Conference Bridge Setup

This chapter provides information to configure conference bridges using Cisco Unified Communications Manager Administration.

See the following for additional information:

- Conference bridges and trusted relay points in the *Cisco Unified Communications Manager System Guide*
- Configuring Secure Conference Bridge in Cisco Unified Communications Manager Administration, *Cisco Unified Communications Manager Features and Services Guide*.
- Configuring Secure Conference Bridge in Cisco Unified Communications Manager Administration, *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Videoconferencing 3511 MCU and Cisco Unified Videoconferencing 3540 MCU Module Administrator Guide*
- *Cisco Unified Serviceability Administration Guide*

About Conference Bridge Setup

In Cisco Unified Communications Manager Administration, use the **Media Resources** > **Conference Bridge** menu path to configure conference bridges.

Conference Bridge Configuration Tips

Make sure that the following prerequisites are met before you proceed with configuration of a conference bridge:

- Configure the device pools.

Note Software conference bridges automatically get created when the Cisco Unified Communications Manager server gets created. You cannot add software conference bridges to Cisco Unified Communications Manager Administration.

- For software conference bridges, activate the Cisco IP Voice Media Streaming Application service. See the *Cisco Unified Serviceability Administration Guide*.

The software conference bridge provided by the Cisco IP Voice Media Streaming Application service supports both IPv4 and IPv6 audio media connections. The software conference bridge is configured automatically in dual mode when the platform is configured for IPv6 and the IPv6 enterprise parameter is enabled. The software conference bridge supports only IPv4 for the TCP control channel.

Conference Bridge Deletion

Keep in mind that you cannot delete Cisco Unified Communications Manager Conference Bridge Software.

Cisco Unified Communications Manager allows you to delete devices that may be associated with components such as media resource groups. To find out what dependencies the conference device may have, choose the Dependency Records link from the drop-down list box and click Go from the Conference Bridge Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Conference Bridge Settings

Consult the conference bridge configuration settings table that corresponds to the type of conference bridge that you are configuring.

Software Conference Bridge Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

You cannot add software conference bridges to Cisco Unified Communications Manager by using Conference Bridge Configuration. Software conference bridges automatically get added when a Cisco Unified Communications Manager server gets added. After a Cisco Unified Communications Manager server gets added, the software conference bridge gets displayed in the Find/List Conference Bridges window (by default, the first software conference bridge gets configured during Cisco Unified Communications Manager installation) when you perform a search. You can update software conference bridges, but you cannot delete them.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the software conference bridge configuration settings.

Table 1: Software Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	This field automatically displays Cisco Conference Bridge Software.
Host Server	This field automatically displays the Cisco Unified Communications Manager server for this software conference bridge.
Conference Bridge Name	This field automatically displays the software conference bridge name. The format of the name specifies CFB_ followed by a digit that represents the value of the software conference bridge; for example, CFB_3 represents the third conference bridge in the Cisco Unified Communications Manager system.
Description	This field automatically displays a description, but the administrator can update this field.
Device Pool	Choose a device pool that has the highest priority within the Cisco Unified Communications Manager group that you are using or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See topics related to TRP insertion in Cisco Unified Communications Manager in the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See topics related to trusted relay points and media resource management in the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Hardware Conference Bridge Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

Note The hardware model type for Conference Bridge contains a specific Media Access Control (MAC) address and device pool information.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the hardware conference bridge configuration settings.

Table 2: Hardware Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco Conference Bridge Hardware. For a description of this type, see the *Cisco Unified Communications Manager System Guide*.
MAC Address	Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB
Description	This field automatically generates from the MAC address that you provide. You can update this field if you choose.
Device Pool	Choose a device pool that has the highest priority within the Cisco Unified Communications Manager group that you are using or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Special Load Information	Enter any special load information or leave blank to use default.

Cisco IOS Conference Bridge Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco IOS conference bridge configuration settings.

Table 3: Cisco IOS Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco IOS Conference Bridge or Cisco IOS Enhanced Conference Bridge. For a description of this type, see the *Cisco Unified Communications Manager System Guide*.
Conference Bridge Name	Enter the same name that exists in the gateway Command Line Interface (CLI). You can enter up to 15 characters. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-),and underscore (_).
Description	This field automatically generates from the conference bridge name that you provide. You can update this field if you choose.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.
Device Security Mode	This field displays for Cisco IOS Enhanced Conference Bridge only. If you choose Non Secure Conference Bridge, the nonsecure conference establishes a TCP port connection to Cisco Unified Communications Manager on port 2000. **Tip** Ensure this setting matches the security setting on the conference bridge, or the call will fail. The Encrypted Conference Bridge setting supports the secure conference feature. See the *Cisco Unified Communications Manager System Guide* for secure conference bridge configuration procedures.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Cisco Video Conference Bridge Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco video conference bridge configuration settings.

Table 4: Cisco Video Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco Video Conference Bridge (IPVC-35xx). For a description of this type, see the *Cisco Unified Communications Manager System Guide*.
MAC Address	Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB
Description	This field automatically generates from the conference bridge name that you provide. You can update this field if you choose.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Product-Specific Configuration	

Field	Description
Model-specific configuration fields that the device manufacturer defines	The device manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon under the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer.

Cisco Conference Bridge (WS-SVC-CMM) Settings

Conference Bridge for Cisco Unified Communications Manager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco Conference Bridge (WS-SVC-CMM) configuration settings.

Table 5: Cisco Conference Bridge (WS-SVC-CMM) Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco Conference Bridge (WS-SVC-CMM). For a description of this type, see the *Cisco Unified Communications Manager System Guide*.
Description	Enter a description (up to 50 characters) or leave blank to generate automatically from the MAC address that you provide. Invalid characters comprise quotes (“), angle brackets (<>), backslash (), ampersand,(&), and percent sign (%).
MAC Address	Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example: 1231123245AB

Field	Description
Subunit	From the drop-down list box, choose the value for the daughter card for a given slot on the Communication Media Module card.
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
Maximum Capacity	Choose the maximum number of streams for a given service on a daughter card. Possible values include 32, 64, 96, and 128 streams. Ensure that each daughter card has as many ports as the value that you choose.
Product-Specific Configuration	

Field	Description
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the "?" information icon under the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer.

Cisco IOS Heterogeneous Video Conference Bridge Settings

Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Cisco IOS Heterogeneous Video Conference Bridge specifies the IOS-based conference bridge type that supports heterogeneous video conferences. In a heterogeneous video conference, all the conference participants connect to the conference bridge with phones that use different video format attributes. In heterogeneous conferences, transcoding and transsizing features are required from the DSP to convert the signal between the various formats.

For heterogeneous video conferences, callers connect to the conference as audio participants under either of the following conditions:

- Insufficient DSP resources.
- The conference bridge is not configured to support the video capabilities of the phone.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco IOS Heterogeneous Video Conference Bridge configuration settings.

Table 6: Cisco IOS Heterogeneous Video Conference Bridge Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.

Field	Description
Location	Use location to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Cisco IOS Guaranteed Audio Video Conference Bridge Settings

Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me voice and video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Cisco IOS Guaranteed Audio Video Conference Bridge specifies the IOS-based video conference bridge type where DSP resources are reserved for the audio portion of the conference, and video service is not guaranteed. Callers on video phones may have video service if DSP resources are available at the start of the conference. Otherwise, the callers connect to the conference as audio participants.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco IOS Heterogeneous Video Conference Bridge configuration settings.

Table 7: Cisco IOS Guaranteed Audio Video Conference Bridge Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge
Description	Enter a description for your conference bridge
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.
Location	Use location to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Cisco IOS Homogeneous Video Conference Bridge Settings

Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Cisco IOS Homogeneous Video Conference Bridge specifies the IOS-based conference bridge type that supports homogeneous video conferences. A homogeneous video conference is a video conference in which all participants connect using the same video format attributes. All the video phones support the same video format and the conference bridge sends the same data stream format to all the video participants.

If the conference bridge is not configured to support the video format of a phone, the caller on that phone connects to the conference as an audio only participant.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco IOS Homogeneous Video Conference Bridge configuration settings.

Table 8: Cisco IOS Homogeneous Video Conference Bridge Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.
Location	Use location to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

Cisco TelePresence MCU Settings

Cisco TelePresence MCU refers to a set of hardware conference bridges for Cisco Unified Communications Manager.

The Cisco TelePresence MCU is a high-definition (HD) multipoint video conferencing bridge. It delivers up to 1080p at 30 frames per second, full continuous presence for all conferences, full trans-coding, and is ideal for mixed HD endpoint environments.

The Cisco TelePresence MCU supports SIP as the signaling call control protocol. It has a built in Web Server that allows for complete configuration, control and monitoring of the system and conferences. The Cisco TelePresence MCU provides XML management API over HTTP.

Cisco TelePresence MCU allows both ad hoc and meet-me voice and video conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

Field	Description
Conference Bridge Name	Enter a name for your conference bridge
Description	Enter a description for your conference bridge
Username	Enter the Cisco TelePresence MCU administrator username.
Password	Enter the Cisco TelePresence MCU administrator password.
Confirm Password	Enter the Cisco TelePresence MCU administrator password.
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU. The default HTTPS port is 443. For information on how to create a TLS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU, see topics related to setting up a TLS connection with Cisco TelePresence MCU.
HTTP Port	Enter the Cisco TelePresence MCU HTTP port. The default port is 80.

Note The HTTP configuration must match what is configured on the Cisco TelePresence MCU. This information allows Cisco Unified Communications Manager to invoke the remote management API on the Cisco TelePresence MCU.

Cisco TelePresence Conductor Settings

Cisco TelePresence Conductor provides intelligent conference administrative controls and is scalable, supporting device clustering for load balancing across MCUs and multiple device availability. Administrators can implement the Cisco TelePresence Conductor as either an appliance or a virtualized application on VMware

with support for Cisco Unified Computing System (Cisco UCS) platforms or third-party-based platforms. Multiway conferencing, that allows for dynamic two-way to three-way conferencing, is also supported.

Cisco TelePresence Conductor supports both ad hoc and meet-me voice and video conferencing. Cisco TelePresence Conductor dynamically selects the most appropriate Cisco TelePresence resource for each new conference. Ad hoc, "MeetMe" and scheduled voice and video conferences can dynamically grow and exceed the capacity of individual MCUs. One Cisco TelePresence Conductor appliance or Cisco TelePresence Conductor cluster has a system capacity of 30 MCUs or 2400 MCU ports. Up to three Cisco TelePresence Conductor appliances or virtualized applications may be clustered to provide greater resilience.

Cisco TelePresence Conductor also provides the XML management API over HTTP, and has a built-in Web Server for complete configuration, control and monitoring of the system and conferences. For more information, see the *Cisco TelePresence Conductor Administrator Guide* and the *Cisco Unified Communications Manager System Guide*.

Note If you are using encryption with Cisco TelePresence Conductor, select cisco-telepresence-conductor-interop as the default normalization script.

The following table describes the Cisco TelePresence Conductor configuration settings.

Table 9: Cisco TelePresence Conductor Configuration Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.
Conference Bridge Prefix	The Conference Bridge Prefix is used only for centralized deployments when the conference resources are deployed across a Small Medium Enterprise (SME) and the HTTP and SIP signaling are intended for different destinations. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
SIP Trunk	Select a SIP trunk to use for this conference bridge from a list of existing SIP trunks.
HTTP Interface Info	
Override SIP Trunk Destination	Check this check box to override the SIP trunk destination. Use this feature if the HTTP and SIP signaling are intended for different destination IP addresses, for example, when the device is used in a centralized deployment. Click the "+" and "-" buttons to add or remove IP addresses and hostnames. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
Hostname/IP Address	Enter one or more hostnames or IP addresses for the HTTP signaling destination if you have selected to override the SIP trunk destination.

Field	Description
Username	Enter the Cisco TelePresence Conductor administrator username.
Password	Enter the Cisco TelePresence Conductor administrator password.
Confirm Password	Enter the Cisco TelePresence Conductor administrator password
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence Conductor. The default HTTPS port is 443.
HTTP Port	Enter the Cisco TelePresence Conductor HTTP port. The default port is 80.

Set Up TLS and HTTPS Connection with Cisco TelePresence MCU

If you are using SRTP with Cisco TelePresence MCU, you must set up a TLS and HTTPS connection with Cisco TelePresence MCU so that you do not expose keys and other security-related information during call negotiations.

Note This procedure details tasks that are performed in Cisco Unified Communications Manager. For detailed instructions on how to import and export certificates in Cisco TelePresence MCU, see your Cisco TelePresence MCU product documentation.

Note For HTTPS, the IP address of MCU should be configured as Alternate Name in the MCU certificate, because Unified Communications Manager allows only an IP address to be configured for MCU on the conference bridge window.

Procedure

Step 1 Download the Cisco Unified Communications Manager security certificate by performing the following steps:

a) In Cisco Unified Operating System Administration, choose **Security** > **Certificate Management.**
b) Click **Find**.
c) Click **CallManager.pem** to view the certificate.
d) Click **Download** and save the file to a local drive.

Step 2 Upload the Cisco Unified Communications Manager certificate to Cisco TelePresence MCU.

Step 3 Generate self-signed certificates for Cisco TelePresence MCU and save the certificates to a local drive.

Step 4 Upload self-signed certificates to the Cisco TelePresence MCU.

Step 5 Upload Cisco TelePresence MCU certificates to Cisco Unified Communications Manager by doing the following:

a) In Cisco Unified Operating System Administration, choose **Security** > **Certificate Management**.
b) Click **Upload Certificate/Certificate Chain**.
c) From the Certificate Name drop-down list box, choose **CallManager-trust**.
d) Click **Browse** and locate the Cisco TelePresence MCU certificate that you saved locally.
e) Click **Upload File** to upload certificates.

Step 6 In Cisco Unified Communications Manager Administration, choose **System** > **Security** > **SIP Trunk Security Profile** and create a secure SIP Trunk Security Profile that uses the following settings:

- Device Security Mode must be Encrypted
- Incoming Transport Type and Outgoing Transport Type must be TLS
- X.509 Subject Name must be set to the defined Common Name that is used in the Cisco TelePresence MCU certificates

Step 7 On the Cisco TelePresence MCU, configure SIP signaling encryption with TLS, and media encryption with SRTP.

Video conference resource setup

SIP Trunk Setup for Video Conference Bridge Devices

The following video conference bridge devices use SIP trunks for video conferences on Cisco Unified Communications Manager clusters:

- Cisco TelePresence MCU
- Cisco TelePresence Conductor

Set the following SIP trunk parameters for use with SIP video conference bridge devices. Use the default setting for all other SIP trunk parameters.

- Device Name
- Description
- Device Pool
- Location
- Destination Address
- Destination Port

Note Multiple IP addresses and ports can be specified.

- SIP Trunk Security Profile: You must select TelePresence Conference as the SIP trunk security profile.
- SIP Profile

Note For improved performance, use the default standard SIP profile for TelePresence conferencing that has the Options ping configured.

- Assign the encryption interworking script to SIP trunks that are used for Cisco TelePresence Conductor if encryption is used.

See topics related to setting up trunks for more details about SIP trunk configuration.

Limitations

- Media Termination Point (MTP) Required: Cisco Unified Communications Manager ignores this configuration for all ad hoc conference calls even if this is selected on the SIP trunk.
- Early Offer Support for Voice and Video calls: Cisco Unified Communications Manager ignores this configuration for all ad hoc conference calls even if this is selected on the SIP profile that is associated with the SIP trunk that is linked to the conferencing resource server.
- SIP Rel1xx Option: Cisco Unified Communications Manager ignores this configuration for ad hoc conference calls even if this is enabled on the SIP profile associated with the SIP trunk that is linked to the conferencing resource server.
- RSVP over SIP: Cisco Unified Communications Manager ignores this configuration for all ad hoc conference calls if this is enabled for E2E. If this is configured for local RSVP, the configuration will be effective.

Set Up TelePresence Video Conference Bridge

Use Cisco Unified Communications Manager Administration to add and configure a video conference bridge device. Each video conference bridge device must be assigned to a SIP trunk when you configure the video conference device for the node.

Before you begin

Set up a SIP trunk before you proceed. See topics related to trunk setup and SIP trunk setup for video conference bridge devices for details.

Procedure

Step 1 Select **Media Resources** > **Conference Bridge**.

The **Find and List Conference Bridges** window displays.

Step 2 Click **Add New**. The **Conference Bridge Configuration** window displays.

Step 3 Select the type of SIP video conference bridge device from the **Conference Bridge Type** drop-down list.

Step 4 Enter a name and description for the video conference bridge device in the **Device Information** pane.

Note For field descriptions, see topics related to configuration settings for the selected video conference bridge type.

Step 5 Select a SIP trunk from the **SIP Trunk** drop-down list.

Step 6 Enter the following mandatory information HTTP interface username, password, and confirm the password in the **HTTP Interface Info** pane.

- Username
- Password
- Confirm Password
- HTTP Port

Step 7 (Optional) Check the **Use HTTPS** check box.

Step 8 Click **Save**.

Synchronize Conference Device Settings

To synchronize a conference device with the most recent configuration changes, perform the following procedure, which applies any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose **Media Resources** > **Conference Bridge**.

The Find and List Conference Bridges window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.

The window displays a list of conference bridges that match the search criteria.

Step 4 Check the check boxes next to the conference bridges that you want to synchronize. To choose all conference bridges in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected.

The Apply Configuration Information dialog displays.

Step 6 Click OK.