

# Cisco CallManager 3.3 Gatekeeper Configuration

Document ID: 44946

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Configure the Gatekeeper and Trunk in Cisco CallManager

Add a Gatekeeper

Add a Gatekeeper Controlled H.225 Trunk

### Configure the Gatekeeper on the Router

Sample Gatekeeper Configuration

Debugs

Cisco CallManager Trace

### Verify

### Troubleshoot

### Related Information

---

## Introduction

A gatekeeper device, also known as a Cisco Multimedia Conference Manager (MCM), supports the H.225 Registration, Admission, and Status Protocol (RAS) message set that is in use for call admission control, bandwidth allocation, and dial pattern resolution (call routing). The gatekeeper can provide these services for communications between Cisco CallManager clusters and H.323 networks. You can configure multiple gatekeeper devices for each Cisco CallManager cluster as well as configure alternate gatekeepers for redundancy. For alternate gatekeeper configuration details, refer to the MCM documentation.

Gatekeeper configuration with Cisco CallManager comprises of these two steps:

1. Configure the gatekeeper and trunk in Cisco CallManager.
2. Configure the gatekeeper on the router.

## Prerequisites

### Requirements

This document is intended for the networking personnel who deploy the IP Telephony networks. Readers of this document should have knowledge of these topics:

1. Voice Over IP Configuration
2. IP Telephony Concepts

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco CallManager version 3.3(2) spB – 171.69.85.171
- Gatekeeper IOS® version c3640-ix-mz.122-15.T2 – 172.16.13.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

# Configure the Gatekeeper and Trunk in Cisco CallManager

Each Cisco CallManager cluster can register with one or more gatekeepers. This section describes how to configure the gatekeeper in Cisco CallManager. You also need to configure trunk devices on the Trunk Configuration page. See the Trunk Configuration section for details.

## Add a Gatekeeper

Use this procedure in order to add a gatekeeper device.

1. Select **Device > Gatekeeper** in order to display the Gatekeeper Configuration page.
2. Enter the appropriate settings. See Table 1 for details about different options. The default settings are used for this setup.
3. Click **Insert** in order to add the new gatekeeper.

The Gatekeepers list displays the page updates, and the name of the new gatekeeper.

## Gatekeeper Configuration Options

Table 1 describes the gatekeeper configuration settings.

**Table 1**

Field	Description
Host Name/IP Address	Enter the IP address or Domain Name System (DNS) name of the gatekeeper in the appropriate field.  You can register multiple gatekeepers for each Cisco CallManager cluster.
Description	<del>Enter a descriptive name for the gatekeeper.</del>
Registration Request Time to Live	Do not change this value unless you have an instruction to do so by a Cisco Technical Support engineer. Enter the time in seconds. The default value specifies 60 seconds.  The Registration Request Time to Live field indicates the length of time that the gatekeeper considers a registration request (RRQ) valid. The system must send a keepalive RRQ to the gatekeeper before the RRQ Time to Live expires.

	Cisco CallManager sends an RRQ to the gatekeeper in order to register and subsequently to maintain a connection with the gatekeeper. The gatekeeper can confirm (RCF) or deny (RRJ) the request.
Registration Retry Timeout	Do not change this value unless you have an instruction to do so by a Cisco Technical Support engineer. Enter the time in seconds. The default value specifies 300 seconds.  The Registration Retry Timeout field indicates the length of time that Cisco CallManager waits before it retries gatekeeper registration after a failed registration attempt.
Enable Device	This check box allows you to register this gatekeeper with Cisco CallManager. By default, this check box remains checked. In order to unregister the gatekeeper from Cisco CallManager, uncheck this check box. The gatekeeper unregisters within approximately one minute after you update this field.

You can configure trunks in Cisco CallManager administration in order to function in either of these ways:

- Non-gatekeeper-Controlled Trunks
- Gatekeeper-Controlled Trunks

**Note:** This document *only* focuses on how to configure Gatekeeper-Controlled H.225 trunks.

### Gatekeeper-Controlled Trunk

In this case, a single intercluster trunk is sufficient to communicate with all remote clusters. Similarly, a single H.225 trunk is necessary to communicate with any H.323 gatekeeper-controlled endpoints. You also need to configure route patterns or route groups in order to route the calls to and from the gatekeeper. In this configuration, the gatekeeper dynamically determines the appropriate IP address for the destination of each call to a remote device, and the local Cisco CallManager uses that IP address in order to complete the call.

This configuration works well in large as well as smaller systems. For large systems where many clusters exist, this configuration helps in order to avoid the configuration of individual intercluster trunks between each cluster.

If you configure gatekeeper-controlled trunks, Cisco CallManager automatically creates a virtual trunk device. The IP address of this device changes dynamically in order to reflect the IP address of the remote device which the gatekeeper determines. Use trunks when you configure the route patterns or route groups that route calls to and from a gatekeeper.

### Add a Gatekeeper Controlled H.225 Trunk

Use this procedure in order to add a gatekeeper controlled H.225 trunk.

1. In Cisco CallManager Administration select **Device > Trunk**, select **Add a New Trunk**. You then see another page.

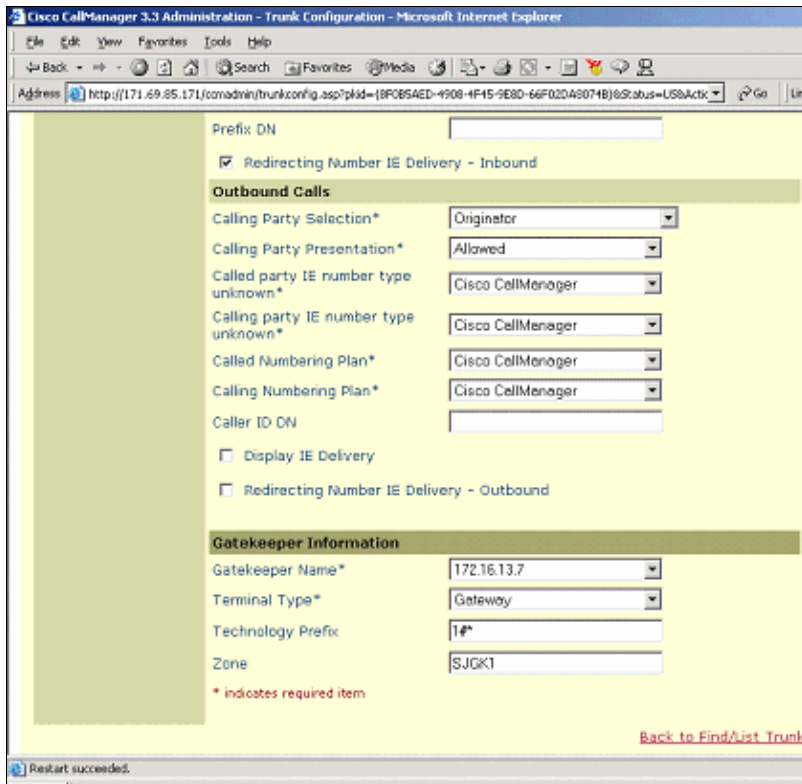
2. Select **H.225 Trunk** (Gatekeeper Controlled) and then select **Next**. You then see another page.

The screenshot shows the Cisco CallManager Administration interface. At the top, there is a navigation menu with 'System', 'Route Plan', 'Service', 'Feature', 'Device', 'User', 'Application', and 'Help'. Below the menu is the 'Cisco CallManager Administration' header with the Cisco logo. The main heading is 'Add a New Trunk'. A sub-heading asks to 'Select the type of Trunk you would like to create:'. There are two dropdown menus: 'Trunk type\*' is set to 'H.225 Trunk (GateKeeper Controlled)' and 'Device Protocol\*' is set to 'H.225'. A note below the dropdowns states '\* indicates required item'. A 'Next' button is located at the bottom right of the form area.

3. Specify the Device Name and Device Pool information. In this configuration all other values are left as default.

The screenshot shows the 'Trunk Configuration' page in a Microsoft Internet Explorer browser window. The browser title is 'Cisco CallManager 3.3 Administration - Trunk Configuration - Microsoft Internet explorer'. The address bar shows a URL starting with 'http://171.69.85.171/cmadmin/trunkconfig.asp?pkid={BFC65AED-4908-4F15-9E8D-66F02DA8074B}&Status=US&Acti...'. The page title is 'Trunk Configuration'. There are two links at the top right: 'Add a New Trunk' and 'Back to Find/List Trunk'. The main content area shows the following information: 'Product: H.225 Trunk (GateKeeper Controlled)', 'Device Protocol: H.225', and 'Status: Update completed.'. Below this are three buttons: 'Update', 'Delete', and 'Reset Trunk'. The 'Device Information' section contains several fields: 'Device Name\*' (TrunkDeviceGK), 'Description' (TrunkDevice), 'Device Pool\*' (Default), 'Media Resource Group List' (< None >), 'Location' (< None >), and 'AAR Group' (< None >). There is a checkbox for 'Media Termination Point Required' which is unchecked. The 'Call Routing Information' section has a sub-heading 'Inbound Calls' and contains: 'Significant Digits\*' (All), 'Calling Search Space' (< None >), 'AAR Calling Search Space' (< None >), and 'Prefix DN'. At the bottom left, there is a status message: 'Restart succeeded.'.

4. On the same page specify the Gatekeeper IP address and terminal type. In the Technology prefix section specify the appropriate Technology (for example Prefix 1#\*) and in the zone box select the appropriate zone (for example SJGK1).



5. Select **Insert** and select **OK** to the message that indicates to reset the trunk.
6. The page refreshes. Select **Reset Trunk** and choose either **Restart** or **Reset** appropriately.

## Configure a Route Pattern

Configure a route pattern in order to route calls to each gatekeeper–controlled trunk.

Refer to Route Pattern Configuration for further information.

In the Route Pattern configuration, specify the pattern to route the call towards the Trunk Device.

This graphic represents an example of how to configure a route pattern in Cisco CallManager. Use the appropriate route pattern as per your route plan.

Cisco CallManager 3.3 Administration - Route Pattern Configuration - Microsoft Internet Explorer

Address: http://171.69.85.171/cmadmin/routepatternconf.asp?pkid={EA7705E1-FDEA-46A6-85A1-D98A7546F1E3}

System Route Plan Service Feature Device User Application Help

**Cisco CallManager Administration**  
For Cisco IP Telephony Solutions

**Route Pattern Configuration**

[Add a New Route Pattern](#)  
[Back to Find/List Route Patterns](#)

**Route Pattern: 316618XXXX**  
Status: Ready  
Note: Any update to this route pattern automatically resets the associated gateway/route list

Copy Update Delete

**Pattern Definition**

Route Pattern\* 316618XXXX

Partition < None >

Description Going to the Gatekeeper Trunk

Numbering Plan\* North American Numbering Plan

Route Filter < None >

Gateway/Route List\* TrunkDeviceGK (Edit)

Route Option  Route this pattern  Block this pattern

Provide Outside Dial Tone  Urgent Priority

**Calling Party Transformations**

Use Calling Party's External Phone Number Mask

Calling Party Transform Mask

Numbering Plan\* North American Numbering Plan

Route Filter < None >

Gateway/Route List\* TrunkDeviceGK (Edit)

Route Option  Route this pattern  Block this pattern

Provide Outside Dial Tone  Urgent Priority

**Calling Party Transformations**

Use Calling Party's External Phone Number Mask

Calling Party Transform Mask

Prefix Digits (Outgoing Calls)

Calling Party Presentation Default

**Called Party Transformations**

Discard Digits < None >

Called Party Transform Mask

Prefix Digits (Outgoing Calls)

**ISDN Network-Specific Facilities Information Element**

Carrier Identification Code

Network Service Protocol -- Not Selected --

Network Service Service Parameter Name Service Parameter Value

-- Not Selected -- < Not Exist >

\* indicates required item.

## Configure the Gatekeeper on the Router

Cisco CallManager registers with a gatekeeper with the use of its IP address and the H.323 ID. You can specify the CallManager IP address in one of these ways:

- In static configuration, use the **gw-type-prefix <prefix> gw ipaddr <address>** command on the gatekeeper in order to specify each Cisco CallManager IP address explicitly.
- In dynamic configuration, when a Cisco CallManager registers with the gatekeeper, it sends its IP address and the specified technology prefix to the gatekeeper. The gatekeeper then registers this Cisco CallManager as a valid gatekeeper-controlled VoIP device.

In order to specify the directory number range for a particular Cisco CallManager, use the **zone prefix** command to configure the range on the gatekeeper. For example, this command specifies the DN for zone SJGK1 that starts from 408–527.

```
zone prefix SJGK1 408527*
```

The maximum number of active calls that are allowed for each zone depends on the codec in use for each call and the bandwidth that is allocated for the zone. Cisco CallManager requests different bandwidths for different codecs:

Codec	Requested Bandwidth by CallManager
G.711	128 kbps
G.729	16 kbps
G.723	14 Kbps

Use Regions in Cisco CallManager in order to specify the codec type. Use the **bandwidth** command on the gatekeeper in order to specify the available bandwidth. For example, this command allocates 512 kbps to the SJGK1 zone.

```
bandwidth total zone SJGK1 512
```

With an allocation of 512 kbps, the SJGK1 zone in this example can support up to:

- 4 G.711 calls or
- 32 G.729 calls or
- 36 G.723 calls at the same time

**Note:** In a scenario where Gatekeeper controls several zones, Cisco recommends you make use of the **bandwidth interzone** command. The **bandwidth total** command can cause issues in some configurations. For more information about Gatekeeper considerations, refer to the *Centralized Gatekeeper Configuration* section of Cisco IP Telephony Solution Reference Network Design.

## Sample Gatekeeper Configuration

```
interface FastEthernet0/0
ip address 172.16.13.7 255.255.255.224
duplex auto
speed auto
```

```
gatekeeper
zone local SJGK1 cisco.com
zone prefix SJGK1 408*
gw-type-prefix 1#* default-technology
no shutdown
```

*!--- The Cisco CallManager trunks register and appear as VoIP-GW.*

```
3640-1#show gatekeeper endpoints
```

```

                                GATEKEEPER ENDPOINT REGISTRATION
                                =====
CallSignalAddr  Port  RASignalAddr  Port  Zone Name      Type  Flags
-----
171.69.85.31   1720  171.69.85.31   4724  SJGK1          TERM
E164-ID: 3166188111
```

```
171.69.85.171 4613 171.69.85.171 1160 SJGK1 VOIP-GW
H323-ID: TrunkDevice1GK_1
Total number of active registrations = 2
```

For more information about how to configure the gatekeeper, refer to VoIP with Gatekeeper.

## Debugs

In this sample scenario, the IP phone makes a call for the H.323 NetMeeting Client (NetMeeting is directly registered with the gatekeeper). Cisco CallManager then sends the call to the gatekeeper through the gatekeeper trunk. This is the output for the **debug RAS** command on the gatekeeper.

```
Oct 15 06:06:22.595: RAS INCOMING PDU ::=

value RasMessage ::= admissionRequest :
{
  requestSeqNum 4343
  callType pointToPoint : NULL
  endpointIdentifier {"61C97A1000000001"}
  destinationInfo
  {
    dialedDigits : "3166188111"
  }
  srcInfo
  {
    dialedDigits : "4085273175"
  }
  srcCallSignalAddress ipAddress :
  {
    ip 'AB4555AB'H
    port 1720
  }
  bandwidth 1280
  callReferenceValue 8
  conferenceID '80480FB2D81C911D08000000AC10F07F'H
  activeMC FALSE
  answerCall FALSE
  canMapAlias TRUE
  callIdentifier
  {
    guid '80480FB2D81C911D08000000AC10F07F'H
  }
  gatekeeperIdentifier {"SJGK1"}
}

Oct 15 06:06:22.599: ARQ (seq# 4343) rcvd
Oct 15 06:06:22.603: H225 NONSTD OUTGOING PDU ::=

value ACFnonStandardInfo ::=
{
  srcTerminalAlias
  {
    e164 : "4085273175"
  }
  dstTerminalAlias
  {
    e164 : "3166188111"
  }
}

Oct 15 06:06:22.603: H225 NONSTD OUTGOING ENCODE BUFFER::= 00 01048073
B85A64A8 01048064 994BB444
Oct 15 06:06:22.603:
Oct 15 06:06:22.603: RAS OUTGOING PDU ::=
```

```

value RasMessage ::= admissionConfirm :
{
  requestSeqNum 4343
  bandwidth 1280
  callModel direct : NULL
  destCallSignalAddress ipAddress :
  {
    ip 'AB45551F'H
    port 1720
  }
  irrFrequency 240
  nonStandardData
  {
    nonStandardIdentifier h221NonStandard :
    {
      t35CountryCode 181
      t35Extension 0
      manufacturerCode 18
    }
    data '0001048073B85A64A801048064994BB444'H
  }
  willRespondToIRR FALSE
  uuiesRequested
  {
    setup FALSE
    callProceeding FALSE
    connect FALSE
    alerting FALSE
    information FALSE
    releaseComplete FALSE
    facility FALSE
    progress FALSE
    empty FALSE
  }
}

```

```

Oct 15 06:06:22.611: RAS OUTGOING ENCODE BUFFER ::= 2B 8010F640 050000AB
45551F06 B800EF40 B5000012 11000104 8073B85A 64A
80104 8064994B B4442800 C0000100 020000
Oct 15 06:06:22.615:
Oct 15 06:06:22.615: IPSOCK_RAS_sendto: msg length 48 from 172.16.13.7:1719
to 171.69.85.171: 1160
Oct 15 06:06:22.615: RASLib::RASSendACF: ACF (seq# 4343) sent to 171.69.85.171
Oct 15 06:06:25.439: RecvUDP_IPSockData successfully rcvd message of
length 113 from 171.69.85.31:4724
Oct 15 06:06:25.439: RAS INCOMING ENCODE BUFFER ::= 26 D0000B03 C0003600
31004200 38004600 41004500 38003000 30003000 300
03000 30003000 32020480 64994BB4 44048064 994BB444 00AB4555 1F06B800
00AB4555 AB06B800 013ED080 480FB2D8 1C911D08 000000
AC 10F07F44 E0200100 11008048 0FB2D81C 911D0800 0000AC10 F07F0100
Oct 15 06:06:25.443:

```

## Cisco CallManager Trace

*!--- Cisco CallManager sends the RRQ to the gatekeeper.*

```

10/14/2003 23:26:40.082 CCM|value V2Message ::= registrationRequest :
{
  requestSeqNum 4372,
  protocolIdentifier { 0 0 8 2250 0 2 },
  discoveryComplete FALSE,
  callSignalAddress

```

```

    {
      ipAddress :
        {
          ip 'AB4555AB'H,
        }
    },
    port 4613
  },
  rasAddress
  {
    ipAddress :
      {
        ip 'AB4555AB'H,
        port 1160
      }
  },
  terminalType
  {
    gateway
    {
      protocol
      {
        h323 :
          {
            },
          voice :
            {
              supportedPrefixes
              {
                {
                  prefix e164 : "1#*"
                }
              }
            }
          }
        },
      mc FALSE,
      undefinedNode FALSE
    },
    gatekeeperIdentifier "SJGK1",
    endpointVendor
    {
      vendor
      {
        t35CountryCode 181,
        t35Extension 0,
        manufacturerCode 18
      }
    },
    timeToLive 60,
    keepAlive TRUE,
    endpointIdentifier "61C97A1000000001"
  }
}

```

*!--- 171.69.85.171 is the IP address of the Cisco CallManager.*

*!--- Registration is confirmed at this point (there is omission of some output).*

```

10/14/2003 23:26:40.142 CCM|value V2Message ::= registrationConfirm :
{
  requestSeqNum 4372,
  protocolIdentifier { 0 0 8 2250 0 4 },
  callSignalAddress
  {

```

```
    },
    gatekeeperIdentifier "SJGK1",
    endpointIdentifier "61C97A1000000001",
    timeToLive 60,
    willRespondToIRR FALSE
  }
}
```

```
!--- Cisco CallManager sends Admission Request (ARQ) to
!--- the gatekeeper in order to place the call.
```

```
10/14/2003 23:27:26.063 CCM|value V2Message ::= admissionRequest :
```

```
{
  requestSeqNum 4376,
  callType pointToPoint : NULL,
  endpointIdentifier "61C97A1000000001",
  destinationInfo
  {
    e164 : "3166188111"
```

```
!-- This is the phone number of the called
!-- party that is the NetMeeting client.
```

```
  },
  srcInfo
  {
    e164 : "4085273175"
```

```
!-- This is the phone number of the calling party
!-- that is the IP phone.
```

```
  },
  srcCallSignalAddress ipAddress :
  {
    ip 'AB4555AB'H,
    port 1720
  },
  bandwidth 1280,
  callReferenceValue 13,
  conferenceID '806076A3DB1C911D0D000000AC10F07F'H,
  activeMC FALSE,
  answerCall FALSE,
  canMapAlias TRUE,
  callIdentifier
  {
    guid '806076A3DB1C911D0D000000AC10F07F'H
  },
  gatekeeperIdentifier "SJGK1"
}
```

```
!--- This line indicates the client that sends this request.
```

```
<NID::171.69.85.171><CT::1,100,90,1.1098993><IP::172.16.240.127>
```

```
!--- Here is the Advanced Communications Function (ACF)
!--- message from the gatekeeper.
```

```
10/14/2003 23:27:26.093 CCM|value V2Message ::= admissionConfirm :
```

```
{
  requestSeqNum 4376,
```

**bandwidth 1280,**

*!-- For a G.711 call, the bandwidth confirmed is 128 kbps.*

```
callModel direct : NULL,
destCallSignalAddress ipAddress :
{
  ip 'AB4555AB'H,
  port 4613
},
irrFrequency 240,
nonStandardData
{
  nonStandardIdentifier h221NonStandard :
  {
    t35CountryCode 181,
    t35Extension 0,
    manufacturerCode 18
  },
  data '0001048073B85A64A801048064994BB444'H
},
willRespondToIRR FALSE,
uuiesRequested
{
  setup FALSE,
  callProceeding FALSE,
  connect FALSE,
  alerting FALSE,
  information FALSE,
  releaseComplete FALSE,
  facility FALSE,
  progress FALSE,
  empty FALSE
}
}
```

*!-- Cisco CallManager displays the RAS information.*

```
10/14/2003 23:27:26.143 CCM|SPROCRas - {
h323-uu-pdu
{
h323-message-body setup :
{
  protocolIdentifier { 0 0 8 2250 0 2 },
  sourceAddress
  {
    e164 : "4085273175",
    h323-ID : "4085273175"
  },
  sourceInfo
  {
    terminal
    {
    },
    mc FALSE,
    undefinedNode FALSE
  },
  destinationAddress
  {
    e164 : "3166188111"
  },
  activeMC FALSE,
  conferenceID '806076A3DB1C911D0D000000AC10F07F'H,
  conferenceGoal create : NULL,
```

```
callType pointToPoint : NULL,
sourceCallSignalAddress ipAddress :
{
  ip 'AB4555AB'H,
  port 1720
},
callIdentifier
{
  guid '806076A3DB1C911D0D000000AC10F07F'H
},
mediaWaitForConnect FALSE,
canOverlapSend FALSE
},
h245Tunneling FALSE,
nonStandardControl
{
  {
    nonStandardIdentifier h221NonStandard :
    {
      |<CLID::ADESALU-SUNPC-Cluster><NID::171.69.85.171>
10/14/2003 23:27:26.143 CCM|t35CountryCode 181,
      t35Extension 0,
      manufacturerCode 18
    },
    data '80440400010100'H
  }
}
}
```

## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

---

## Related Information

- [VoIP with Gatekeeper](#)
- [Voice Technology Support](#)
- [Voice and Unified Communications Product Support](#)
- [Recommended Reading: Troubleshooting Cisco IP Telephony](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Oct 13, 2005

Document ID: 44946

---