TAC Notice: What's Changing on TAC Web

Configuring an Anonymous Device Gatekeeper with Cisco CallManager 3.2

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Send

Contents

Introduction

This document explains how to set up an anonymous device gatekeeper using a Cisco CallManager 3.2 server. It requires the use of a Cisco IOS® Software router to act as a gatekeeper and a Cisco IOS router

to act as an H.323 gateway. The primary focus of this document is on how to configure the Cisco CallManager 3.2 server to use a gatekeeper. After finishing this configuration, you are able to make calls in either direction using Call Admision Control (CAC) between an IP phone registered to the Cisco CallManager 3.2 server and an analog phone attached to the Cisco IOS gateway.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

Before attempting this configuration, please ensure that you meet the following prerequisites:

- You have a sample network with a Cisco CallManager server.
- You have an IP Phone (model 7910, 7940, or 7960).
- You have a Cisco IOS gateway with an FXS port.
- You have an analog phone attached to the FXS port on the Cisco IOS gateway.
- You have a Cisco IOS router with an image that supports H.323 gatekeeper functionality.
- All devices can ping each other.
- The IP phone can call the analog phone with two-way voice capability.
- The analog phone can call the IP phone with two-way voice capability.

Note: For more information, refer to the network diagram below.

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco IOS Router acting as a H.323 VoIP gateway running 12.2(8)YM.
- Cisco IOS Router acting as a H.323 VoIP gatekeeper running 12.2(15)T.
- Cisco CallManager server running 3.2(2c).
- 7960 IP Phone.
- Generic analog phone.
- 2900XL switch.

The information presented in this document was created from devices in a specific lab environment. All

of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Background Theory

An anonymous device gatekeeper handles call routing decsions for the Cisco IOS and Cisco CallManager gateways that are registered to it. This means that the Cisco CallManager servers in the cluster do not need to know about every other gateway in the network. Instead, their route patterns or VoIP dial peers are configured to point to the anonymous device gatekeeper. The anonymous device gatekeeper keeps track of the dial plan for the network. See the document titled Understanding Cisco IOS H.323 Gatekeeper Call Routing for additional information on this subject.

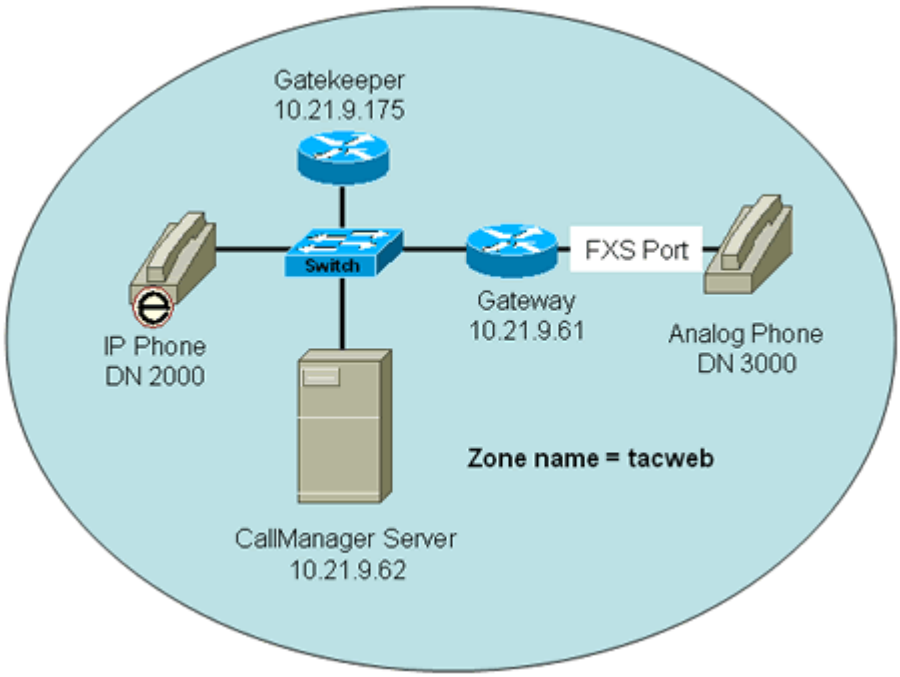
The configuration presented in this document is normally used in networks used for learning internetworking skills. The concepts and commands are the same as you will encounter in a live environment. The primary difference is that this scenario doesn't have a WAN connection for VoIP traffic that would benefit from CAC. In this case, the bandwidth being allocated for CAC comes from the backplane of the switch. In other words this configuration shows how to do CAC on a LAN. This eliminates the uncessary level of complexity required to document a third Cisco IOS gateway for demonstrating how CAC operates in conjunction with a Cisco CallManager server.

Note: The configuration of gatekeepers in Cisco CallManager 3.3 is completely different. You cannot use this document to configure CAC on a Cisco CallManager 3.3 server.

Implementing CAC successfully requires a well-thought-out network design and corresponding CAC overlay. A complete explanation of designing and implementing a CAC solution — including all of the available options for implementing CAC on Cisco IOS gateways and gatekeepers — is beyond the scope of this document. There are several very good resources available on cisco.com to assist in understanding and implementing CAC using Cisco IOS-based gateways and gatekeepers. Search for *gatekeeper* on cisco.com. You can then filter your search with additional words such as troubleshooting, understanding, and so forth. You can also limit the scope of your search to Products and Services and/or Technical Support (TAC-authored content only).

Network Diagram

This document uses the network setup shown in the diagram below.



Configure the Cisco CallManager Gatekeeper Parameters

This section explains how to create an instance of an anonymous device gatekeeper in Cisco CallManager.

Step-by-Step Instructions

1. Select **Device > GateKeeper**.

   Note: If you have an existing gatekeeper you might want to delete it and start over, to ensure that you are starting with the default values for any parameters that are not specifically mentioned in this section.

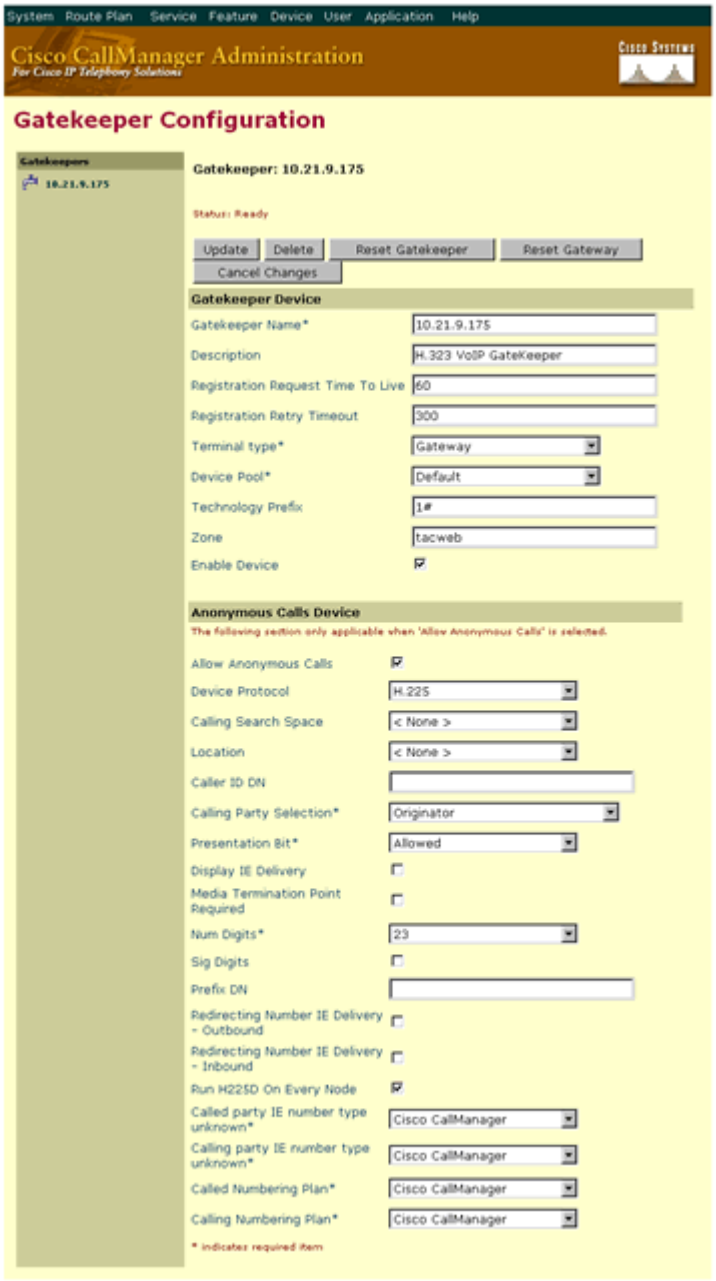
   Note: Your gatekeeper parameter settings should match those shown in the screen that follows the table.

   Enter the following parameters:

Parameter	Setting
GateKeeper Name	Use the DNS name or the IP address of the Cisco IOS GateKeeper router. In this case 10.21.9.175
Terminal Type	Gateway
Device Pool	Default
	1#

	Note: The "*" used in the gatekeeper configuration [1#*] is not included here.
Zone	tacweb
	Note: This is the same zone name used in the gatekeeper and the gateway.
Enable Device	Check this field.
Allow Anonymous Calls	Check this field.
Device Protocol	Select H.225.
Calling Party Selection	Originator
Presentation Bit	Allowed

The parameter page appears as shown:



2. Click **Insert** or **Update** as indicated.

Changing the Route Pattern to Use the Cisco CallManager Gatekeeper

This section explains how to point a route pattern at a gatekeeper (in this case, the anonymous device gatekeeper) instead of a gateway or route list.

Step-by-Step Instructions

1. Select **Route Plan > Route Pattern**.

2. Click **Find**.

3. Click the **Route Pattern** that you had already configured to route calls to the analog phone (in this case, the route pattern for extension 3000).

4. Change the **Gateway/Route List** parameter to point to the entry named `AnonymousDevice`. (This is the gatekeeper that you just created.)

   Note: If your previous configuration allowed calls from your IP phone to your analog phone (as noted in the prerequisites for this document) you should not need to make any further changes. The remainder of the parameters for the route pattern as shown below are set to values that are known to work for the scenario used in this document.

5. Click **Update**.

Configure the Gatekeeper Parameters

This section explains how to configure the Cisco IOS gatekeeper parameters required for CAC.

Use the following configuration for the Cisco gatekeeper:

```
!
!
gatekeeper
zone local tacweb cisco.com 10.21.9.175
zone prefix tacweb 2*
zone prefix tacweb 2* gw-priority 10 10.21.9.62
zone prefix tacweb 2* gw-priority 0 10.21.9.61
zone prefix tacweb 3*
```

```
zone prefix tacweb 3* gw-priority 10 10.21.9.61
zone prefix tacweb 3* gw-priority 0 10.21.9.62
gw-type-prefix 1#* default-technology
bandwidth total zone tacweb 256
no shutdown
!
!
```

Notes for this configuration:

1. The gatekeeper is controlloing the zone named *tacweb*. This is why it is configured as a local zone. The IP address is a local address used as the source address for CAC IP packets from the gatekeeper.

2. The zone prefix commands for the tacweb zone are the dialing plan for this zone. This is how the gatekeeper associates dialed numbers with the correct zone.

   A priority of 1 or higher indicates that a gateway is a viable path to route calls to the prefix configured. A priority of 0 indicates that a gateway is not a viable path to route calls to the prefix configured.

   A complete explanation of how gatekeepers make routing decisions is beyond the scope of this document. See the document titled Understanding Cisco IOS H.323 Gatekeeper Call Routing for more information on how gatekeepers make call routing decisions.

3. In this scenario you are not prepending technology prefixes to the dialed digits when the calls are routed to the gatekeeper. This is why the **gw-type-prefix 1#* default-technology** command is required on the gatekeeper and the **h323-gateway voip tech-prefix 1#** command is required on the Cisco IOS gateway as well as the ***Technology Prefix 1#*** parameter on the Cisco CallManager gatekeeper configuration. If you neglect to do this calls will not complete successfully.

   Note: Do not include the trailing ***** on the Cisco IOS gateway or the Cisco CallManager server configurations. This is only required on the gatekeeper.

4. This zone has a total bandwidth capacity of 256 kbps.

   Note: There are two versions of the command for setting the bandwidth for a zone depending on the version of Cisco IOS you are running on the gatekeeper. The versions are **bandwidth total zone** and **zone bw**.

Configure the Gateway Parameters

This section explains how to configure the Cisco IOS gateway parameters required for CAC.

Use the following configuration for the Cisco gateway:

```
!
interface FastEthernet0/0
ip address 10.21.9.61 255.255.255.0
h323-gateway voip interface
h323-gateway voip id tacweb ipaddr 10.21.9.175 1719
h323-gateway voip h323-id tacweb-gw
h323-gateway voip tech-prefix 1#
```

```
!
voice-port 1/0
!
voice-port 1/1
!
dial-peer voice 1 pots
destination-pattern 3000
port 1/0
!
dial-peer voice 2 voip
destination-pattern 2000
session target ras
!
gateway
!
!
```

Notes for this configuration:

1. In this scenario you do not prepend technology prefixes to the dialed digits when the calls are routed to the gatekeeper. This is why the **h323-gateway voip tech-prefix 1#** command is required on the Cisco IOS gateway and the **gw-type-prefix 1#* default-technology** command is required on the gatekeeper as well as the **Technology Prefix 1#** parameter on the Cisco CallManager gatekeeper configuration.. If you neglect to do this, calls do not complete successfully.

   Note: Do not include the trailing "*" on the Cisco IOS gateway or the Cisco CallManager server configurations. This is only required on the gatekeeper.

2. You must include the **gateway** command. The other parameters that can be applied under the **gateway** command are optional.

3. The **session target ras** command on the gateway causes it to route calls to 2000 (the Directory Number (DN) of the IP phone) to the gatekeeper. This is a very simplified example. Normally you would use wild cards such as 2.... to avoid having to setup up separate dial peers for all DNs with an initial digit of 2.

4. The **h323-gateway voip h323-id** command is used to provide a unique identifier for this gateway that will appear in the **show gatekeeper endpoints** command on the gatekeeper.

5. The voice ports 1/0 and 1/1 in the Cisco IOS gateway are FXS ports. Only one of them — port 1/0 — is in use. The destination pattern (3000) under pots dial-peer registers as a E164-ID with the gatekeeper. You can see this in the output of the **show gatekeeper endpoints** command on the gatekeeper.

Verify

This section provides some of the basic commands available to verify that your gatekeeper configuration is working. There are several other documents on cisco.com that explain verifying and troubleshooting gatekeeper configurations in greater detail. See the Related Information section below.

Use the show gatekeeper endpoints Command

Use the **show gatekeeper endpoints** command on the gatekeeper to verify that the two gateways (Cisco CallManager server and the Cisco IOS gateway router) have registered.

```
GateKeeper#show gatekeeper endpoints
   GATEKEEPER ENDPOINT REGISTRATION
   ================================
   CallSignalAddr  Port  RASSignalAddr   Port  Zone Name Type    Flags
   --------------- ----- --------------- ----- --------- ------- -----
   10.21.9.61      1720  10.21.9.61      54492 tacweb    VOIP-GW
   E164-ID: 3000
   H323-ID: tacweb-gw
   10.21.9.62      1720  10.21.9.62      1710  tacweb    VOIP-GW
   H323-ID: 10.21.9.62
   Total number of active registrations = 2
```

Parameter	Description

E164-ID: 3000	The destination pattern on the POTs Dial peer 1 on the Cisco IOS gateway router
	
	Note: In this case this is an FXS port, so it connects to an end station (in this case, the analog phone shown in the network diagram).
	
	`dial-peer voice 1 pots`
	`  destination-pattern 3000`
	`  port 1/0`

H323-ID: tacweb-gw	The h.323-id parameter on the fast ethernet interface of the Cisco IOS gateway router `h323-gateway voip h323-id tacweb-gw`
H323-ID: 10.21.9.62	This is the IP address of the Cisco CallManager server.

Use the show gateway Command on the IOS Gateway to Verify its Registration Status

Use the **show gateway** command on the Cisco IOS gateway to verify that the gateway has registered with the gatekeeper.

```
GateWay>show gateway
H.323 ITU-T Version: 4.0   H323 Stack Version: 0.1
 Gateway  tacweb-gw  is registered to Gatekeeper tacweb

Alias list (CLI configured)
 E164-ID 3000
 H323-ID tacweb-gw
Alias list (last RCF)
 E164-ID 3000
 H323-ID tacweb-gw
 H323 resource thresholding is Disabled
GateWay>
```

This output shows that the Cisco IOS gateway has registered with the gatekeeper.

Make Calls in Both Directions to Verify Connectivity

You must try to make calls in both directions to ensure that your dial plan is correct and that the gatekeeper will function for calls initiated by either phone.

1. Call the IP phone from the analog phone. You should be able to establish a call and have two-way voice communication.

   Proceed to Step 2 even if you are not able to make the call successfully.

2. Call the analog phone from the IP phone. You should be able to establish a call and have two-way voice communication.

   If you were able to make calls in both directions, proceed to the next section, Use the Show Gatekeeper Calls Command to Verify CAC is Working, to verify that the calls you are making are using CAC.

   If you only have one-way voice communication, refer to the Related Information section at the end for links to documents on troubleshooting one-way voice issues. When you have fixed the one-way voice problem, proceed to the next section.

   If you have a problem placing a call in either direction, or both directions, refer to the Troubleshooting section below.

Use the show gatekeeper calls Command to Verify that CAC is Working

This section helps you to verify that the calls you are making are using CAC.

1. Make a call from the analog phone (3000) to the IP phone (2000) and leave both phones off-hook. Then use the **show gatekeeper calls** command to view an active call.

```
GateKeeper#show gatekeeper calls
Total number of active calls = 1.
                        GATEKEEPER CALL INFO
                        ====================
LocalCallID                          Age(secs)   BW
10-38197                             27          128(Kbps)
 Endpt(s): Alias                  E.164Addr
   src EP: tacweb-gw              3000
           CallSignalAddr  Port   RASSignalAddr   Port
           10.21.9.61      1720   10.21.9.61      54492
 Endpt(s): Alias                  E.164Addr
   dst EP: 10.21.9.62             2000
           CallSignalAddr  Port   RASSignalAddr   Port
           10.21.9.62      1720   10.21.9.62      1710

GateKeeper#
```

   The output above shows that CAC is active for this call. The source and destination DNs (3000 and 2000) are in bold text.

2. Make a call from the IP phone (2000) to the analog phone (3000) and leave both phones off-hook. Then use the **show gatekeeper calls** command to view an active call.

```
GateKeeper#show gatekeeper calls
Total number of active calls = 1.
                         GATEKEEPER CALL INFO
                         ====================
LocalCallID                        Age(secs)   BW
9-32825                            45          128(Kbps)
 Endpt(s): Alias                 E.164Addr
   src EP: 10.21.9.62            2000
           CallSignalAddr  Port  RASSignalAddr   Port
           10.21.9.62      1720  10.21.9.62      1710
 Endpt(s): Alias                 E.164Addr
   dst EP: tacweb-gw             3000
           CallSignalAddr  Port  RASSignalAddr   Port
           10.21.9.61      1720  10.21.9.61      54492

GateKeeper#
```

The output above shows that CAC is active for this call. The source and destination DNs (3000 and 2000) are in bold text.

Reduce the zone bandwidth Parameter to Block All Calls

If you want to perform a final conclusive test that CAC is operation, reduce the ***Zone Bandwidth*** parameter to less that 128. 128 is the bandwidth that the calls are using based on the output from the **show gatekeeper calls** command above.

1. Shut down the gatekeeper first:

   ```
   Gatekeeper(config-gk)#shutdown
   ```

2. Issue the command to reduce the zone's bandwidth:

   ```
   Gatekeeper(config-gk)#bandwidth total zone tacweb 64
   ```

3. Bring the gatekeeper online again:

   ```
   Gatekeeper(config-gk)#no shut
   ```

   You should get an immediate reorder tone after dialing the fourth digit of either DN. If you do not get a reorder tone and the call goes through, you might not have changed the route pattern on the Cisco CallManager server to point to the AnonymousDevice (gatekeeper). Verify this setting. You should also verify that you made the change to the ***zone bandwidth*** parameter.

4. Remember to change the ***zone bandwidth*** back to an amount that will allow the calls to proceed.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting the Gatekeeper Configuration

Follow the instructions below to troubleshoot your configuration.

1. If your gateways are not registering with the gatekeeper and you have verified that all of your

configuration commands are correct, refer to Troubleshooting Gatekeeper Registration Issues.

2. If your gateways are registering with the gatekeeper, and you cannot place calls in either or both directions:
    - Verify that you have the zone prefix commands for your DNs on the gatekeeper.
    - Verify that the zone bandwidth is not set below 128.
    - Try stopping and restarting the Cisco CallManager service on the server.
    - Try shutting down the gatekeeper and restarting it.
    - Try switching your Cisco CallManager route pattern back to the gateway that you used to verify the prerequisites for this document to ensure that you can place place calls in both directions without CAC. If you cannot place calls using your original gateway, you will have to resolve the problem before you can successfully test CAC.

    There are several other documents available on cisco.com that explain verifying and troubleshooting gatekeeper configurations in greater detail; to locate these, see the Related Information section below.

Related Information

- **Understanding H.323 Gatekeepers**
- **Troubleshooting and Understanding Cisco Gatekeeper Bandwidth Management**
- **Understanding Cisco IOS H.323 Gatekeeper Call Routing**
- **Troubleshooting Gatekeeper Registration Issues**
- **Troubleshooting Gatekeeper Endpoint Call Admission Issues**
- **Configuring Basic Gatekeeper Call Admission Control**
- **Troubleshooting One Way Voice Issues**
- **Voice, Telephony and Messaging Technologies**
- **Voice, Telephony and Messaging Devices**
- **Voice, Telephony and Messaging Software**
- **Voice, Telephony and Messaging TAC eLearning Solutions**
- **Recommended Reading: Troubleshooting Cisco IP Telephony, Cisco Press, ISBN 1587050757**
- **Technical Support - Cisco Systems**

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 09, 2003 Document ID: 42063
