# Configure H.323 Trunks



# H.323 Trunk Overview

If you have an H.323 deployment, H.323 trunks provide connectivity to remote clusters and other H.323 devices, such as gateways. H.323 trunks support most of the audio and video codecs that Unified Communications Manager supports for intra-cluster communications, with the exception of wideband audio and wideband video. H.323 trunks use the H.225 protocol for call control signaling and the H.245 protocol for media signaling.

Within Cisco Unified CM Administration, H.323 trunks can be configured using the Inter-cluster Trunk (Non-Gatekeeper Controlled) trunk type and protocol options.

If you have a non-gatekeeper H.323 deployment, you must configure a separate intercluster trunk for each device pool in the remote cluster that the local Unified Communications Manager can call over the IP WAN. The intercluster trunks statically specify either the IPv4 addresses or hostnames of the remote devices.

You can configure up to 16 destination addresses for a single trunk.

### Intercluster Trunks

When configuring intercluster trunk connections between two remote clusters, you must configure an intercluster trunk on each cluster and match the trunk configurations so that the destination addresses used by one trunk match the call processing nodes that are used by the trunk from the remote cluster. For example:

- Remote cluster trunk uses Run on all Active Nodes—The remote cluster trunk uses all nodes for call processing and load balancing. In the local intercluster trunk that originates in the local cluster, add in the IP addresses or hostnames for each server in the remote cluster.
- Remote cluster does not use Run on all Active Nodes—The remote cluster trunk uses the servers from the Unified Communications Manager Group that is assigned to the trunk's device pool for call processing and load balancing. In the local intercluster trunk configuration, you must add the IP address or hostname of each node from the Unified Communications Manager group used by the remote cluster trunk's device pool.

### Secure Trunks

To configure secure signaling for H.323 trunks, you must configure IPSec on the trunk. For details, see the *Security Guide for Cisco Unified Communications Manager*. To configure the trunk to allow media encryption, check the SRTP allowed check box in the **Trunk Configuration** window.

**Note** Gatekeepers are no longer widely used, but you can also configure your H.323 deployment to use gatekeeper-controlled trunks. For details on how to set up gatekeeper-controlled trunks, refer to *Cisco Unified Communications Manager Administration Guide,* Release 10.0(1).

# H.323 Trunk Prerequisites

Plan out your H.323 deployment topology. For intercluster trunks, make sure you know which servers the corresponding remote cluster trunks use for call processing and load balancing. You will have to configure your local intercluster trunk to connect to each call processing server used by the trunk in the remote cluster.

If you are using Cisco Unified Communications Manager groups assigned to a trunk device pool for load balancing on the trunk, complete the configuration in chapter "Configure Trunks", *Core Settings for Device Pools Configuration Task Flow* section.

# Configure H.323 Trunks

Use this procedure to configure trunks for an H.323 deployment.

### Procedure

**Step 1** From Cisco Unified CM Administration, choose **Device** > **Trunk**.

**Step 2** Click **Add New**.

**Step 3** From the **Trunk Type** drop-down list box, choose **Inter-Cluster Trunk (Non-Gatekeeper Controlled)**.

**Step 4** From the **Protocol** drop-down list box, choose **Inter-Cluster Trunk**.

**Step 5** In the **Device Name** text box, enter the unique identifier for the trunk.

**Step 6** From the **Device Pool** drop-down list box, select the device pool that you configured for this trunk.

**Step 7** If you want to use every node in the local cluster for processing for this trunk, check the **Run on all Active Unified CM Nodes** check box.

**Step 8** If you want to allow encrypted media across the trunk, check the **SRTP Allowed** check box.

**Step 9** If you want to configure H.235 pass through, check the **H.235 Pass Through Allowed** check box.

**Step 10** In the **Remote Cisco Unified Communications Manager Information** section, enter an IP address or hostname for each remote server to which this trunk connects.