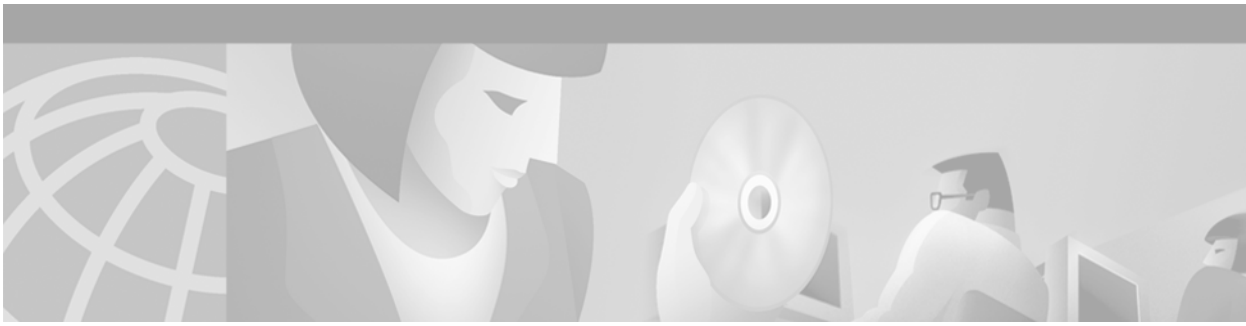


Configuring H.323 Gateways

This chapter describes the configuration of H.323 gateways and contains the following sections:

For a complete description of the gateway commands used in this chapter, refer to the *Cisco IOS Voice, Video, and Fax Command Reference*. To locate documentation for other commands that appear in this chapter, use the command reference master index or search online. For general information about H.323 gateways and their functions, see the "H.323 Applications" chapter in this configuration guide.

For more information on configuring Cisco mobile telephony products, see Appendix F, "Global System for Mobile Communications Full Rate and Enhanced Full Rate Codecs."

To identify the hardware platform or software image information associated with a feature in this chapter, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms"section in the "Using Cisco IOS Software" chapter.

H.323 Gateway Prerequisite Tasks

Before configuring the router as a gateway, perform the following tasks:

- Establish a working IP network. For more information about configuring IP, refer to the *Cisco IOS IP Configuration Guide*.
- Develop a network plan that details the requirements and characteristics of your Voice over IP (VoIP) network. For further information, see the "Voice over IP Overview" chapter of this configuration guide and refer to the *Voice over IP Implementation Guide*.
- Ensure that the routers you intend to configure as H.323 gateways are running a Cisco IOS software image that contains gateway functionality. (Software images that support gateway features contain *-gw-* in the code image name.)

To use the H.323 security and accounting features described in this document, keep the following in mind:

- These features use the H.235 standard. Because the standard is broad, ensure that the gatekeeper provides H.235 functionality that specifically complements the gateway implementation described in this document.
- In addition, because the H.323 gateway sends the accounting information using a non-standard field in the ClearToken message, ensure that the gatekeeper is able to handle this information.

H.323 Gateway Configuration Task List

An H.323 gateway is an endpoint on a LAN that provides real-time, two-way communication between H.323 terminals on the LAN and other International Telecommunication Union Telecommunication Standardization Sector (ITU-T) terminals in the WAN. An H.323 gateway can also communicate with another H.323 gateway. Gateways allow H.323 terminals to communicate with non-H.323 terminals by converting protocols. The gateway is the point at which a circuit-switched call is encoded and repackaged into IP packets. Because gateways function as H.323 endpoints, they provide admission control, address lookup and translation, and accounting services. In an environment in which both gatekeepers and gateways are used, only gateways are configured to send VoIP data.

To configure an H.323 gateway, perform the tasks described in the following sections. Except for the first task, all tasks are optional.

Identifying a Router Interface As an H.323 Gateway

To configure a Cisco device as an H.323 gateway in a service provider environment, configure at least one of its interfaces as a gateway interface. Use either an interface that is connected to the gatekeeper or a loopback interface for the gateway interface. The interface that is connected to the gatekeeper is usually a LAN interface—Fast Ethernet, Ethernet, FDDI, or Token Ring.

To configure a gateway interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gateway`	Enables the gateway and enters gateway configuration mode.
Step 2	`Router(config-gateway)# exit`	Exits gateway configuration mode.
Step 3	`Router(config)# ip cef`	(Optional) Enables Cisco Express Forwarding (CEF) routing.

	Command	Purpose
Step 4	`Router(config)# interface type number [name-tag]`	Enters interface configuration mode for the interface that is connected to the gatekeeper. The keywords and arguments are as follow: • *type*—Specifies the type of interface to be configured. • *number*—Specifies the port, connector, or interface card number. The number is assigned at the factory at the time of installation or when added to a system and can be displayed with the **show interfaces** command. • *name-tag*—(Optional) Specifies the logic name to identify the server configuration so that multiple entries of server configuration can be entered.
Step 5	`Router(config-if)# h323-gateway voip interface`	Identifies this interface as a VoIP gateway interface.
Step 6	`Router(config-if)# h323-gateway voip id gatekeeper-id {ipaddr ip-address [port-number]| multicast} [priority number]`	(Optional) Defines the name and location of the gatekeeper for this gateway. The keywords and arguments are as follows: • *gatekeeper-id*—Indicates the H.323 identification of the gatekeeper. This value must exactly match the gatekeeper ID in the gatekeeper configuration. The recommended format is name.domain-name. • **ipaddr**—Indicates that the gateway will use an IP address to locate the gatekeeper. • *ip-address*—Defines the IP address to be used to identify the gatekeeper. • *port-number*— (Optional) Defines the port number used. • **multicast**—Indicates that the gateway will use multicast to locate the gatekeeper. • **priority** *number*—(Optional) The priority of this gatekeeper. The range is 1 through 127, and the default value is 127.
Step 7	`Router(config-if)# h323-gateway voip h323-id interface-id`	(Optional) Defines the H.323 name of the gateway, identifying this gateway to its associated gatekeeper. The *interface-id* argument is the H.323 name (ID) used by this gateway when this gateway communicates with its associated gatekeeper. Usually, this ID is the name of the gateway, with the gatekeeper domain name appended to the end: name@domain-name.
Step 8	`Router(config-if) h323-gateway voip tech-prefix prefix`	(Optional) Defines the technology prefix that the gateway will register with the gatekeeper. The *prefix* argument defines the numbers used as the technology prefixes. Each technology prefix can contain up to 11 characters. Although not required, a pound symbol (#) is frequently used as the last digit in a technology prefix. Valid characters are 0 through 9, the pound symbol (#), and the asterisk (*).

Verifying Gateway Interface Configuration

To find the current registration information and status of the gateway, use the **show gateway** command.

Configuring Gateway RAS

The Registration, Admission, and Status (RAS) signaling function performs registration, admissions, status, and disengage procedures between the H.323 VoIP gateway and the H.323 VoIP gatekeeper. RAS tells the gatekeeper to translate the E.164 phone number of the session target into an IP address.

In the RAS exchange between a gateway and a gatekeeper, a technology prefix is used to identify the specific gateway when the selected zone contains multiple gateways. The **tech-prefix** dial-peer configuration command is used to define technology prefixes. See the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter in this configuration guide for more information on the **tech-prefix** command, or refer to the *Cisco IOS Voice, Video, and Fax Command Reference*.

In most cases there is a dynamic protocol exchange between the gateway and the gatekeeper that enables the gateway to inform the gatekeeper about technology prefixes and where to forward calls. If, for some reason, that dynamic registry feature is not in effect, statically configure the gatekeeper to query the gateway for this information. To configure the gatekeeper to query for this information, see the "Configuring H.323 Gatekeepers and Proxies" chapter. To configure RAS, define specific parameters for the applicable plain old telephone service (POTS) and VoIP dial peers. The POTS dial peer informs the system of which voice port to direct incoming VoIP calls to and (optionally) determines that RAS-initiated calls will have a technology prefix prepended to the destination telephone number. The VoIP dial peer determines how to direct calls that originate from a local voice port into the VoIP cloud to the session target. The session target indicates the address of the remote gateway where the call is terminated. There are several different ways to define the destination gateway address:

- By statically configuring the IP address of the gateway.
- By defining the Domain Name System (DNS) of the gateway.
- By using RAS. If RAS is being used, the gateway determines the destination target by querying the RAS gatekeeper.

To configure RAS, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice number pots`	Enters dial-peer configuration mode to configure a POTS peer. The *number* argument is a tag that identifies the dial peer. (This number has local significance only.) Valid entries are from 1 to 2,147,483,647.
Step 2	`Router(config-dial-peer)# destination-pattern [+]string[T]`	Specifies the E.164 address associated with this dial peer. The keywords and arguments are as follows: • **+**—(Optional) Specifies a character indicating an E.164 standard number. The plus sign (+) is not supported on the Cisco MC3810 multiservice concentrator. • *string*—Indicates a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: – The asterisk (*) and pound sign (#)—Indicates the keys that appear on standard touch-tone dial pads. – Comma (,)—Inserts a pause between digits. – Period (.)—Matches any entered digit (this character is used as a wildcard). – Percent sign (%)—Indicates that the previous digit/pattern occurred zero or multiple times, similar to the wildcard usage in the regular expression. – Plus sign (+)—Matches a sequence of one or more matches of the character/pattern. **Note** The plus sign used as part of the digit string is different from the plus sign that can be used in front of the digit string to indicate that the string is an E.164 standard number. – Circumflex (^)—Indicates a match to the beginning of the string. – Dollar sign ($)—Matches the null string at the end of the input string. – Backslash symbol (\)—Is followed by a single character matching that character or used with a single character having no other significance (matching that character). – Question mark (?)— Indicates that the previous digit occurred zero or one time.

	Command	Purpose
		– Brackets ([])—Indicate a range of digits. A range is a sequence of characters enclosed in the brackets, and only numeric characters from "0" to "9" are allowed in the range. This is similar to a regular expression rule. – Parentheses (())—Indicate a pattern and is the same as the regular expression rule—for example, 408(555). Parentheses are used in conjunction with symbols ?, %, or +. For more information on applying wildcard symbols to destination patterns and the dial strings that result, see the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter. • **T**—(Optional) Control character indicating that the **destination-pattern** value is a variable-length dial string.
Step 3	**Cisco AS5300 Universal Access Server** `Router(config-dial-peer)# port controller:D`	Associates this POTS dial peer with a specific voice port. The keywords and arguments are as follows: • *controller*—Specifies the T1 or E1 controller. • **:D**—Indicates the D channel associated with the ISDN PRI. **Note** The syntax of the **port** command is platform specific. For information on how to configure this command for your specific device, see the **port** command documentation in the "Configuring Voice Ports" chapter.
Step 4	`Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.
Step 5	`Router(config)# dial-peer voice tag voip`	Enters dial-peer configuration mode to configure a VoIP peer. The *tag* argument identifies the dial peer. (This number has local significance only.) Valid entries are from 1 to 2,147,483,647.
Step 6	`Router(config-dial-peer)# destination-pattern [+]string[T]`	For an explanation of the command, keywords, and arguments, see Step 2 of this configuration task table.
Step 7	`Router (config-dial-peer)# tech-prefix number`	The *number* argument defines the numbers used as the technology prefix. Each technology prefix can contain up to 11 characters. Although not strictly necessary, a pound symbol (#) is frequently used as the last digit in a technology prefix. Valid characters are 0 though 9, the pound symbol (#), and the asterisk (*).
Step 8	`Router (config-dial-peer)# session target ras`	Specifies that the RAS protocol is being used to determine the IP address of the session target—meaning that a gatekeeper will translate the E.164 address to an IP address.

Verifying RAS Configuration

To verify the POTS and VoIP dial-peer configuration, use the **show dial-peer voice** command. The following example shows output for a VoIP dial peer using RAS on a Cisco AS5300 universal access server:

```
Router# show dial-peer voice 1234

VoiceOverIpPeer1234
tag = 1234, destination-pattern = 1234',
answer-address = ',
group = 1234, Admin state is up, Operation state is up,
incoming called-number = ', connections/maximum = 0/unlimited,
application associated:
type = voip, session-target = ras',
technology prefix: 8#
ip precedence = 0, UDP checksum = disabled,
session-protocol = cisco, req-qos = controlled-load,
acc-qos = best-effort,
fax-rate = voice, codec = g729r8,
Expect factor = 10, Icpif = 30,
VAD = enabled, Poor QOV Trap = disabled,
```

Troubleshooting Tips

To troubleshoot the dial-peer configuration, perform the following tasks:

- To display the types and addressing of RAS messages sent and received, use the **debug ras** command. The debug output lists the message type using mnemonics defined in ITU-T specification H.225.
- To display additional information about the actual contents of the H.225 RAS messages, use the **debug h225 asn1** command.

Configuring AAA Functionality on the Gateway

For the gateway to provide authentication and accounting services, enable and configure your gateway to support authentication, authorization, and accounting (AAA) services. AAA enables the gateway to interact with a RADIUS security server to authenticate users (typically incoming calls) and to perform accounting services. For more information about RADIUS and AAA security services, refer to the *Cisco IOS Security Configuration Guide*.

AAA Authentication

The gateway normally uses AAA in conjunction with interactive voice response (IVR) to check the legitimacy of a prospective gateway user on the basis of an account number (collected by IVR) or Automatic Number Identification (ANI). When the gateway uses AAA with IVR, the IVR application collects the user account and personal identification number (PIN) information and then passes it to the AAA interface. The AAA interface makes a RADIUS authentication request using the given information and, based on the information received from the RADIUS server, forwards either a pass message or a fail message to the IVR application.

For more information about configuring IVR, see the “Configuring Interactive Voice Response” chapter. For more information about authentication services using AAA, refer to the “Configuring Authentication” chapter in the *Cisco IOS Security Configuration Guide*.

AAA Accounting

A call leg is a discrete segment of a call connection that lies between two points in the connection. Each call made through the gateway consists of two call legs: incoming and outgoing. The RADIUS server collects basic start-stop connection accounting data or syslog accounting information during the accounting process for each call leg created on the gateway.

To collect basic start-stop connection accounting data, the gateway must be configured to support gateway-specific H.323 accounting functionality. The gateway sends accounting data to the RADIUS server in one of four ways, as is shown in the following sections:

- Using RADIUS AV Pairs, page 256
- Appendix , “Using RADIUS AV Pairs”Overloading the Acct-Session-Id Field, page 257
- Using Vendor-Specific RADIUS Attributes, page 258
- Using Syslog Records, page 259

Using RADIUS AV Pairs

Basic start-stop connection accounting data and standard RADIUS attributes are used where possible using standard Internet Engineering Task Force (IETF) RADIUS attribute/value (AV) pairs. Table 20 shows the IETF RADIUS attributes that are supported.

Table 20 Supported IETF RADIUS Accounting Attributes

Number	Attribute	Description
30	Called-Station-Id	Allows the network access server to send the called telephone number as part of the Access-Request packet (using Dialed Number Identification Service [DNIS] or similar technology). This attribute is only supported on ISDN and on modem calls on the Cisco AS5200 and Cisco AS5300 routers if used with ISDN PRI.
31	Calling-Station-Id	Allows the network access server to send the calling telephone number as part of the Access-Request packet (using ANI or similar technology). This attribute has the same value as the remote-addr attribute from TACACS+. This attribute is supported only on ISDN and on modem calls on the Cisco AS5200 and Cisco AS5300 routers if used with ISDN PRI.
42	Acct-Input-Octets	Indicates how many octets have been received from the port over the course of the accounting service being provided.
43	Acct-Output-Octets	Indicates how many octets have been sent to the port over the course of delivering the accounting service.
44	Acct-Session-Id	Indicates a unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session-Id numbers restart at 1 each time the router is power-cycled or the software is reloaded.
47	Acct-Input-Packets	Indicates how many packets have been received from the port over the course of this service being provided to a framed user.
48	Acct-Output-Packets	Indicates how many packets have been sent to the port in the course of delivering this service to a framed user.

For more information about RADIUS and the use of IETF-defined attributes, refer to the *Cisco IOS Security Configuration Guide*.

Overloading the Acct-Session-Id Field

Attributes that cannot be mapped to standard RADIUS attributes are packed into the Acct-Session-Id attribute field as ASCII strings separated by the "/" character. The Acct-Session-Id attribute contains the RADIUS account session ID, which is a unique identifier that links accounting records associated with the same login session for a user. To support additional fields, the following string format has been defined for this field:

```
<session id>/<call leg setup time>/<gateway id>/<connection id>/<call origin>/
<call type>/<connect time>/<disconnect time>/<disconnect cause>/<remote ip address>
```

Table 21 shows the field attributes to be used with the Overloaded Acct-Session-Id method and provides a brief description of each.

Table 21 Field Attributes in Overloaded Acct-Session-Id

Field Attribute	Description
SESSION-ID	Specifies the standard RADIUS account session ID.
SETUP-TIME	Provides the Q.931 setup time for this connection in Network Time Protocol (NTP) format. NTP time formats are displayed as %H:%M:%S.%k %Z %tw %tn %td %Y where: • %H is hour (00 to 23). • %M is minutes (00 to 59). • %S is seconds (00 to 59). • %k is milliseconds (000 to 999). • %Z is time zone string. • %tw is day of week (Saturday through Sunday). • %tn is month name (January through December). • %td is day of month (01 to 31). • %Y is year including century (for example, 1998).
GATEWAY-ID	Indicates the name of the underlying gateway in the form of "gateway.domain_name."
CALL-ORIGIN	Indicates the origin of the call relative to the gateway. Possible values are **originate** and **answer**.
CALL-TYPE	Indicates call leg type. Possible values are **telephony** and **VoIP**.
CONNECTION-ID	Specifies the unique global identifier used to correlate call legs that belong to the same end-to-end call. The field consists of 4 long words (128 bits). Each long word is displayed as a hexadecimal value and is separated by a space character.
CONNECT-TIME	Provides the Q.931 connect time for this call leg, in NTP format.
DISCONNECT-TIME	Provides the Q.931 disconnect time for this call leg, in NTP format.

Table 21 Field Attributes in Overloaded Acct-Session-Id

Field Attribute	Description
DISCONNECT-CAUSE	Specifies the reason a call was taken offline as defined in the Q.931 specification.
REMOTE-IP-ADDRESS	Indicates the address of the remote gateway port where the call is connected.

Because of the limited size of the Acct-Session-Id string, it is not possible to embed many information elements in it. Therefore, this feature supports only a limited set of accounting information elements.

Use the **gw-accounting h323** command to configure the overloaded session ID method of applying H.323 gateway-specific accounting.

Using Vendor-Specific RADIUS Attributes

The IETF draft standard specifies a method for communicating vendor-specific information between the network access server (NAS) and the RADIUS server by using the vendor-specific attribute (Attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes that are not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string of the format:

```
protocol: attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" are an appropriate AV pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. The full set of features available for TACACS+ authorization can also be used for RADIUS.

For further information on vendor-specific RADIUS attributes, refer to the *RADIUS Vendor-Specific Attributes Voice Implementation Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm

The VSA fields and their ASCII values are listed in Table 22.

Table 22 VSA Fields and Their ASCII Values

IETF RADIUS Attribute	Vendor-Specific Company Code	Subtype Number	Attribute Name	Description
26	9	23	h323-remote-address	Indicates the IP address of the remote gateway.
26	9	24	h323-conf-id	Identifies the conference ID.
26	9	25	h323-setup-time	Indicates the setup time for this connection in Coordinated Universal Time (UTC), formerly known as Greenwich Mean Time (GMT) and Zulu time.

Table 22 VSA Fields and Their ASCII Values (continued)

IETF RADIUS Attribute	Vendor-Specific Company Code	Subtype Number	Attribute Name	Description
26	9	26	h323-call-origin	Indicates the origin of the call relative to the gateway. Possible values are **originating** and **terminating,** which are equivalent to **originate** and **answer** in the Call-Origin field.
26	9	27	h323-call-type	Indicates call leg type. Possible values are **telephony** and **VoIP**.
26	9	28	h323-connect-time	Indicates the connection time for this call leg in UTC.
26	9	29	h323-disconnect-time	Indicates the time this call leg was disconnected in UTC.
26	9	30	h323-disconnect-cause	Specifies the reason a connection was taken offline per the Q.931 specification.
26	9	31	h323-voice-quality	Specifies the impairment/calculated planning impairment factor (ICPIF) affecting voice quality for a call.
26	9	33	h323-gw-id	Indicates the name of the underlying gateway.

Use the **gw-accounting h323 vsa** command to configure the VSA method of applying H.323 gateway-specific accounting.

Using Syslog Records

The syslog accounting option exports the information elements associated with each call leg through a system log message, which can be captured by a syslog daemon on the network. The syslog output consists of the following:

```
<server timestamp> <gateway id> <message number> : <message label> : <list of AV pairs>
```

The syslog message fields are listed in Table 23.

Table 23 Syslog Message Output Fields

Field	Description
server timestamp	The time stamp created by the server when it receives the message to log.
gateway id	The name of the gateway that emits the message.
message number	The number assigned to the message by the gateway.
message label	A string that identifies the message category.
list of AV pairs	A string consisting of <attribute name> <attribute value> pairs separated by commas.

Use the **gw-accounting h323 syslog** command to configure the syslog record method of gathering H.323 accounting data.

To configure RADIUS authentication and accounting services (as facilitated through authentication, authorization, and accounting [AAA]), use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA) security services.
Step 2	`Router(config)# gw-accounting {h323 [vsa]| syslog}`	Configures gateway-specific H.323 accounting, which may be **h323** or **syslog**. The keywords are as follows: • **h323**—Enables standard H.323 accounting using standard IETF RADIUS attributes. • **vsa**—(Optional) Enables H.323 accounting using RADIUS vendor-specific attributes. • **syslog**—Enables the system logging facility to output accounting information in the form of a system message. **Note** Because the Acct-Session-Id attribute is a standard IETF RADIUS attribute, use the **gw-accounting h323** command to gather accounting data using the overloaded Acct-Session-Id attribute.
Step 3	`Router(config)# aaa authentication login h323 radius`	Sets AAA authentication at login. The keywords are as follows: • **h323**—Defines a method list called h323. • **radius**—Specifies that the RADIUS security protocol be used.
Step 4	`Router(config)# aaa accounting connection h323 start-stop radius`	Defines a method list called **h323**. The keywords are as follows: • **start-stop**—Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether the start accounting notice was received by the accounting server. • **radius**—Specifies that only the RADIUS security protocol be used.

	Command	Purpose
Step 5	`Router(config)# radius-server host ip-address auth-port number acct-port number`	Identifies the RADIUS server and the ports that will be used for authentication and accounting services. The keywords and arguments are as follows: • *ip-address*—Specifies the IP address of the RADIUS server host. • **auth-port**—Specifies User Datagram Protocol (UDP) for authentication requests. • *number*—Specifies the port number for authentication requests; the host is not used for authentication if set to 0. The default authentication port number is 1645. • **acct-port**—Specifies the UDP destination port for accounting requests. • *number*—Port number for accounting requests; the host is not used for accounting if set to 0. The default accounting port number is 1646.
Step 6	`Router(config)# radius-server key key`	Specifies the password used between the gateway and the RADIUS server. The *key* argument specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The *key* is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If the key includes spaces, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Verifying AAA and RADIUS Configuration

To view the configured RADIUS and AAA parameters for this gateway, use the **show running-config** command.

Configuring H.235 Gateway Security

The Cisco H.235-based security and accounting features provide an alternative means for securing H.323 calls. Before Cisco IOS Release 12.0(7)T, only RAS and AAA were used to configure the security and accounting functions for H.323 calls. The H.235-based security and accounting features described in this section can be used by a gatekeeper, which is considered a known and trusted entity, to authenticate, authorize, and route H.323 calls.

The Cisco H.323 gateway supports the use of CryptoH323Tokens for authentication. The CryptoH323Token is defined in the ITU-T H.225 Version 2 standard and is used in a "password-with-hashing" security scheme as described in section 10.3.3 of the H.235 specification.

A cryptoToken can be included in any RAS message to authenticate the sender of the message. A separate database can be used for user ID and password verification.

Cisco H.323 gateways support three levels of authentication:

- Endpoint—The RAS channel used for gateway-to-gatekeeper signaling is not a secure channel. To ensure secure communication, H.235 allows gateways to include an authentication key in their RAS messages. This key is used by the gatekeeper to authenticate the source of the messages. At the endpoint level, validation is performed on all messages from the gateway. The cryptoTokens are validated using the password configured for the gateway.

  Note To secure the RAS messages and calls, it is essential that the gatekeeper provides authentication based on the secure key. The gatekeeper must support H.235 security using the same security scheme as the Cisco gateway.

- Per-Call—When the gateway receives a call over the telephony leg, it prompts the user for an account number and PIN. These two numbers are included in certain RAS messages sent from the endpoint to authenticate the originator of the call.
- All—This option is a combination of the other two. With this option, the validation of cryptoTokens in admission request (ARQ) messages is based on an the account number and PIN of the user who is making a call. The validation of cryptoTokens sent in all the other RAS messages is based on the password configured for the gateway.

CryptoTokens for registration requests (RRQs), unregistration requests (URQs), disengage requests (DRQs), and the terminating side of ARQs contain information about the gateway that generated the token. The cryptoTokens include the gateway identification (ID)—which is the H.323 ID configured on the gateway—and the gateway password. The cryptoTokens for the originating-side ARQ messages contain information about the user that is placing the call, including the user ID and PIN.

Although the scenarios in this document describe how to use the security and accounting features in a prepaid call environment, these features may also be used to authorize IP calls that originate in another domain (inter-service provider or inter-company calls).

The H.235-based security and accounting features can be used in conjunction with AAA. The gateway can be configured to use the gatekeeper for call authentication or authorization, and AAA can be used for call accounting.

In addition, the H.235-based security and accounting features include support for the following:

- Settlement with the gatekeeper, which allows the gateway to obtain, track, and return accounting information.
- Call metering, which allows the gateway to terminate a call if it exceeds the allotted time (in the case of prepaid calls).

Note The H.235 security and accounting features described in this document are separate from, and should not be confused with, the standard interactive voice response (IVR) and AAA features used to authenticate inbound calls or with the settlement functions provided by the Open Settlement Protocol (OSP).

Settlement with the Gatekeeper

The H.235 security and accounting features are designed to support a variety of situations in which some form of authentication or tracking is required. The security features allow control access through the use of a userID-password database. The accounting enhancements allow call usage to be tracked at the origin and at the destination.

Fields have been added to the RAS messages to enhance the accounting capabilities of the Cisco H.323 gateway. These fields allow the gateway to report call-usage information to the gatekeeper. The call-usage information is included in the DRQ message that is sent when the call is terminated.

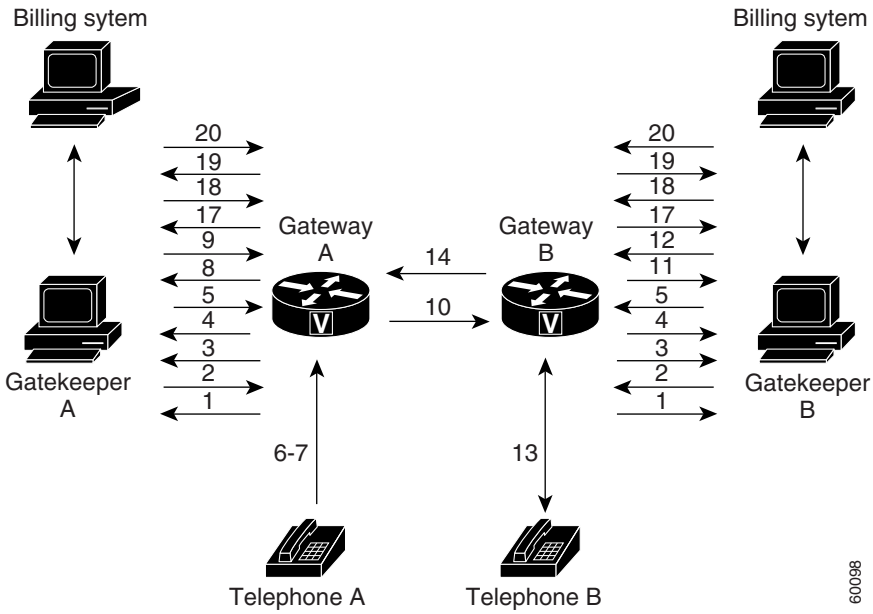
Call Tracking

With prepaid calling services, an account number and PIN must be entered and the duration of the call must be tracked against the remaining credit of the customer. The Cisco H.323 gateway monitors prepaid account balances and terminates a call if the account is exceeded.

Note Because the authentication information includes a time stamp, it is important that all the Cisco H.323 gateways and the gatekeepers (or other entity that is performing the authentication) be synchronized. The Cisco H.323 gateways must be synchronized using the Network Time Protocol (NTP). illustrates the flow of a possible call for which H.323 security and accounting features are used.Flow for a Call That Requires H.323 Security and Accounting Features.

Figure 55 illustrates the flow of a possible call for which H.323 security and accounting features are used.

Figure 55 Flow for a Call That Requires H.323 Security and Accounting Features



In this example, Telephone A is attempting to establish a phone call to Telephone B. The following numbered explanations correspond to the action taking place at each numbered reference in Figure 1.

Gateways Establish Secure Communication with the Gatekeepers

1. Gateways A and B send gatekeeper request (GRQ) messages to their respective gatekeepers. The GRQ message includes the authentication capability and the algorithm object ID.
2. Gatekeepers A and B respond to their respective gateways with gatekeeper confirmation (GCF) messages. The GCF message includes the authentication capability and the algorithm object ID.
3. If the values for the H.323 security parameters do not match what is expected, the gatekeeper responds with a gatekeeper rejection (GRJ) message that contains a reject reason of securityDenial. This prompts the gateway to resend the GRQ.
4. Gateways A and B send registration request (RRQ) messages to their respective gatekeepers. The RRQ message includes authentication information in the cryptoToken field.
5. Gatekeepers A and B respond to their respective gateways with registration confirmation (RCF) messages.

   If an authentication failure occurs, the gatekeeper responds with a registration rejection (RRJ) message.

Secure Telephone Communications Are Initiated

6. Telephone A establishes a connection with Gateway A.
7. Gateway A initiates the interactive voice response (IVR) script to obtain the account number and PIN of the user as well as the desired destination telephone number.
8. Gateway A sends an admission request (ARQ) message to Gatekeeper A. The gateway must include additional information in the ARQ message to enable the gatekeeper to authenticate the call. The information included in the ARQ message varies depending on whether the ARQ message is being sent by the source or the destination gateway. At this point in the scenario, it is the source gateway that is requesting admission. Therefore, the ARQ message includes the account number and PIN of the user. This information is encrypted using MD5 hashing and is included in the cryptoTokens field.
9. Gatekeeper A validates the authentication information, resolves the destination telephone number, and determines the appropriate destination gateway (which is Gateway B in this case). Then Gatekeeper A sends an admission confirmation (ACF) message to Gateway A. The ACF message includes the billing information of the user (such as a reference ID and current account balance for prepaid call services) and an access token.
10. Gateway A sends a setup message to Gateway B. The setup message also includes the access token.
11. Gateway B sends an ARQ message to Gatekeeper B. The ARQ message includes the access token received from Gateway A.
12. Gatekeeper B validates the authentication information in the access token and responds to Gateway B with an ACF message.

    If the authentication information is in error, Gatekeeper B sends an admission rejection (ARJ) message to Gateway B with a reject reason of securityDenial.
13. Gateway B initiates a call to the destination telephone.
14. When the destination telephone is answered, Gateway B sends a connect message to Gateway A.
15. Gateways A and B start their timers to meter the call. If the caller is using prepaid call services, the meter is constantly compared to the account balance of the user, which was included in the ACF message sent in Step 9.

Telephone Communications Are Terminated

16. The call is terminated when one of the parties hangs up or, in the case of prepaid call services, when either of the gateways determines that the account balance of the user has been exceeded.

17. Gateways A and B send DRQ messages to the their respective gatekeepers. The DRQ message contains the resulting billing information.
18. Gatekeepers A and B send disengage confirmation (DCF) messages to their respective gateways.

Communication Between the Gateways and the Gatekeepers Is Terminated

19. Gateways A and B send URQ messages to their respective gatekeepers.
20. Gatekeepers A and B send unregistration confirmation (UCF) messages to their respective gateways.

Downloading IVR Scripts

The Tool Command Language (TCL) IVR scripts are the default scripts for all Cisco voice features that use IVR.

The H.323 security and accounting enhancements described in this document require the use of one of the following IVR scripts:

- voip_auth_acct_pin_dest.tcl
- voip_auth_acct_pin_dest_2.tcl

Note For more information on TCL IVR applications, see the "Configuring TCL IVR Applications" chapter.

voip_auth_acct_pin_dest.tcl

The voip_auth_acct_pin_dest.tcl script does the following:

- Prompts the caller to enter an account number, PIN, and destination number. This information is provided to an H.323 gatekeeper, which authenticates and authorizes the call.

  If the caller is using a debit card account number, the following will occur:

  - The gatekeeper returns the remaining credit time amount.
  - The TCL script monitors the time remaining and, based on a configured value, plays a "time running out" message to the caller. The message (such as, "You have only 3 minutes remaining on your credit.") is played only to the calling party. The called party hears silence during this time. For example, if the configured time-out value is 3 minutes, the message is played when the caller has only 3 minutes of credit left.
  - The TCL script plays a warning message when the credit of the user has been exhausted. The message (such as, "Sorry, you have run out of credit.") is played only to the calling party. The called party hears silence during this time.

- Allows the caller to make subsequent calls to different destinations without disconnecting from the call leg. Thus, the caller is required to enter the account ID and PIN only once (during initial authorization). For making subsequent calls, the caller needs to enter only the destination number. After completing a call to one destination, the caller can disconnect the call by pressing the pound (#) key on the keypad and holding it down from 1 to 2 seconds. If the # key is pressed down for more than 1 second, it is treated as a long pound (#). The called party is disconnected, and the caller is prompted to enter a new destination number. Once a new destination number is entered, the call is authenticated and authorized using this number and the previously provided account number and PIN.

  This feature also allows the caller to continue making additional calls if the called party hangs up.

- Reauthenticates and authorizes each new call. Each time a caller enters a new destination number, the TCL script reauthenticates or authorizes the call with the gatekeeper and, if the caller is using a debit card account, obtains the remaining credit time information.
- Allows the caller to enter the necessary information without having to hear all or any of the prompts. The TCL script will stop playing (or will not begin playing) the prompt if it detects that the caller wants to enter the information without listening to the prompt.

Note The normal terminating character for the account number, PIN, and destination number is the pound (#) key.

- Allows the caller to interrupt announcements by pressing the touch tone key. This TCL script stops playing announcements when the system detects that the caller has pressed any touch tone key.
- Allows the caller to interrupt partially entered numbers and restart from the beginning by pressing a designated key on the keypad. The asterisk (*) key is configured as the interrupt key in the TCL script. The caller can use the asterisk key to cancel an entry and then reenter the account number, PIN, or destination number. The caller is allowed to re-enter a field only a certain number of times. The number of retries may be configured. The default is three times.
- Can terminate a field by size instead of the terminating character (#). The TCL script allows a specified number of digits to be entered in the account number and PIN fields. This means that the caller can type all the digits (without the terminating character) and the script determines how to extract different fields from the number strings. If the caller uses the terminating character, the terminating character takes precedence and the fields are extracted accordingly.
- Supports two languages. The IVR script supports two languages, which must be similar in syntax. The languages must be similar in the manner in which numbers are constructed—especially for currency, amount, and time. All the prompts are recorded and stored in both languages. The language selection is made when the caller presses a predefined key in response to a prompt (such as, “For English, press 1. For Spanish, press 2.”). The TCL script uses the selected language until the caller disconnects.

voip_auth_acct_pin_dest_2.tcl

The voip_auth_acct_pin_dest_2.tcl script is a simplified version of the voip_auth_acct_pin_dest.tcl script. It prompts the caller for an account number followed by a PIN. The caller is then prompted for a destination number. This information is provided to the H.323 gatekeeper that authenticates and authorizes the call. This script provides prompts only in English.

If the caller is using a debit account number, it plays a “time running out” message when the caller has 10 seconds of credit time remaining. It also plays a “time has expired” message when the credit of the caller has been exhausted.

H.235 Gateway Security Configuration Tasks

To use the H.235 security features for routing H.323 calls as illustrated above, do the following:

- Enable H.323 security on the gateway.
- Download the appropriate TCL IVR scripts from the Cisco Connection Online Software Support Center. The URL to this site is as follows:

  http://www.cisco.com/cgi-bin/tablebuild.pl/tclware
- Configure the IVR inbound dial peer on the gateway router.

To enable security on the gateway, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gateway`	Enters gateway configuration mode.
Step 2	`Router(config-gateway)# security password` *password* `level {endpoint | per-call | all}`	Enables security and specifies the level of validation to be performed. The keywords and arguments are as follows: • *password*—Specifies the gateway password. • **endpoint**—Specifies that validation be performed on all RAS messages sent by the gateway using the cryptoTokens that are generated based on the security password configured for the gateway. • **per-call**—Specifies that validation be performed only on the admission messages from the H.323 endpoints to the gateway ARQ messages). The gateway prompts the user for an account number and PIN. These two numbers are sent from the endpoint and are used to authenticate the originator of the call. • **all**—This option is a combination of the **endpoint** and **per-call** options. Specifies that validation be performed on all RAS messages sent by the gateway. The validation of cryptoTokens in ARQ messages is based on the account number and PIN of the user making the call, and the validation of cryptoTokens sent in all other RAS messages is based on the password configured for the gateway.
Step 3	`Router(config-gateway)# exit`	Exits gateway configuration mode.
Step 4	`Router(config)# dial-peer voice` *tag* `pots`	Enters the dial-peer configuration mode to configure a POTS dial peer. The *tag* value of the dial-peer voice POTS command uniquely identifies the dial peer. Valid entries are from 1 to 2,147,483,647.
Step 5	`Router(config-dial-peer)# call application voice` *application-name location {word}*	Enters the command to initiate the IVR application and the selected TCL application name. Enter the application name and the location where the TCL IVR script is stored. The arguments are as follows: • *application-name*—Specifies the character string that defines the name of the application. • *location*—Specifies the location of the TCL file in URL format. Valid storage locations are TFTP, FTP, and Flash. • *word*—Specifies the text string that defines an attribute-value (AV) pair specified by the TCL script and understood by the RADIUS server.
Step 6	`Router(config-dial-peer)# destination-pattern [+]`*string*`[T]`	Specifies the E.164 address associated with this dial peer. For an explanation of the keywords and arguments, see Step 2 of the configuration table in the "Configuring Gateway RAS" section on page 252.

	Command	Purpose
Step 7	**Cisco AS5300 Universal Access Server** `Router(config-dial-peer)# port controller number:D`	Configures the voice port associated with this dial peer. • *controller number*—Specifies the T1 or E1 controller. • **:D**—Indicates the D channel associated with the ISDN PRI. **Note** The syntax of the **port** command is specific to Cisco hardware platforms. For information on how to configure this command for a specific device, refer to the **port** command documentation in the *Cisco IOS Voice, Video, and Fax Command Reference*.

Verifying H.235 Gateway Security Configuration

To display the security password and level when it is enabled, use the **show running-config** command. By default, security is disabled.

```
Router# show running-config
security password 151E0A0E level all
```

Configuring Alternate Gatekeeper Support

An alternate gatekeeper provides redundancy for a gateway in a system in which gatekeepers are used. A gateway may use up to two alternate gatekeepers as a backup in the case of a primary gatekeeper failure.

A gatekeeper manages H.323 endpoints in a consistent manner, allowing them to register with the gatekeeper and to locate another gatekeeper. The gatekeeper provides logic variables for proxies or gateways in a call path to provide connectivity with the Public Switched Telephone Network (PSTN), to improve quality of service (QoS), and to enforce security policies. Multiple gatekeepers may be configured to communicate with one another, either by integrating their addressing into the DNS or by using Cisco IOS configuration options.

Alternate gatekeeper support has the following restrictions:

- This feature can be used only with a gatekeeper that supports the alternate gatekeeper functionality.
- The timer/retry number of RAS messages remains internal to the gateway as currently implemented. This feature does not include commands to allow tuning of these parameters.
- The alternate gatekeeper list is volatile—when the gateway loses power or is reset or reloaded, the alternate gatekeeper list that has been acquired from the gatekeeper is lost.

Gatekeeper Clustering

With gatekeeper clustering there is the potential that bandwidth may be overcommitted in a cluster. For example, suppose that there are five gatekeepers in a cluster and that they share 10 Mbps of bandwidth. Suppose that the endpoints registered to those alternates start placing calls quickly. It is possible that within a few seconds, each gatekeeper could be allocating 3 Mbps of bandwidth if the endpoints on each of the gatekeepers request that much bandwidth. The net result is that the bandwidth consumed in the cluster is 15 Mbps.

The alternate gatekeeper was purposely designed to restrict bandwidth because there is no clear way to sync bandwidth information quickly and efficiently. To work around this problem, "announcement" messages were restricted to intervals as small as 10 seconds. If the gatekeepers get into a situation in which endpoints request bandwidth rapidly, the problem will be discovered and corrective action will take place within at least 10 seconds. Assuming that the gatekeepers are probably not all synchronized on their timers, the announcement messages from the various gatekeepers are likely to be heard more quickly. Therefore, the problem will be less severe. The potential exists, however, for overcommitment of the bandwidth between announcement messages if the call volume increases substantially in a short amount of time (as small as 10 seconds).

Note If you monitor your bandwidth, it is recommended that you consider lowering the maximum bandwidth so that if "spikes" such as those described above do occur, some bandwidth will still be available.

To configure alternate gatekeeper support on a gateway, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface Ethernet 0/1`	Enters interface configuration mode for the selected Ethernet interface.
Step 2	`Router(config-if)# ip address`	Identifies the IP address of the Ethernet interface.
Step 3	`Router(config-if)# h323-gateway voip interface`	Identifies this interface as a Voice over IP (VoIP) gateway interface.
Step 4	`Router(config-if)# h323-gateway voip id` *gatekeeper-id* {**ipaddr** *ip-address* [*port-number*]| **multicast**} [**priority** *number*]	Identifies the gatekeeper for this gateway interface and sets the attributes. For an explanation of the keywords and arguments, see Step 6 in the "Identifying a Router Interface As an H.323 Gateway" section on page 250.
Step 5	`Router(config-if)# h323-gateway voip id` *gatekeeper-id* {**ipaddr** *ip-address* [*port-number*] | **multicast**} [**priority** *number*]	To identify the alternate gatekeeper, use the following keywords and arguments: • *gatekeeper-id*—Indicates the H.323 identification of the gatekeeper. This value must exactly match the gatekeeper identification (ID) in the gatekeeper configuration. The recommended format is *name.domain-name*. • **ipaddr**—Indicates that the gateway will use an IP address to locate the gatekeeper. • *ip-address*—Defines the IP address used to identify the gatekeeper. • *port-number*—(Optional) Defines the port number used. • **multicast**—Indicates that the gateway will use multicast to locate the gatekeeper. • **priority** *number*—(Optional) Specifies the priority of this gatekeeper. The range is 1 through 127, and the default value is 127.

	Command	Purpose
Step 6	`Router(config-if)# h323-gateway voip h323-id interface-id`	Identifies the H.323 ID of a particular H.323 endpoint, which in this case is the gateway. The *interface-id* argument is the H.323 name (ID) used by this gateway when this gateway communicates with its associated gatekeeper. Usually, this ID is the name of the gateway, with the gatekeeper domain name appended to the end: name@domain-name.

Verifying Configuration of the Alternate Gatekeeper

To see that there is an alternate gatekeeper configured, enter the **show gate** command

```
Alternate Gatekeeper List
    priority 126 id GK1 ipaddr 172.18.193.61 1719
    priority 127 id GK2 ipaddr 172.18.193.63 1719
```

Configuring Dual Tone Multifrequency Relay

Dual tone multifrequency (DTMF) is the tone generated on a touch-tone phone when the keypad digits are pressed. During a call, DTMF may be entered to access interactive voice response (IVR) systems, such as voice mail and automated banking services.

Although DTMF is usually transported accurately when using high-bit-rate voice codecs such as G.711, low-bit-rate codecs such as G.729 and G.723.1 are highly optimized for voice patterns and tend to distort DTMF tones. As a result, IVR systems may not correctly recognize the tones.

DTMF relay solves the problem of DTMF distortion by transporting DTMF tones “out of band,” or separate from the encoded voice stream.

For a more thorough explanation of DTMF relay, see the “H.323 Applications” chapter.

To configure DTMF relay on a gateway, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice tag voip`	Defines a Voice over IP (VoIP) dial peer and enters dial-peer configuration mode. The keywords and argument are as follows: • *tag*—Indicates the digit that defines a particular dial peer. Valid entries are from 1 to 2,147,483,647. • **voip**—Indicates that this is a VoIP peer using voice encapsulation on the POTS network. Use this keyword to configure DTMF relay.

	Command	Purpose
Step 2	`Router(config-dial-peer)# dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal]`	Forwards DTMF tones. The keywords are as follows: • **cisco-rtp**—(Optional) Forwards DTMF tones by using RTP with a Cisco proprietary payload type. • **h245-alphanumeric**—(Optional) Forwards DTMF tones by using the H.245 "alphanumeric" User Input Indication (UII) method. It supports tones 0 through 9, *, #, and A through D. Use this keyword to configure DTMF relay. • **h245-signal**—(Optional) Forwards DTMF tones by using the H.245 "signal" UII method. It supports tones 0 through 9, *, #, and A through D.
Step 3	`Router(config-dial-peer)# codec codec {clear-channel | g711alaw | g711ulaw | g723ar53 | g723ar63 | g723r53 | g723r63 | g726r16 | g726r24 |g726r32 | g726r53 | g726r63 |g728 | g729abr8 | g729ar8 | g729br8 | g729r8 | gsmefr | gsmfr} [bytes payload_size]`	Specifies the voice coder rate of speech for a dial peer. • The *codec* keywords are as follows: – **clear-channel**—Clear channel at 64,000 bits per second (bps). – **g711ala**—G.711 a-Law at 64,000 bits per second. – **g711ula**—G.711 u-Law at 64,000 bps. – **g723ar53**—G.723.1 Annex A at 5300 bps. – **g723ar63**—G.723.1 Annex A at 6300 bps. – **g723r53**—G.723.1 at 5300 bps. – **g723r63**—G.723.1 at 6300 bps. – **g726r16**—G.726 at 16,000 bps. – **g726r24**—G.726 at 24,000 bps. – **g726r32**—G.726 at 32,000 bps. – **g728**—G.728 at 16,000 bps. – **g729abr8**—G.729 Annex A and B at 8000 bps. – **g729ar8**—G729 Annex A at 8000 bps. – **g729br8**—G.729 Annex B at 8000 bps. – **g729r8**—G.729 at 8000 bps. This is the default codec. – **gsmefr**—Global System for Mobile Communications Enhanced Full Rate (GSMEFR) at 12,200 bps. – **gsmfr**—Global System for Mobile Communications Full Rate (GSMFR) at 13,200 bps.

	Command	Purpose
		• **bytes**—(Optional) Specifies the number of bytes in the voice payload of each frame. • *payload-size*—(Optional) The number of bytes in the voice payload of each frame. Refer to the **codec** (dial-peer) command table titled "Voice Payload-Per-Frame Options and Defaults" in the *Cisco IOS Voice, Video, and Fax Command Reference* for valid entries and default values.
Step 4	`Router(config-dial-peer)# destination-pattern [+]string[T]`	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number to be used for a dial peer (depending on the dial plan). For an explanation of the keywords and arguments, see Step 2 of the configuration task table in the "Configuring Gateway RAS" section on page 252.

Step 5	**Cisco 2600 and 3600 Series Routers**
	`Router(config-dial-peer)# session target {ipv4:destination-address | dns:[$s$. | $d$. | $e$. | $u$.] host-name | loopback:rtp | loopback:compressed | loopback:uncompressed}`
	Cisco AS5300 Universal Access Server
	`Route(config-dial-peer)# session target {ipv4:destination-address | dns:[$s$. | $d$. | $e$. | $u$.] host-name | loopback:rtp | loopback:compressed | loopback:uncompressed | mailto:{name | $d$.}@domain-name}`
		Specifies a network-specific address for a specified dial peer or destination gatekeeper.
		Keywords and arguments are as follows:
		Cisco 2600 and 3600 Series Routers
		• **ipv4:***destination-address*—IP address of the dial peer.
		• **dns:***host-name*—Indicates that the DNS will be used to resolve the name of the IP address. Valid entries for this parameter are characters representing the name of the host device. (Optional) You can use one of the following four wildcards with this keyword when defining the session target for VoIP peers:
		– **s.**—Indicates that the source destination pattern will be used as part of the domain name.
		– **d.**—Indicates that the destination number will be used as part of the domain name.
		– **e.**—Indicates that the destination pattern is used as part of the domain name in reverse dotted format for tpc.int DNS format. For example, if the destination number is 310 555-1234 and the session target is configured as e.cisco.com, the translated DNS name will be 4.3.2.1.5.5.5.0.1.3.cisco.com**.**
		– **u.**—Indicates that the unmatched portion of the destination pattern (such as a defined extension number) will be used as part of the domain name.
		• **loopback:rtp**—Indicates that all voice data will be looped back to the originating source. This is applicable for VoIP peers.

Command	Purpose
	• **loopback:compressed**—Indicates that all voice data will be looped back in compressed mode to the originating source. This is applicable for POTS peers. • **loopback:uncompressed**—Indicates that all voice data will be looped back in uncompressed mode to the originating source. This is applicable for POTS peers. **Cisco AS5300 Universal Access Server** In addition to the above, the following keywords and arguments apply to the Cisco AS5300 universal access server: • **mailto:***name*—Specific recipient e-mail address, name, or mailing list alias. • **@***domain-name*—Specifies the appropriate domain name associated with the e-mail address.

Configuring FXS Hookflash Relay

A "hookflash" indication is a brief on-hook condition during a call. The indication is not long enough in duration to be interpreted as a signal to disconnect the call.

PBXs and telephone switches are frequently programmed to intercept hookflash indications and use them as a way to allow a user to invoke supplemental services. In a traditional telephone network, a hookflash results in a voltage change on the telephone line. Because there is no equivalent of this voltage change in an IP network, a message may be sent over the IP network that represents a hookflash. To send a hookflash indication using this message, an H.323 endpoint sends an H.245 user input indication message that contains an "H.245-signal" or "H.245-alpha" structure.

Hookflash relay is supported on the Cisco 2600, 3600, and 7200 series routers and on the MC3810 multiservice concentrator.

For a further explanation of configuring hookflash relay, see the "H.323 Applications" chapter.

To configure hookflash relay on a gateway, use the following commands beginning in global configuration mode:

Note Hookflash relay is enabled only when the **dtmf-relay h245-signal** command is configured on the applicable VoIP dial peers. Hookflash is relayed using an h245-signal indication and can be sent only when an h245-signal is available.

	Command	Purpose

Step 1	**Cisco 2600 and 3600 Series Routers**
	`Router(config)# voice-port {slot-number/subunit-number/port} | {slot/port:ds0-group-no}`
	
	Cisco 7200 Series Routers
	`Router(config)# voice-port {slot/port:ds0-group-no} | {slot-number/subunit-number/port}`
	
	Cisco MC3810 Multiservice Concentrator
	`Router(config)# voice-port slot/port`
		Enters voice-port configuration mode.
		
		The keywords and arguments are as follows:
		
		Cisco 2600 and 3600 Series Routers
		• *slot-number*—Specifies the slot number in the Cisco router in which the voice interface card is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed.
		• *subunit-number*—Specifies the subunit on the voice interface card in which the voice port is located. Valid entries are 0 or 1.
		• *port*—Indicates the voice port. Valid entries are 0 or 1.
		• *slot*—Specifies the router location in which the voice port adapter is installed. Valid entries are from 0 to 3.
		
		Cisco 7200 Series Routers
		• *slot*—Specifies the router location in which the voice port adapter is installed. Valid entries are from 0 to 3.
		• *port*—Indicates the voice interface card location. Valid entries are 0 or 1.*ds0-group-no*—Defines DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.
		• *slot-number*—Indicates the slot number in the Cisco router in which the voice interface card is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed.
		• *subunit-number*—Indicates the subunit on the voice interface card in which the voice port is located. Valid entries are 0 or 1.
		• *port*—Indicates the voice port number. Valid entries are 0 or 1.
		
		Cisco MC3810 Multiservice Concentrator
		• *slot*—Specifies the slot number in the Cisco router in which the voice interface card is installed. The only valid entry is 1.
		• *port*—Specifies the voice port number. Valid ranges are as follows:
		– Analog voice ports: from 1 to 6.
		– Digital T1: from 1 to 24.
		– Digital E1: from 1 to 15 and from 17 to 31.

	Command	Purpose
Step 2	`Router(config-voice-port)# timing hookflash-input duration`	Specifies the maximum duration of a hookflash indication. If the hookflash lasts longer than the specified limit, the Foreign Exchange Station (FXS) interface processes the indication as an on-hook. The *duration* is shown in milliseconds. Possible values are 50 through 1550. The default value is 600 milliseconds.
Step 3	`Router(config-voice-port)# timing hookflash-out duration`	Specifies the duration, in milliseconds, of the hookflash indications that the gateway generates on a Foreign Exchange Office (FXO) interface. Valid entries are from 50 through 1550 milliseconds. The default is 400 milliseconds.

Configuring Multiple Codecs

Normally only one codec is specified when a dial peer is configured on a gateway. However, a prioritized list of codecs can be configured to increase the probability of establishing a connection between endpoints during the H.245 exchange phase. For more information about configuring multiple codecs, see the "Codec Negotiation" section in the "H.323 Applications" chapter.

To configure multiple codecs for a dial peer, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# voice class codec tag`	Enters voice class configuration mode and assigns an identification tag number for a codec voice class. The *tag* argument is the unique number assigned to the voice class. The valid range is from 1 to 10,000. Each tag number must be unique on the router.
Step 2	`Router(config-class)# codec preference value codec-type [bytes payload-size]`	Adds codecs to the prioritized list of codecs. The keywords and arguments are as follows: • *value*—Specifies the order of preference, with 1 being the most preferred and 12 being the least preferred. • *codec-type*—Specifies the type of codec preferred. Types are as follows: – **clear-channel**—Clear channel at 64,000 bps. – **g711alaw**—G.711a-Law at 64,000 bps. – **g711ulaw**—G.711 u-Law at 64,000 bps. – **g723ar53**—G.723.1 Annex-A at 5300 bps. – **g723ar63**—G.723.1 Annex-A at 6300 bps. – **g723r53**—G.723.1 at 5300 bps. – **g723r63**—G.723.1 at 6300 bps. – **g726r16**—G.726 at 16,000 bps. – **g726r24**—G.726 at 24,000 bps.

		– **g726r32**—G.726 at 32,000 bps. – **g728**—G.728 at 16,000 bps.**g729abr8**—G.729 Annex-A and B at 8000 bps. – **g729br8**—G.729 Annex-B at 8000 bps. – **g729r8**—G.729 at 8000 bps. This is the default codec. – **gsmefr**—Global System for Mobile Communications Enhanced Full Rate (GSMEFR) at 12,200 bps. – **gsmfr**—Global System for Mobile Communications Full Rate (GSMFR) at 13,200 bps. • **bytes**—(Optional) Specifies that the size of the voice frame is in bytes. – *payload-size*—(Optional) Number of bytes that you specify as the voice payload of each frame. Values depend on the codec type and the packet voice protocol.
Step 3	`Router(config-class)# exit`	Exits voice class configuration mode.
Step 4	`Router(config)# dial-peer voice` *tag* `voip`	Enters dial-peer configuration mode to configure a VoIP peer. The *tag* value of the **dial-peer voice** VoIP command uniquely identifies the dial peer. (This number has local significance only.)
Step 5	`Router(config-dial-peer)# voice-class codec` *tag*	The *tag* is the unique number assigned to the voice class. The valid range for this tag is from 1 to 10,000. The tag number maps to the tag number created using the **voice class codec** global configuration command.

Verifying Multiple Codecs Configuration

To show the codecs defined for a particular prioritized list of codecs, use the **show running-config** command.

Configuring Rotary Calling Pattern

Rotary calling pattern routes an incoming call that arrives over a telephony interface back out through another telephony interface under certain circumstances. Rotary calling pattern primarily provides reliable service during network failures. Call establishment using rotary calling pattern is supported by rotary group support of dial peers, where multiple dial peers may match a given destination phone number and be selected in sequence. In addition, if the destinations need to be tried in a certain order, preference may be assigned. Use the **preference** command when configuring the dial peers to reflect the preferred order (0 being the highest preference and 10 the lowest).

If several dial peers match a particular destination pattern, the system attempts to place a call to the dial peer configured with the highest preference. If the call cannot be completed because of a system outage (for example, the gatekeeper or gateway cannot be contacted), the rotary call pattern performs the following tasks:

- Lists all the conditions under which this instance occurs.
- Retries the call to the next highest preference dial peer.
- Continues until no more matching dial peers are found.

If there are equal priority dial peers, the order is determined randomly.

Note The hunting algorithm precedence may be configured. See the **preference** command discussed in the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter.

Configuring H.323 Support for Virtual Interfaces

H.323 support for virtual interfaces allows the IP address of the gateway to be configured so that the IP address included in the H.323 packet is always the source IP address of the gateway, regardless of the physical interface and protocol used. This single-address feature allows firewall applications to be easily configured to work with H.323 messages.

To configure a source IP address for a gateway, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface type slot/port`	Enters interface configuration mode to configure parameters for the specified interface. The keywords and arguments are as follows: • *type*—Indicates the type of interface. • *slot*—Specifies the number of the slot being configured. • *port*—Specifies the number of the port being configured. **Note** This syntax will vary, depending on the platform.
Step 2	`Router(config-if)# h323-gateway voip bind srcaddr ip-address`	Sets the source IP address to be used for this gateway. The *ip-address* argument specifies the IP address to be used for outgoing H.323 traffic, which includes H.225, H.245, and RAS messages. Typically, this is the IP address assigned to the Ethernet interface.

Verifying the Source IP Address of the Gateway

To verify the source IP address of the gateway, enter the **show running-config** command. The output shows the source IP address that is bound to the interface.

```
router# show running-config

interface Loopback0
 ip address 10.0.0.0 255.255.255.0
 no ip directed-broadcast
 h323-gateway voip bind srcaddr 10.0.0.0
!
interface Ethernet0/0
 ip address 172.18.194.50 255.255.255.0
 no ip directed-broadcast
 h323-gateway voip interface
 h323-gateway voip id j70f_2600_gk2 ipaddr 172.18.194.53 1719
 h323-gateway voip h323-id j70f_3640_gw1
 h323-gateway voip tech-prefix 3#
.
.
.
```

In the following example, Ethernet interface 0/0 is used as the gateway interface. For convenience, the **h323-gateway voip bind srcaddr** command has been specified on the same interface. The designated source IP address is the same as the IP address assigned to the interface.

```
interface Ethernet0/0
 ip address 172.18.194.50 255.255.255.0
 no ip directed-broadcast
 h323-gateway voip interface
 h323-gateway voip id j70f_2600_gk2 ipaddr 172.18.194.53 1719
 h323-gateway voip h323-id j70f_3640_gw1
 h323-gateway voip tech-prefix 3#
 h323-gateway voip bind srcaddr 172.18.194.50
```

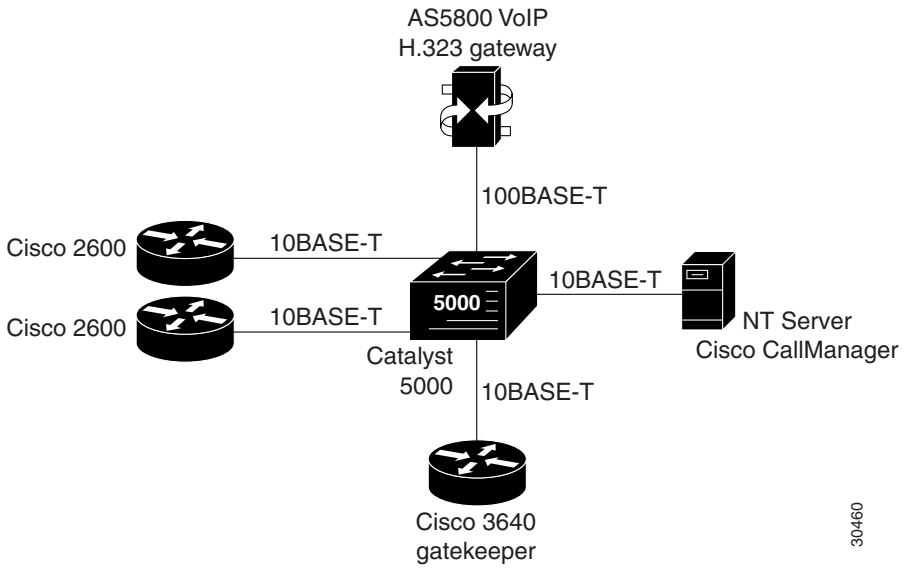
H.323 Gateway Configuration Examples

This section includes the following gateway configuration examples:

H.323 Gateway RAS Configuration Example

Figure 56 shows a Cisco 2600 router and a Cisco AS5800 universal access server as gateways and a Cisco 3640 router as a gatekeeper.

Figure 56 VoIP for the Cisco AS5800



The following example shows a Cisco AS5800 universal access server configured as a gateway using RAS:

```
! Configure the T1 controller. (This configuration is for a T3 card.)
controller T1 1/0/0:1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
! Configure POTS and VoIP dial peers.
dial-peer voice 11111 pots
 incoming called-number 12345
 destination-pattern 9#11111
 direct-inward-dial
 port 1/0/0:1:D
 prefix 11111
!
dial-peer voice 12345 voip
 destination-pattern 12345
 tech-prefix 6#
 session target ras
!
! Enable gateway functionality.
gateway
!
! Enable Cisco Express Forwarding.
ip cef
!
! Configure and enable the gateway interface.
interface FastEthernet0/3/0
 ip address 172.16.0.0.255.255.255.0
 no ip directed-broadcast
 no keepalive
```

```
 full-duplex
 no cdp enable
h323-gateway voip interface
 h323-gateway voip id gk3.gg-dn1 ipaddr 172.18.0.0 1719
 h323-gateway voip h323-id gw3@gg-dn1
 h323-gateway voip tech-prefix 9#
!
! Configure the serial interface.(This configuration is for a T3 serial interface.)
interface Serial1/0/0:1:23
 no ip address
 no ip directed-broadcast
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
```

AAA Functionality on the Gateway Configuration Example

The following example shows AAA functionality configured on a Cisco AS5300 universal access server.

```
version 12.2
no service single-slot-reload-enable
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service tcp-small-servers
!
hostname doc-rtr53-05

aaa new-model
aaa authentication login default local
aaa authentication login NO_AUTHENT none
aaa authentication login h323 group radius
aaa authentication ppp default if-needed local
aaa authorization exec default local if-authenticated
aaa authorization exec NO_AUTHOR none
aaa authorization commands 15 default local if-authenticated
aaa authorization commands 15 NO_AUTHOR none
aaa accounting exec default start-stop group tacacs+
aaa accounting exec NO_ACCOUNT none
aaa accounting commands 15 default stop-only group tacacs+
aaa accounting commands 15 NO_ACCOUNT none
aaa accounting connection h323 start-stop group radius
enable secret 5 $1$l545$V4haZZN8AOKem8T1DhF5i/
enable password 7 060506324F41
!
resource-pool disable
!
call rsvp-sync
ip subnet-zero
no ip source-route
no ip finger
ip domain-name the.net
ip name-server 172.22.53.210
ip name-server 172.19.23.12
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
```

```
controller T1 1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 3
 framing esf
 clock source line secondary 3
 linecode b8zs
 pri-group timeslots 1-24
!
gw-accounting h323
gw-accounting voip
translation-rule 1
 Rule 1 408555.... 5
 Rule 2 650 5
!
interface Loopback0
 ip address 172.21.10.10 255.255.255.255
!
interface Loopback1
 ip address 172.21.104.254 255.255.255.0
!
interface Ethernet0
 no ip address
 shutdown
!
interface Virtual-Template1
 description Template for Multilink Users
 ip unnumbered Loopback1
 no logging event link-status
 no snmp trap link-status
 peer default ip address pool addr-pool
 ppp authentication chap
 ppp multilink
!
interface Serial0:23
 description description Headquarters 324-1937 active PRI line
 no ip address
 no logging event link-status
 no snmp trap link-status
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 fair-queue 64 256 0
 no cdp enable
!
interface Serial1:23
 no ip address
 no logging event link-status
 no snmp trap link-status
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 fair-queue 64 256 0
 no cdp enable
!
interface Serial2:23
 no ip address
 no logging event link-status
 no snmp trap link-status
```

```
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 fair-queue 64 256 0
 no cdp enable
!
interface Serial3:23
 no ip address
 no logging event link-status
 no snmp trap link-status
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 fair-queue 64 256 0
 no cdp enable
!
interface FastEthernet0
 ip address 172.21.101.23 255.255.255.0
 duplex auto
 speed auto
!
radius-server host 10.10.10.10 auth-port 1612 acct-port 1616
radius-server retransmit 3
radius-server key 7 00071C080A520E
!
dial-peer voice 1 pots
!
dial-peer voice 2 voip
 destination-pattern +1234...
 session target ipv4:10.1.1.1
!
dial-peer voice 3 voip
 destination-pattern 555*
 session target ipv4:10.1.1.2
!
dial-peer voice 4 voip
 destination-pattern 555
 session target ipv4:10.1.2.2
!
dial-peer voice 90 voip
 destination-pattern 555.%
 session target ipv4:10.1.2.2
!
dial-peer voice 50 voip
 destination-pattern 408555%
 session target ipv4:10.1.1.2
!
dial-peer voice 55 voip
 destination-pattern 408555.%
 session target ipv4:10.2.2.2
!
line con 0
 exec-timeout 0 0
 authorization commands 15 NO_AUTHOR
 authorization exec NO_AUTHOR
 login authentication NO_AUTHENT
 transport input none
line 1 48
 autoselect during-login
 autoselect ppp
 modem InOut
 transport preferred none
 transport output telnet
line aux 0
line vty 0 4
 password 7 03470A1C140635495C
```

```
 transport preferred none
 transport input telnet
 transport output telnet
!
!
!ntp clock-period 17180261
ntp update-calendar
ntp server 172.22.255.1 prefer
```

H.323 Gateway Security Configuration Example

The following example illustrates H.323 security configuration on a Cisco AS5300 gateway.

```
hostname um5300
!
enable password xyz
!
resource-pool disable
!
clock timezone EST -5
clock summer-time EDT recurring
ip subnet-zero
no ip domain-lookup
!
isdn switch-type primary-5ess
isdn voice-call-failure 0
call application voice xyz tftp://172.18.16.2/samp/xyz.tcl
call application voice load xys
mta receive maximum-recipients 1024
!
xgcp snmp sgcp
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary 1
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2
!
controller T1 3
!
voice-port 0:D
!
voice-port 1:D
!
dial-peer voice 4001 pots
 application xyz
 destination-pattern 4003
 port 0:D
 prefix 4001
!
dial-peer voice 513 voip
 destination-pattern 1513200....
 session target ras
!
```

```
dial-peer voice 9002 voip
 destination-pattern 9002
 session target ras
!
dial-peer voice 4191024 pots
 destination-pattern 4192001024
 port 0:D
 prefix 4001
!
dial-peer voice 1513 voip
 destination-pattern 1513.......
 session target ras
!
dial-peer voice 1001 pots
 destination-pattern 14192001001
 port 0:D
!
gateway
 security password 151E0A0E level all
!
 interface Ethernet0
 ip address 10.99.99.7 255.255.255.0
 no ip directed-broadcast
 shutdown
!
interface Serial0:23
 no ip address
 no ip directed-broadcast
 isdn switch-type primary-5ess
 isdn protocol-emulate user
 isdn incoming-voice modem
 fair-queue 64 256 0
 no cdp enable
!
interface Serial1:23
 no ip address
 no ip directed-broadcast
 isdn switch-type primary-5ess
 isdn protocol-emulate user
 isdn incoming-voice modem
 isdn guard-timer 3000
 isdn T203 10000
 fair-queue 64 256 0
 no cdp enable
!
interface FastEthernet0
 ip address 172.18.72.121 255.255.255.192
 no ip directed-broadcast
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id um5300@vgkcisco3 ipaddr 172.18.72.58 1719
 h323-gateway voip h323-id um5300
 h323-gateway voip tech-prefix 1#
!
no ip http server
ip classless
ip route 10.0.0.0 172.18.72.65
!
!
line con 0
 exec-timeout 0 0
 length 0
 transport input none
```

```
line aux 0
line vty 0 4
 password xyz
 login
!
ntp clock-period 17179974
ntp server 172.18.72.124
```

H.235 Security Example

The following example shows output from configuring secure registrations from the gatekeeper and identifying which RAS messages the gatekeeper will check to find authentication tokens:

```
dial-peer voice 10 voip
 destination-pattern 4088000
 session target ras
 dtmf-relay h245-alphanumeric
!
gateway
 security password 09404F0B level endpoint
```

The following example shows output from configuring which RAS messages will contain gateway generated tokens:

```
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
radius-server host 10.25.0.0 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server deadtime 5
radius-server key lab
radius-server vsa send accounting
!
gatekeeper
 zone local GK1 test.com 10.0.0.3
 zone remote GK2 test2.com 10.0.2.2 1719
 accounting
 security token required-for registration
 no use-proxy GK1 remote-zone GK2 inbound-to terminal
 no use-proxy GK1 remote-zone GK2 inbound-to gateway
 no shutdown
```

Alternate Gatekeeper Configuration Example

In the following example, the gateway is configured to have alternate gatekeepers. The primary and secondary gatekeepers are configured with the priority option. The priority range is 1 through 127. The first alternate gatekeeper has been configured as priority 120; the second alternate gatekeeper has not been configured, so it remains at the default setting of 127.

```
interface Ethernet 0/1
 ip address 172.18.193.59 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK1 ipaddr 172.18.193.65 1719 priority 120
 h323-gateway voip id GK2 ipaddr 172.18.193.66 1719
 h323-gateway voip h323-id cisco2
```

DTMF Relay Configuration Example

The following example shows DTMF relay configured on a gateway.

```
dial-peer voice 1 voip
 dtmf-relay h245-alphanumeric
 codec g723r53
 destination-pattern 5....
 session target ipv4:192.168.100.2
```

FXS Hookflash Relay Configuration Example

The following example shows how to implement hookflash-in and hookflash-out timing for the hookflash after voice port 1/0/0 has been configured.

```
voice-port 1/0/0
 timing hookflash-in 200
 timing hookflash-out 200
```

Multiple Codec Configuration Example

The following configuration shows how to create a list of prioritized codecs and apply that list to a specific VoIP dial peer:

```
 voice class codec 99
  codec preference 1 g711alaw
  codec preference 2 g711ulaw bytes 80
  codec preference 3 g723ar53
  codec preference 4 g723ar63 bytes 144
  codec preference 5 g723r53
  codec preference 6 g723r63 bytes 120
  codec preference 7 g726r16
  codec preference 8 g726r24
  codec preference 9 g726r32 bytes 80
  codec preference 10 g728
  codec preference 11 g729br8
  codec preference 12 g729r8 bytes 50
!
dial-peer voice 1919 voip
  voice-class codec 99
```

Rotary Calling Pattern Configuration Example

The following example configures POTS dial peer 10 for a preference of 1, POTS dial peer 20 for a preference of 2, and Voice over Frame Relay dial peer 30 for a preference of 3:

```
dial-peer voice 10 pots
 destination pattern 5552150
 preference 1

dial-peer voice 20 pots
 destination pattern 5552150
 preference 2

dial-peer voice 30 vofr
 destination pattern 5552150
 preference 3
```

H.323 Support for Virtual Interfaces Configuration Example

In the following example, Ethernet interface 0/0 is used as the gateway interface. For convenience, the **h323-gateway voip bind srcaddr** command has been specified on the same interface. The designated source IP address is the same as the IP address assigned to the interface.

```
interface Ethernet0/0
 ip address 172.18.194.50 255.255.255.0
 no ip directed-broadcast
 h323-gateway voip interface
 h323-gateway voip id j70f_2600_gk2 ipaddr 172.18.194.53 1719
 h323-gateway voip h323-id j70f_3640_gw1
 h323-gateway voip tech-prefix 3#
 h323-gateway voip bind srcaddr 172.18.194.50
```