuration window is populated with the information listed in a device's running configuration (obtained by entering the `sh run` command). As a result, if the default values for any of the available options are not provided in the running configuration, then these values will not appear in the SIP user agent configuration window.

Procedure

-
- Step 1** From the tree, right-click the gateway to configure. A popup menu appears.
- Step 2** Select **Configure SIP User Agent...** The Configure SIP User Agent window appears with the General tab active.
- Step 3** In the **Type** drop-down list, select the type of server interface:
- DNS—Sets the global SIP server interface to a DNS. An example of a DNS entry is mygateway.company.com.
 - IPv4—Sets the global SIP server interface to an IP address.

- Step 4** Enter IP address and port (SIP server port number), or DNS address.
- Step 5** Select which protocol SIP will listen for: tcp or udp.
- Step 6** Enter the maximum number of proxy or redirect servers that can forward a request through the gateway. This is also known as the maximum number of hops. You can enter any number from 1 through 70.
- Step 7** Enter any other SIP-related CLI commands that are not provided in this window.



Note CWVM will not validate these commands.

- Step 8** Select the **Retry Counters** tab.
- Step 9** Enter the number of times to retry attempts for the following SIP messages.

SIP Retry	Description	Possible Value (in milliseconds)	Default Value
Invite	Number of times an INVITE request is retransmitted.	1 - 10	6
Response	Number of times a RESPONSE request is retransmitted.	1 - 10	6
Bye	Number of times a BYE request is retransmitted.	1 - 10	10
Cancel	Number of times a CANCEL request is retransmitted.	1 - 10	10
Info	Number of information messages the gateway has received (inbound) and transmitted (outbound).	1 - 10	6
Refer	Number of times a REFER request is retransmitted.	1 - 10	10
Keepalive	Number of times a KEEPALIVE request is retransmitted.	1 - 10	6
Update	Number of times an UPDATE request is retransmitted.	1 - 10	10
Prack	Number of times a PRACK request is retransmitted.	1 - 10	10
Comet	Number of times a COMET request is retransmitted. Note Deprecated in Cisco IOS 12.4(2)T and later (grayed out).	1 - 10	10
Notify	Number of times a NOTIFY message is retransmitted.	1 - 10	10
Rel1xx	Number of times a Rel1xx request is retransmitted.	1 - 10	6
Register	Number of REGISTER requests received or sent.	1 - 10	10

SIP Retry	Description	Possible Value (in milliseconds)	Default Value
Subscribe	Number of SUBSCRIBE requests received or sent.	1 - 10	10
Options	Number of times an OPTIONS request is retransmitted.	1 - 10	10



Note If a value is not entered for any of these fields, then the default value for that field is configured in the gateway.

Step 10 Select the **Timer Counters** tab.

Step 11 Enter the number of milliseconds for the following SIP signaling timers.

SIP Timer	Description	Possible Value (in milliseconds)	Default Value
Trying	Length of time to wait before a TRYING message is retransmitted.	100 - 1000	500
Connect	Length of time to wait before a CONNECT message is retransmitted.	100 - 1000	500
Disconnect	Length of time to wait before a DISCONNECT message is retransmitted.	100 - 1000	500
Expire	Length of time to wait before an EXPIRES message is retransmitted.	60000 - 180000	180000
Info	Number of information messages the gateway has received (inbound) and transmitted (outbound).	100 - 1000	500
Refer	Length of time to wait before a RETRY request is retransmitted.	100 - 1000	500
Connection Aging	Length of time (in minutes) to wait before a TCP or UDP connection is aged out.	<ul style="list-style-type: none"> • 5 - 30 (minutes)—Cisco IOS 12.4(11)T • 5 - 1440 (minutes)—Cisco IOS 12.4(11)XW, 12.4(15)T1 	5
Keepalive Active	Rate at which to send KEEPALIVE message requests.	10 - 600	120
Options	Length of time to wait before an OPTIONS response is retransmitted.	100-1000	500
Prack	Length of time to wait before a PRACK acknowledgment is retransmitted.	100 - 1000	500

SIP Timer	Description	Possible Value (in milliseconds)	Default Value
Comet	Length of time to wait before a COMET message is retransmitted. Note Deprecated in Cisco IOS 12.4(2)T and later (grayed out).	100 - 1000	500
Notify	Length of time to wait before a NOTIFY response is retransmitted.	100 - 1000	500
Rel1xx	Length of time to wait before a Rel1xx response is retransmitted.	100 - 1000	500
Register	Length of time to wait before a REGISTER request is retransmitted.	100 - 1000	500
Hold	Length of time to wait before a BYE request is sent.	15 - 2880	0
Buffer-Invite	Length of time to wait before sending either of the following: <ul style="list-style-type: none"> The INVITE message and FACILITY message (if it has arrived). The INVITE message only (if the FACILITY message has not arrived). 	50 - 5000	—
Keepalive Down	Rate at which to send KEEPALIVE message requests after SIP servers fail to respond and the keepalive retry counter is exhausted.	1 - 120	30
Update	Length of time to wait before an UPDATE message is retransmitted.	100 - 1000	500



Note If a value is not entered for any of these fields, then the default value for that field is configured in the gateway.

Step 12 Click **Finish**. The gateway is configured.

Monitoring an Active Call

Procedure

- Step 1** From the tree view, right-click the gateway that you want to monitor. A popup menu appears.
- Step 2** Select **Monitor > Active Calls...** The active calls for the gateway appear in the Active Calls window.

Column Name	Description
Incoming Call Leg Address	Incoming calling number or telephony IP address of remote voice gateway
Outgoing Call Leg Address	Outgoing calling number or telephony IP address of remote voice gateway
Duration	Duration of call
State	<ul style="list-style-type: none"> Connecting—Call is being set up Active—Call is active

- Step 3** Click **Refresh** to see current status.
- Step 4** Enter the time interval in which you want the screen to refresh.
- Step 5** Click **Finish**. The Active Calls window closes.

Monitoring DSP Status

Procedure

- Step 1** From the tree view, right-click the gateway that has DSP enabled. A popup menu appears.
- Step 2** Select **Monitor > DSP Status....** DSP status information appears in the Active Calls window. The types of card information displayed include:
- Index
 - Type
 - Description
 - Serial number
 - Hardware and software version
 - Resource and Hiwater utilization
 - Status
 - Last reset time
- Step 3** Click **Finish**.



Note

If your device has a voice interface card that is supported by the NM-1V, NM-2V, or NM-HDA network modules, the information provided in this dialog box may not be available.

Viewing Gateway Resource Information

You can see current CPU and memory usage, as well as the total number of active call legs in progress.

Procedure

-
- Step 1** From the tree view, right-click the gateway that you want to monitor. A popup menu appears.
 - Step 2** Select **Monitor > Resource Info...** Gateway status information appears in the Router Statistics window.
 - Step 3** Click **Finish**.
-

Deleting a Gateway

You can delete a gateway from CWVM at any time, in any view. You can delete a gateway from a specific view only while viewing it in the VoIP or VoFR/ATM views. You cannot delete a gateway from the All Gateways view without also deleting it from CWVM. To delete a gateway, you can use either of the following procedures.

Procedure A: All Gateways View

-
- Step 1** In the All Gateway view, right-click the gateway that you want to delete. A popup menu appears.
 - Step 2** Select **Delete**. The Select an Option window appears, asking you to confirm that you want to delete the gateway from the VoIP view and from CWVM.
 - Step 3** Make your selection.
 - Step 4** Click **OK** to confirm that you want to delete the gateway from VoIP view or CWVM.
-

Procedure B: VoIP and VoFR/ATM Views

-
- Step 1** In the VoIP or VoFR/ATM views, right-click the gateway that you want to delete. A popup menu appears.
 - Step 2** Select **Delete**. The Delete Router window appears.
 - Step 3** Click **Delete only from this view** or **Delete from the system**.
If the gateway you are deleting was displayed in the All subtab under the VoIP view, the Delete Router window displays the options **Delete only from VoIP view** or **Delete from the system**. Clicking **Delete only from VoIP view** will delete the gateway from all subtabs in the VoIP view.
 - Step 4** Click **OK** to confirm the deletion of the Gateway from the view or from CWVM.
-

Moving a Gateway

You can drag and drop gateways between networks under a single CWVM server. Gateways are updated only in the selected network view. For example, if you are in the VoIP view, and you move a gateway to another network, the VoATM/FR view does not show the gateway under the new network. You should later select the VoATM/FR view and then move the same gateway to the new network, so that the same information is displayed in both network views.

**Caution**

When you use the CLI to configure a gateway to be moved to a new Cisco UBE gatekeeper, you must also move the gateway to the new Cisco UBE gatekeeper in CWVM. If you do not move the gateway to the new Cisco UBE gatekeeper within CWVM, any associated gateways in the originating Cisco UBE gatekeeper will propagate incorrect dial peer information to this gateway as well as receive incorrect dial peer information from the gateway. This could cause calls to be routed incorrectly.

The behavior of moving gateways is as follows:

- Between groups—Dial-peer information from the gateway you are moving is not automatically propagated to the other gateways in the new group. Also, dial-peer information for gateways in the old group is not deleted from the gateway.
- From a group to a Cisco UBE gatekeeper—The zone on the gateway being moved must be valid for the new Cisco UBE gatekeeper. If the zone is not valid, you must create the zone on the new Cisco UBE gatekeeper before moving the gateway. Also, if the telephone numbers on a gateway are not within the prefix range for the zone, then the gateway cannot register those phone numbers with the Cisco UBE gatekeeper, and the phone numbers can be accessed only by explicit dial peers on other gateways.
- From one Cisco UBE gatekeeper to another Cisco UBE gatekeeper—Before moving a gateway to another Cisco UBE gatekeeper within CWVM, you must configure the gateway to be registered with the new Cisco UBE gatekeeper (see [Adding a Gateway to a Cisco UBE Gatekeeper, page 3-23](#), for instructions on how to do this). Also, make sure the zone prefix range in the new Cisco UBE gatekeeper covers the gateway's telephone numbers. If the zone prefix does not cover the gateway's telephone numbers, the gateway cannot register those phone numbers with the Cisco UBE gatekeeper, and the phone numbers can be accessed only by explicit dial peers on other gateways.

**Note**

CWVM does not prevent you from moving the gateway to the new Cisco UBE gatekeeper even if the gateway's phone numbers are not fully covered in the new Cisco UBE gatekeeper. See [Configuring a Cisco UBE Gatekeeper, page 3-8](#), for information on how to add new zones and zone prefixes after the move.

- From a Cisco UBE gatekeeper to a group—Dial-peer information on the gateway is not automatically propagated to the other gateways in the group.

Saving a Running Configuration to NVRAM

You can use CWVM to save the running configuration of a device to its NVRAM (startup configuration).

**Note**

For detailed information about configuring routers, refer to the documentation provided with your Cisco router.

Procedure

- Step 1** From the tree, right-click a gateway. A popup menu appears.
- Step 2** Select **Save NVRAM**.

Step 3 Click **Yes** to confirm. The running configuration of the device is saved to NVRAM.

Backing up and Restoring Gateway Configuration

Procedure

- Step 1** From the tree, right-click a gateway. A popup menu appears.
- Step 2** Select **Configuration Management**. The Configuration Management window appears.
- Step 3** To back up a configuration, click **Backup**. To restore a configuration, click **Restore**.
- Step 4** Enter the hostname where the configuration file resides.



Note CWVM uses TFTP to perform backup or restore. Make sure that TFTP is running on the host and that the TFTP boot directory has required read/write permissions.

- Step 5** Enter the directory where the configuration file resides.
- Step 6** Enter the name of the configuration file.
- Step 7** Select the configuration type that you want to back up or restore.
- Step 8** Click **Finish**.
-

CME Routers

CWVM manages voice routers with Cisco Communications Manager Express (CME) capabilities.

The following topics explain how to work with CME routers:

- [Preparing a CME for CWVM, page 3-34](#)
- [Adding a CME in CWVM, page 3-35](#)
- [Cloning CME Information, page 3-36](#)
- [Searching for a CME, page 3-37](#)
- [Searching for a CME, page 3-37](#)
- [Modifying a CME, page 3-37](#)
- [Deleting a CME, page 3-38](#)

Preparing a CME for CWVM

Before you can add a voice router with CME capabilities, you must ensure that CME mode is active and configured. To use the CME setup tool and enable CME on the router:

```
Router(config)# telephony-service setup
```

Because Telnet is used to communicate with the router, Session Timeout must be configured to a nonzero value for all vty lines. To configure the router Enable or Enable Secret password:

```
Router(config)# enable password lab
```

Use the line password in the line configuration set to enable Telnet:

```
Router(config)# line vty 0 4
Router(config)# password lab
```

To configure Session Timeout for all vty lines:

```
Router# config term
Router(config)# line vty 0 4
Router(config-line)# session-timeout 10
```

When adding a CME device to CWVM, you must know the IP address or DNS name and any passwords the CME has. CWVM searches the CME, automatically detects the type of interfaces enabled on it, and places it in the appropriate view.


Related Topic

- [Adding a CME in CWVM, page 3-35](#)

Adding a CME in CWVM

You can add a CME router in CWVM. Before doing so, verify that you have prepared the router properly. See [Preparing a CME for CWVM, page 3-34](#), for more information.

Procedure

-
- Step 1** From the tree view under the VoIP/CME tab, right-click the group or gateway to which you want to add the CME device. A popup menu appears.
- Step 2** Select **Add CME...** The Add a CME window appears.
- Step 3** Enter the following values for the gateway:
- IP address or DNS name
 - Community string read
 - Community string write
 - Login username
- Step 4** Enter the following passwords for the gateway:
- Logon or Telnet
 - Enable
-  **Note** The device should have “>” at the end of a login prompt and “#” at the end of an enable prompt. For example: `router>` and `router#`.
-
- Step 5** Select **CWVM to Poll** if you want to have CWVM poll the router.
- Step 6** Select **Forward Traps to CWVM** if you want to have CWVM monitor traps on the CME router.



Note If a CME router is manually configured (outside of the CWVM application) to send traps to CWVM, CWVM may receive traps even if this option is not selected. However, CWVM will accept those traps only if the router has been added in CWVM.

- Step 7** Select the gateway time zone from the drop-down list.
- Step 8** Click **Finish**. The Add CME Completed window appears.
- Step 9** Click **OK**. The Change Network Type window appears.
- Step 10** Select the types of voice-network dial peers with which you want to associate the CME.
- Step 11** Read the information displayed about the CME router. If applicable, select whether you want to add the router to a group or gateway.
- Step 12** Click **Choose Capabilities**. The Choose VoIP Capabilities to Be Managed window appears.
- Step 13** Select the VoIP capabilities to be managed for this device.
- Step 14** Click **OK**. The Change Network Type window appears again. Click **OK** to complete the operation.



Note You can add multiple CMEs at one time by importing a batch add file. See [Batch Add Files, page 3-43](#).

Cloning CME Information

Cloning creates a copy of the selected CME router's passwords, community strings, terminal servers, poller and trap options, and login ID. After cloning a CME, you need to change only the IP address or DNS name of the new CME.

Procedure

-
- Step 1** From the tree view under the VoIP/CME tab, right-click the CME you want to clone. A popup menu appears.
 - Step 2** Select **Clone CME...**. The Clone a CME window appears.
 - Step 3** In **Device Address**, enter the IP address of the new CME router.
 - Step 4** Click **Finish**. The Add a CME Completed window appears.
 - Step 5** Click **OK**. The Change Network Type window appears.
 - Step 6** Select the types of voice-network dial peers with which you want to associate the CME.
 - Step 7** Read the information displayed about the CME. If applicable, select whether you want to add the CME to a group or gateway.
 - Step 8** Click **Choose Capabilities**. The Choose VoIP Capabilities to Be Managed window appears.
 - Step 9** Select the VoIP capabilities to be managed for this device.
 - Step 10** Click **OK**. The Change Network Type window appears again. Click **OK** to complete the operation.
-

Searching for a CME

If you have many CMEs displayed in the tree, it can become difficult to find a specific CME. CWVM enables you to locate a specific CME easily.

Procedure

-
- Step 1** From the tree view under the VoIP/CME tab, right-click the CWVM server. A popup menu appears.
- Step 2** Select **Search CME...**. The Search CME window appears.
- Step 3** Enter the IP address of the CME you need to locate:
- Click **CME** to search your current tab view. The CME is highlighted in the tree.
 - Click **All Gateways** to search the All Gateways tab view. The CME is highlighted in the tree. If you started this procedure in the All Gateways view, only this button will be highlighted.
- Step 4** Click **Finish**. The Search CME window closes.
-

Modifying a CME

CWVM gives you the ability to change specific parameters on a CME that you have added to CWVM.



Note

Because CWVM supports a wide variety of Cisco routers, only basic information about routers is provided in this document. For detailed information about routers, refer to the documentation provided with your Cisco router.

Procedure

-
- Step 1** From the tree view under the VoIP/CME tab, right-click the CME that you want to modify. A popup menu appears.
- Step 2** Select **Modify...**
- Step 3** Enter a new login username, if applicable.
- Step 4** Click **CWVM to Poll** to have CWVM poll the router.
- Step 5** Click **Forward Traps to CWVM** to have CWVM monitor traps on the router.



Note

If you configure a CME outside of CWVM to send traps to CWVM, CWVM may receive traps even if this option is not selected. However, CWVM will accept those traps only if you add the CME to CWVM.

- Step 6** Click the types of traps you want to enable.



Note

Call information type traps (dialCtlPeerCallInformation and dialCtlPeerCallSetup) are generated for each call. If CWVM is configured to receive these traps, you may experience severe performance issues on the CWVM server.

- Step 7** Set the poll interval.
- Step 8** Set the gateway time zone.
- Step 9** Click **Change Credentials** to modify community strings and the Enable and Telnet passwords.
- Enter the old community strings, Enable password, and Telnet password in the first field.
 - Enter the new community strings, Enable password, and Telnet password twice to confirm that you have typed them in correctly.
 - Click **OK**. The changes are captured in memory. They are not saved in the database until you click **OK**. If you click **Cancel**, only credential changes are canceled.



Note CWVM will change the credentials only in its database and not on the actual device.

- Step 10** Click **Change Network Type** to modify the network types found on the CME. The Change Network Type window appears:
- Select the types of voice-network dial peers (VoIP, VoATM, or VoFR) with which you want to associate the CME.
 - Read the information displayed about the CME. If applicable, select whether you want to add the CME to a group or gateway.
 - Click **OK** to save the network type changes. The Choose VoIP Capabilities to Be Managed window appears. If you click **Cancel**, only network type changes are canceled.
- Step 11** Click **Choose Capabilities** to modify the capabilities to be monitored on the CME. The Choose VoIP Capabilities to Be Managed window appears:
- As applicable, select Voice Gateway or Cisco Communications Manager Express capabilities.
 - Click **OK** to save the capability changes. The Modify CME window reappears.
- Step 12** Click **Finish**. The CME is modified.



Note If you make changes to both the credentials and network type and then click **Cancel**, only the network changes are canceled.

Deleting a CME

You can delete a CME from CWVM or from a selected tab view only.

Procedure

- Step 1** From the VoIP/CME view, right-click the CME that you want to delete. A popup menu appears.
 - Step 2** Select **Delete**. The Delete Router window appears.
 - Step 3** Click **Delete only from this view** or **Delete from the system**.
 - Step 4** Click **OK** to confirm the deletion of the CME from the view or from CWVM.
-

SRST Routers

CWVM manages voice routers with Survivable Remote Site Telephony (SRST) capabilities.

The following topics explain how to work with SRST routers:

- [Preparing an SRST for CWVM, page 3-39](#)
- [Adding an SRST in CWVM, page 3-39](#)
- [Cloning SRST Information, page 3-40](#)
- [Searching for an SRST, page 3-41](#)
- [Modifying an SRST, page 3-41](#)
- [Deleting an SRST, page 3-43](#)

Preparing an SRST for CWVM

Before you can add a voice router with SRST capabilities, you must ensure that SRST mode is active and configured. To use the SRST setup tool and enable SRST on the router:

```
Router(config)# call-manager-fallback
```

Because Telnet is used to communicate with the router, Session Timeout must be configured to a nonzero value for all vty lines. To configure the router Enable or Enable Secret password:

```
Router(config)# enable password lab
```

Use the line password in the line configuration set to enable Telnet:

```
Router(config)# line vty 0 4
Router(config)# password lab
```

To configure Session Timeout for all vty lines:

```
Router# config term
Router(config)# line vty 0 4
Router(config-line)# session-timeout 10
```

When adding an SRST device to CWVM, you must know the IP address or DNS name and any passwords the SRST has. CWVM searches the SRST device, automatically detects the type of interfaces enabled on it, and places it in the appropriate view.

Related Topic

- [Adding an SRST in CWVM, page 3-39](#)

Adding an SRST in CWVM

You can add an SRST router in CWVM. Before doing so, verify that you have prepared the router properly. See [Preparing an SRST for CWVM, page 3-39](#), for more information.

Procedure

-
- Step 1** From the tree view under the VoIP/SRST tab, right-click the group or gateway in the tree view to which you want to add the SRST device. A popup menu appears.

Step 2 Select **Add SRST...** The Add an SRST window appears.

Step 3 Enter the following values for the router:

- IP address or DNS name
- Community string read
- Community string write
- Login username

Step 4 Enter the following passwords for the router:

- Logon or Telnet
- Enable



Note The device should have “>” at the end of a login prompt and “#” at the end of an enable prompt. For example: `router>` and `router#`.

Step 5 Select **CWVM to Poll** if you want to have CWVM poll the router.

Step 6 Select **Forward Traps to CWVM** if you want to have CWVM monitor traps on the SRST router.



Note If an SRST router is manually configured (outside of the CWVM application) to send traps to CWVM, CWVM may receive traps even if this option is not selected. However, CWVM will accept those traps only if the router has been added in CWVM.

Step 7 Select the gateway time zone from the drop-down list.

Step 8 Click **Finish**. The Add SRST Completed window appears.

Step 9 Click **OK**. The Change Network Type window appears.

Step 10 Select the types of voice-network dial peers with which you want to associate the SRST.

Step 11 Read the information displayed about the SRST router. If applicable, select whether you want to add the router to a group or gateway.

Step 12 Click **Choose Capabilities**. The Choose VoIP Capabilities to Be Managed window appears.

Step 13 Select the VoIP capabilities to be managed for this device.

Step 14 Click **OK**. The Change Network Type window appears again. Click **OK** to complete the operation.



Note You can add multiple SRSTs at one time by importing a batch add file. See [Batch Add Files, page 3-43](#).

Cloning SRST Information

Cloning creates a copy of the selected SRST router’s passwords, community strings, terminals servers, poller and trap options, and login ID. After cloning an SRST, you need to change only the IP address or DNS name of the new SRST.

Procedure

- Step 1** From the tree view under the VoIP/SRST tab, right-click the SRST you want to clone. A popup menu appears.
 - Step 2** Select **Clone SRST...** The Clone an SRST window appears.
 - Step 3** In **Device Address**, enter the IP address of the new SRST router.
 - Step 4** Click **Finish**. The Add an SRST Completed window appears.
 - Step 5** Click **OK**. The Change Network Type window appears.
 - Step 6** Select the types of voice-network dial peers with which you want to associate the SRST.
 - Step 7** Read the information displayed about the SRST. If applicable, select whether you want to add the SRST to a group or gateway.
 - Step 8** Click **Choose Capabilities**. The Choose VoIP Capabilities to Be Managed window appears.
 - Step 9** Select the VoIP capabilities to be managed for this device.
 - Step 10** Click **OK**. The Change Network Type window appears again. Click **OK** to complete the operation.
-

Searching for an SRST

If you have many SRSTs displayed in the tree, it can become difficult to find a specific SRST. CWVM enables you to locate a specific SRST easily.

Procedure

- Step 1** From the tree view under the VoIP/SRST tab, right-click the CWVM server. A popup menu appears.
 - Step 2** Select **Search SRST...** The Search SRST window appears.
 - Step 3** Enter the IP address of the SRST you need to locate:
 - a. Click **SRST** to search your current tab view. The SRST is highlighted in the tree.
 - b. Click **All Gateways** to search the All Gateways tab view. The SRST is highlighted in the tree. If you started this procedure in the All Gateways view, only this button will be highlighted.
 - Step 4** Click **Finish**. The Search SRST window closes.
-

Modifying an SRST

CWVM gives you the ability to change specific parameters on an SRST that you have added to CWVM.



Note

Because CWVM supports a wide variety of Cisco routers, only basic information about routers is provided in this document. For detailed information about routers, refer to the documentation provided with your Cisco router.

Procedure

-
- Step 1** From the tree view under the VoIP/SRST tab, right-click the SRST that you want to modify. A popup menu appears.
- Step 2** Select **Modify...**
- Step 3** Enter a new login username, if applicable.
- Step 4** Click **CWVM to Poll** to have CWVM poll the router.
- Step 5** Click **Forward Traps to CWVM** to have CWVM monitor traps on the router.



Note If an SRST is configured outside of CWVM to send traps to CWVM, CWVM may receive traps even if this option is not selected. However, CWVM will accept those traps only if the SRST has been added to CWVM.

- Step 6** Click the types of traps you want to enable.



Note Call information type traps (dialCtlPeerCallInformation and dialCtlPeerCallSetup) are generated for each call. If CWVM is configured to receive these traps, you may experience severe performance issues on the CWVM server.

- Step 7** Set the poll interval.
- Step 8** Set the gateway time zone.
- Step 9** Click **Change Credentials** to modify community strings and the Enable and Telnet passwords.
- Enter the old community strings, Enable password, and Telnet password in the first field.
 - Enter the new community strings, Enable password, and Telnet password twice to confirm that you have typed them in correctly.
 - Click **OK**. The changes are captured in memory. They are not saved in the database until you click **OK**. If you click **Cancel**, only credential changes are canceled.



Note CWVM will change the credentials only in its database and not on the actual device.

- Step 10** Click **Change Network Type** to modify the network types found on the SRST. The Change Network Type window appears:
- Select the types of voice-network dial peers (VoIP, VoATM, or VoFR) with which you want to associate the SRST.
 - Read the information displayed about the SRST. If applicable, select whether you want to add the SRST to a group or gateway.
 - Click **OK** to save the network type changes. The Choose VoIP Capabilities to Be Managed window appears. If you click **Cancel**, only network type changes are canceled.

- Step 11** Click **Choose Capabilities** to modify the capabilities to be monitored on the SRST. The Choose VoIP Capabilities to Be Managed window appears:
- As applicable, select Voice Gateway or SRST Gateway.
 - Click **OK** to save the capability changes. The Modify SRST window reappears.
- Step 12** Click **Finish**. The SRST is modified.



Note If you make changes to both the credentials and network type and then click **Cancel**, only the network changes are canceled.

Deleting an SRST

You can delete an SRST from CWVM or from a selected tab view only.

Procedure

- Step 1** From the VoIP/SRST view, right-click the SRST that you want to delete. A popup menu appears.
- Step 2** Select **Delete**. The Delete Router window appears.
- Step 3** Click **Delete only from this view** or **Delete from the system**.
- Step 4** Click **OK** to confirm the deletion of the SRST from the view or from the CWVM.

Batch Add Files

You can use batch add files to add multiple groups, Cisco UBE gatekeepers, and devices at one time. For more information on using batch add files, see the following topics:

- [Creating a Batch Add File, page 3-43](#)
- [Importing a Batch Add File, page 3-45](#)

Creating a Batch Add File

You can use a batch file to add multiple groups, Cisco UBE gatekeepers, and devices, to CWVM at one time. To do so, create a text file containing a text entry line for each group, Cisco UBE gatekeeper, or device you want to add. Each line must appear under one of the block labels shown in [Example 3-1](#), as appropriate for the item you are adding, and must be formatted using the corresponding line format. Thus, for each:

- Group, you must create a line under the `[group]` block.
- Cisco UBE directory gatekeeper, you must create a line under the `[directorygatekeeper]` block.
- Cisco UBE gatekeeper, you must create a line under the `[gatekeeper]` block.

- Device of any other type, such as a VoIP (including all voice gateways and CME- or SRST-enabled routers), VoFR, or VoATM device, you must create a line under the [router] block.

**Note**

To ensure that CWVM can import the batch file, create the file with the correct permissions:

- On Solaris—root permission or casuser permission
- On Windows—full permission or casuser permission

Example 3-1 Batch Add Blocks and Line Formats

```
[group]
GroupName, NetworkName, Description (optional)

[directorygatekeeper]
DeviceAddress, NetworkName, DirectoryGatekeeper (At least one of NetworkName or
DirectoryGatekeeper is mandatory), SNMPReadCommunity, SNMPWriteCommunity (optional),
LoginUser (optional), Password (optional), EnablePassword (optional),
IPAddressOfHSRPPBackup (optional), TechPrefixes (optional, multiple colon separated)

[gatekeeper]
DeviceAddress, NetworkName, DirectoryGatekeeper (At least one of NetworkName or
DirectoryGatekeeper is mandatory), SNMPReadCommunity, SNMPWriteCommunity (optional),
LoginUser (optional), Password (optional), EnablePassword (optional),
IPAddressOfHSRPPBackup (optional)

[router]
DeviceAddress, GroupName, GatekeeperDeviceAddress (At least one of GroupName or
GatekeeperDeviceAddress is mandatory), SNMPReadCommunity, SNMPWriteCommunity (optional),
LoginUser (optional), Password (optional), EnablePassword (optional), TrapFlag (optional,
y|any), PollFlag (optional, y|any)
```

To skip optional parameters, replace them with commas. For example `dgk1, net1, ,public, ,user,passwd, , ,1#:2#` would be a correctly formatted Cisco UBE directory gatekeeper entry line with the optional `DirectoryGatekeeper`, `SNMPReadCommunity`, `EnablePassword`, and `IPAddressOfHSRPPBackup` parameters skipped.

Example 3-2 shows a properly formatted batch add text file. Note that the block labels can appear in any order. For readability, create only one label of each type in the file, and put lines for all items of that type under that block label.

Example 3-2 A Typical Batch Add File

```
[group]
Group1,Default
Group2,Default

[router]
172.20.118.4,Group1, ,public,private,CWVM,cisco,cisco,y,n
172.19.50.70,Group1, ,public,private,CWVM,cisco,cisco,n,y
172.20.118.8,Group2, ,public,private,CWVM,cisco,cisco,y,n
172.20.118.9,Group2, ,public,private,CWVM,cisco,cisco,n,y
172.20.118.10,Group2, ,public,private,CWVM,cisco,cisco,n,n
```

```
[gatekeeper]
172.20.118.5,Default,,public,private,CWVM,cisco,cisco
172.19.50.76,Default,,public,private,CWVM,cisco,cisco
172.20.118.15,Default,,public,private,CWVM,cisco,cisco
172.19.50.68,Default,,public,private,CWVM,cisco,cisco
```

Related Topic

- [Importing a Batch Add File, page 3-45](#)

Importing a Batch Add File

You can add multiple groups, gateways, and devices, at one time by importing a text file. When adding a group, Cisco UBE gatekeeper, or Cisco UBE directory gatekeeper, you must have read/write access to that network. Any router with CME or SRST capabilities will be added to the proper view automatically if you have properly configured CME or SRST mode on the device beforehand.

**Note**

You must create a batch add file on the CWVM server machine before you can perform this task.

Procedure

-
- Step 1** From the tree view, right-click the CWVM server to which you want to add groups or gateways. A popup menu appears.
- Step 2** Select **Server > Batch Add...** The Batch Add window appears.
- Step 3** Enter the server location and filename of the batch add file; for example:
c:devices.dat
- Step 4** Click **OK**.
The devices and groups are scheduled to be added in the next minute.
-

Related Topic

- [Creating a Batch Add File, page 3-43](#)

Synchronizing Devices

The **sync device** command updates device information in CWVM to reflect changes you make to the voice port or dial plan on a device through the CLI. You can synchronize gateways, Cisco UBE gatekeepers, and CME or SRST devices.

When you manually change a gateway or Cisco UBE gatekeeper, you must synchronize the gateway or Cisco UBE gatekeeper to update CWVM. You can also manually synchronize devices if you do not want to wait for the next scheduled synchronization.

Procedure

-
- Step 1** From the tree, right-click a gateway or Cisco UBE gatekeeper. A popup menu appears.
- Step 2** Select **Sync with Device**.
- Step 3** Click **Yes**. The device is updated in CWVM, and the CWVM status window displays messages about the synchronization.

Whenever CWVM discovers new, unmanaged VoIP capabilities on a device, or discovers that a previously enabled capability has been removed, it displays information about these new or removed capabilities along with synchronization messages in the CWVM status window.

Automating Tasks

With CWVM, you can schedule certain tasks to execute at a time and date that you specify. Task scheduling is a method to execute network-intensive tasks at off-peak hours.

For more information on task automation, see the following topics:

- [Scheduling a Task, page 3-46](#)
- [Rescheduling a Task, page 3-47](#)
- [Viewing a Scheduled Task, page 3-47](#)
- [Deleting a Scheduled Task, page 3-47](#)

Scheduling a Task

The Schedule Operation window prompts you when you are doing various CWVM tasks that you may want to schedule at a later time. You can use task scheduling to execute network-intensive tasks at off-peak hours.

Procedure

-
- Step 1** When the Schedule Operation window appears, select one of the following:
- **Do NOW**—Runs the operation now.
 - **Schedule**—Allows you to schedule the operation at a later time.
- Step 2** If you selected **Schedule...**, enter the date and time you want the operation to run.
- Step 3** Click **Finish**. The task executes on the date and time specified.
-

Related Topics

- [Viewing a Scheduled Task, page 3-47](#)
- [Rescheduling a Task, page 3-47](#)
- [Deleting a Scheduled Task, page 3-47](#)

Rescheduling a Task

Procedure

- Step 1** From the tree, right-click a CWVM server. The Task Management window appears.
- Step 2** Select the task you want to reschedule. The task is highlighted in the Task Management window.
- Step 3** Click **Reschedule**.
- Step 4** Specify a date and time.
- Step 5** Click **Finish**. The task executes on the date and time specified.
-

Related Topics

- [Scheduling a Task, page 3-46](#)
- [Viewing a Scheduled Task, page 3-47](#)
- [Deleting a Scheduled Task, page 3-47](#)

Viewing a Scheduled Task

Procedure

- Step 1** From the tree, right-click a CWVM server. The Task Management window appears.
- Step 2** Select the task you want to delete. The task is highlighted in the Task Management window.
- Step 3** Click **View Details**.
- Step 4** Click **OK** to confirm the operation.
-

Related Topics

- [Scheduling a Task, page 3-46](#)
- [Rescheduling a Task, page 3-47](#)
- [Deleting a Scheduled Task, page 3-47](#)

Deleting a Scheduled Task

You can delete only scheduled tasks. You cannot delete tasks that are running.

Procedure

- Step 1** From the tree, right-click a CWVM server. The Task Management window appears.
- Step 2** Select the task you want to delete. The task is highlighted in the Task Management window.
- Step 3** Click **Delete**.

Step 4 Click **OK** to confirm the operation. The task is removed from the Task Management window.

Related Topics

- [Scheduling a Task, page 3-46](#)
- [Viewing a Scheduled Task, page 3-47](#)
- [Rescheduling a Task, page 3-47](#)