



Text Part Number:

# Cisco H.323 Gateway Security and Accounting Enhancements

---

This document provides information about the H.323 security and accounting enhancements that have been made to the Cisco H.323 Gateway. It includes the following sections:

- Overview of the Enhancements, page 1
- How the Enhancements Can Be Used, page 3
- Configuring Security on the Gateway, page 5
- Command Reference, page 10
- Changes to RAS Messages, page 15
- Related Documentation, page 18
- Glossary, page 18
- Cisco Connection Online, page 19
- Documentation CD-ROM, page 20

## Overview of the Enhancements

The security and accounting enhancements described in this document provide an alternative means for securing H.323 calls. In previous releases of Cisco IOS software, the security and accounting functions for H.323 calls used RADIUS and Authentication, Authorization, and Accounting (AAA). The enhancements described in this document add H.235-based security, in which H.323 calls are authenticated, authorized, and routed by a Gatekeeper. The Gatekeeper is considered a known and trusted entity.

These new enhancements can be used in conjunction with AAA. You can configure the Gateway to use the Gatekeeper for call authentication/authorization and use AAA for call accounting.

---

**Note** The enhancements described in this document are separate from and should not be confused with the standard Interactive Voice Response (IVR) and Authentication, Authorization, and Accounting (AAA) features used to authenticate inbound calls, or the settlement functions provided by the Open Settlements Protocol.

---

---

### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

Copyright © 1998  
Cisco Systems, Inc.  
All rights reserved.

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

The H.323 security and accounting enhancements include support for the following:

- H.235 Security, with support limited to subscription-based, Message Digest 5 (MD5), hashing-with-password authentication.
- 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).

## H.235 Security

The Cisco H.323 Gateway now supports the use of CryptoH323Tokens for authentication. The CryptoH323Token is defined in H.225 Version 2 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 and is used to authenticate the sender of the message. You can use a separate database for user ID and password verification.

With this release, Cisco H.323 Gateways support three levels of authentication:

- **Endpoint**—The RAS channel used for gateway-to-gatekeeper signalling 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.
- **Per-Call**—When the gateway receives a call over the telephony leg, it prompts the user for an account number and personal identification number (PIN). These two numbers are included in certain RAS messages sent from the endpoint and are used 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 ARQ messages is based on an the account number and PIN of the user making a call and the validation of cryptoTokens sent in all the other RAS messages is based on the password configured for the Gateway.

You can configure the level of authentication for the gateway using the Cisco IOS software command line interface. For more information, see the “security Command” section.

CryptoTokens for registration requests (RRQ), unregistration request (URQ), disengage request (DRQ) and the terminating side of admission request (ARQ) messages contain information about the Gateway that generated the token, including the gateway ID (which is the H.323 ID configured on the Gateway) and the gateway password. CryptoTokens for the originating side ARQ messages contain information about the user that is placing the call, including the user ID and personal identification number (PIN).

## Settlement

To enhance the accounting capabilities of the Cisco H.323 Gateway, fields have been added to the RAS messages. 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 Metering

To support prepaid calls, the Cisco H.323 Gateway monitors prepaid account balances and terminates a call if the account is exceeded.

## Prerequisites

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

- These enhancements use H.235. Because H.235 is a broad standard, you must ensure that your 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, you must ensure that your gatekeeper is able to handle this information.

For more information about specific gatekeepers that can be used with these H.323 security and accounting enhancements, see <http://von.cisco.com/interoperability/>.

## How the Enhancements Can Be Used

The H.323 security and accounting enhancements are designed to support a variety of situations where some form of authentication or tracking is required. The security enhancements allow you to control access through the use of a userID-password database. The accounting enhancements allow you to track call usage at both the origin and destination.

---

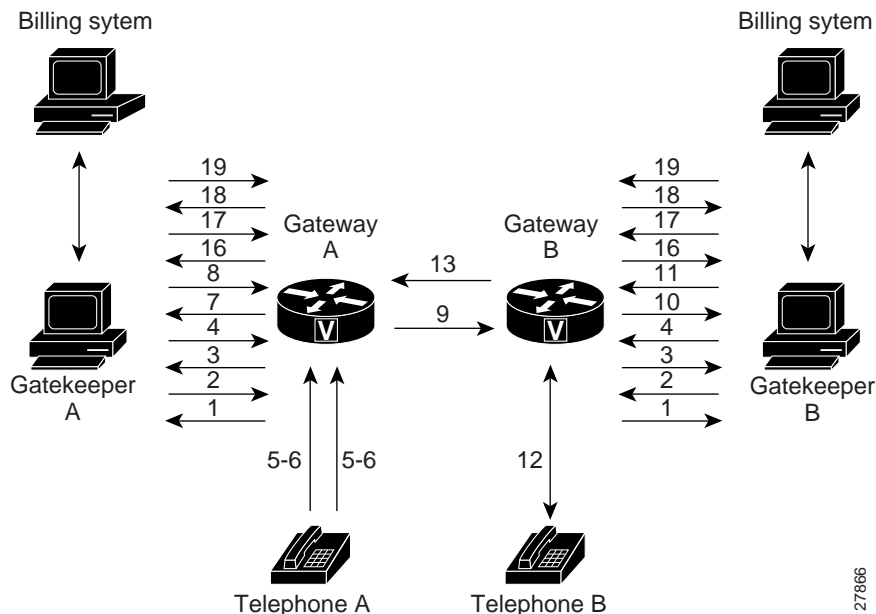
**Note** Because the authentication information includes a timestamp, it is important that all the Cisco H.323 Gateways and the Gatekeepers (or other entity that is performing the authentication) be synchronized. The Cisco H.323 Gateways must be synchronized using the Network Time Protocol (NTP).

---

One use of these features is in the area of prepaid calling services, where a customer must enter an account number and PIN and the duration of the call is tracked against the customer's remaining credit.

Figure 1 illustrates flow of a possible scenario in which H.323 security and accounting features are used.

**Figure 1 Flow for a Call Requiring H.323 Security and Accounting Features**



In this example, the user at Telephone A is attempting to establish a phone call to the user at Telephone B.

**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.  
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.
- 3 Gateways A and B send registration request (RRQ) messages to their respective Gatekeepers. The RRQ message includes authentication information in the cryptoToken field.
- 4 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**

- 5 Telephone A establishes a connection with Gateway A.
- 6 Gateway A initiates the IVR script to obtain the user’s account number and PIN, as well as the desired destination telephone number.
- 7 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 our scenario, it

is the source Gateway that is requesting admission. Therefore, the ARQ message includes the user's account and PIN. This information is encrypted using MD5 hashing and is included in the `cryptoTokens` field.

- 8 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 user's billing information (such as a reference ID and current account balance, for prepaid call services) and an access token.
- 9 Gateway A sends a Setup message to Gateway B. The setup message also includes the access token.
- 10 Gateway B sends an ARQ message to Gatekeeper B. The ARQ message includes the access token received from Gateway A.
- 11 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 ARJ message to Gateway B with a reject reason of `securityDenial`.
- 12 Gateway B initiates a call to the destination telephone.
- 13 When the destination telephone is answered, Gateway B sends a Connect message to Gateway A.
- 14 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 user's account balance, which was included in the ACF message sent in step 8.

#### Telephone Communications Are Terminated

- 15 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 user's account balance has been exceeded.
- 16 Gateways A and B send disengage request (DRQ) messages to their respective Gatekeepers. The DRQ message contains the resulting billing information.
- 17 Gatekeepers A and B send disengage confirmation (DCF) messages to their respective Gateways.

#### Communication Between the Gateways and the Gatekeepers is Terminated

- 18 Gateways A and B send unregistration request (URQ) messages to their respective Gatekeepers.
- 19 Gatekeepers A and B send unregistration confirmation (UCF) messages to their respective Gateways.

## Configuring Security on the Gateway

To use the new H.323 security features as illustrated in the example in the "How the Enhancements Can Be Used" section, you must do the following:

- Download the appropriate Tool Command Language (TCL) IVR scripts from the CCO Software Support Center. The IVR feature was first made available to customers in Cisco IOS Release 11.(3)NA2, with the Service Provider Voice over IP feature set. Scripts using TCL were introduced with Cisco IOS Release 12.0(4)XH. These TCL IVR scripts are the default scripts that must be used with the IVR application in Cisco IOS Release 12.0(4)XH and future releases.

- Configure the IVR inbound dial-peer on the Gateway router.
- Enable H.323 security on the Gateway. With this release, the Cisco IOS software has been modified to include a new command that allows you to configure H.323 security on the Gateway.

## Downloading IVR Scripts

The TCL IVR scripts are the default scripts for all Cisco voice features using IVR. All IVR scripts that were developed for releases before Cisco IOS Release 12.0(5)T have been modified and secured with a proprietary Cisco locking mechanism using TCL. Only Cisco internal technical support personnel can open and modify these scripts. When the TCL script is activated, the system verifies the Cisco signature level. If the script is inconsistent with the authorized signature level, the script does not load and the customer's console screen displays an error message.

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** The audio files used in the IVR scripts are typically loaded via URL-like the scripts or from flash memory. For more information about how to use audio files and the audio files provided by Cisco, see the “Prepaid Distributed Calling Card via Packet Telephony” document, which is located on CCO at: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/0134bowi.htm>

---

### voip\_auth\_acct\_pin\_dest.tcl

The voip\_auth\_acct\_pin\_dest.tcl script:

- Prompts the caller to enter their account number, their personal identification number (PIN), and the 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 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 only have three minutes remaining on your credit”) is played to the calling party only. The called party hears silence during this time. For example, if the configured timeout value is three minutes, when the caller has only three minutes of credit left the message is played.
    - The TCL script plays a warning message, when the user’s credit has been exhausted. The message (such as, “Sorry, you have run out of credit.”) is played to the calling party only. The called party is expected to hear 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 for one to two seconds. If the # button is pressed down for more than one 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 then authenticated and authorized using this number and the previously provided account number and PIN.

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

- Re-authenticates 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 re-enter 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 is configurable. The default is three (3).
- Can terminate a field by size instead of the terminating character (#). The TCL script allows you to specify number of digits 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 currency amount and time. All the prompts are recorded and stored in both languages. The language selection is made when the caller presses a pre-defined key in response to a prompt (such as, “For English press one. For Spanish press two”). 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 an 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 caller’s credit has been exhausted.

## Overview of the Configuration Steps

To call an IVR script and enable H.323 security, enter the following commands:

---

**Note** This list assumes that you have already configured your router and your H.323 gateway.

---

Step	Command	Purpose
1	Router # <b>configure terminal</b>	Enter the global configuration mode.
2	Router (dial-peer) # <b>dial-peer voice</b> <i>number</i> <b>pots</b>	Enter the dial-peer configuration mode to configure a POTS dial peer. The number value of the dial-peer voice POTS command is a tag that uniquely identifies the dial peer.
3	Router (dial-peer)# <b>call application</b> <i>application_name</i>	Enter 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.
4	Router (dial-peer)# <b>destination-pattern</b> <i>e164_address</i>	Enter the E164 address associated with this dial peer.
5	Router (dial-peer)# <b>port</b> <i>port_number</i>	Configure the voice port associated with this dial peer.
6	Router (dial-peer)# <b>exit</b>	Exit the dial-peer configuration mode.
7	Router (config)# <b>gateway</b>	Enter the gateway configuration mode.
8	Router (gateway)# <b>security password</b> <i>password level {endpoint   per-call   all}</i>	Enable H.323 security and specify the level of validation to be performed.

### Sample Resulting Configuration

The following example illustrates the resulting configuration in which an IVR script is called and H.323 security is enabled on the 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 0.0.0.0 0.0.0.0 172.18.72.65
!
!
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
end
```

## Command Reference

This section describes the new **security** command and provides information about the existing **call application voice** and **call application voice load** commands used in the example configuration.

## security Command

To enable H.323 security on the Gateway and configure the level of security, use the **security** command.

**[no] security password *password* level { endpoint | per-call | all }**

The no form of this command disables H.323 security on the Gateway.

### Syntax Description

<i>password</i>	The Gateway password.
<b>endpoint</b>	Validation will be performed on all RAS messages sent by the Gateway. The validation will be performed using the cryptoTokens that are generated based on the security password configured for the Gateway.
<b>per-call</b>	Validation will be performed only on the admission messages from the H.323 endpoints to the Gateway (ARQ messages).
<b>all</b>	Validation will be performed on all RAS messages sent by the Gateway. All RAS messages (except ARQ messages) include cryptoTokens that are based on the security password configured for the Gateway. The cryptoToken in ARQ messages is based on a user-supplied account number and PIN.

### Command Mode

Gateway configuration

## call application voice Command

To create and then call the application that will interact with the IVR feature (as well as define debit card parameters, such as PIN length), use the **call application voice** command.

**[no] call application voice** {*application name*} {**language** *value* | **operator-number** *value*| **pin-length** *value* | **retry-count** *value* | **set-location** *value* | **uid-lenth** *value* | **warning-time** *value*}

### Syntax Description

<i>application name</i>	<p>Specifies which TCL application the system is to call, or use for the calls configured on the inbound dial-peer. Enter the name of the TCL script file and the path name where the TCL scripts are stored. An abbreviated name can be configured to represent the full TCL application and path name included in one word.</p> <p>For example, the application name “test” can be an alias for: tftp://keyer/debitaudio/.</p> <p>Enter the path name first, and then the script file name. Valid storage locations can be URL or TFTP server.</p>
<b>language</b> <i>value</i>	<p>Indicates the language used for playing the audio files. For example, enter “1” corresponding to the English language or enter “2” corresponding to the Spanish language audio files. Any number can be configured to represent the languages.</p> <p>Syntax: <b>language</b> <i>digit language</i></p> <p>Example: <b>call application voice test language 1 en</b></p> <p>Parameters are:</p> <ul style="list-style-type: none"> <li>digit—minimum is 0, maximum is 9.</li> <li>language—2 characters representing the language. Enter “aa” to represent all.</li> </ul>
<b>operator-number</b> <i>value</i>	<p>The designated operator telephone number of the service provider, (or any other number designated by the customer). This is the number that calls are terminated to when debit time allowed has run out, or debit (\$) amount is exceeded.</p>
<b>pin-length</b> <i>value</i>	<p>The number of characters of the PIN number. Possible values are 0 through 10.</p>
<b>retry-count</b> <i>value</i>	<p>The number of times the user is allowed to reattempt to enter the information that they are prompted for. Possible values are 1 through 5.</p>
<b>set-location</b> <i>value</i>	<p>The location of the audio files. This location must correspond with both the category and language of the value entered for the language parameter.</p> <p>Syntax: <b>set-location</b> <i>language category url_or_tftp_location</i></p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>language—en = English, sp = Spanish.</li> <li>category—minimum is 0, maximum is 4. (0 means all)</li> </ul> <p>The audio files can be divided into category groups (0 - 4). For example, audio files representing the days and months can be represented by category “1”, audio files representing units of currency can be category “2”, audio files units of time (seconds, minutes, and hours) can be represented by category “3”.</p> <p>Example: <b>set-location en 1 tftp://keyer/debit audio/</b></p>

<b>uid-length</b> <i>value</i>	The number of characters in the user ID. Possible values are 1 through 20.
<b>warning-time</b> <i>value</i>	How far in advance (in seconds) the user is warned that their allowed calling time is running out. Possible values are 1 through 600.

### Command Usage Notes

Keep the following in mind when using the **call application voice** command:

- The command **no call application voice** *tcl\_script name* removes the entire application and all parameters, if configured.
- The command **no call application voice** *tcl\_script name* **pin-len** resets the PIN length to its default.
- Using the “no” form of the command with any other parameter deletes the setting for that particular parameter.
- The name of the application should be put into the dial peer.

### Command Mode

Dial-peer configuration mode

## call application voice load Command

To load the selected TCL script from the URL, use the **call application voice load** command. The software checks the signature lock to ensure it is a Cisco-supported TCL script.

**call application voice load** *name*

### Syntax Description

---

<i>name</i>	Defines the TCL application to use for the call. Enter the name of the TCL application you want this dial peer to use.
-------------	--

---

### Command Mode

Privileged EXEC command mode

## Changes to RAS Messages

In support of the new H.323 security and accounting features, fields have been added to several of the RAS messages. In general, all the RAS messages sent by the Gateway, with the exception of the Gateway Request (GRQ), include authentication data in the cryptoToken field. This section lists each of the messages that changed and describes the fields that have been added.

### GRQ Message

When H.323 security is enabled on the Gateway, the following fields are added to the GRQ message:

Field	Description
authenticationCapability	This field should have a value of pwdHash.
algorithmOIDs	The object ID for the MD5 algorithm. The OID used to indicate MD5 will be {1 2 840 113549 2 5}

### GCF Message

When H.323 security is enabled on the Gateway, the following fields should be the GCF message:

Field	Description
authenticationMode	This field should have a value of pwdHash.
algorithmOIDs	The object ID for the MD5 algorithm. The OID used to indicate MD5 will be {1 2 840 113549 2 5}

If the authenticationMode or the algorithmOID fields do not contain the values specified above, the Gatekeeper responds with a GRJ message that contains a reject reason of securityDenial. This prompts the Gateway to resend the GRQ.

### RRQ Message

If H.323 security is enabled on the Gateway, the following fields are added to the RRQ message:

Field	Description
cryptoTokens	This field contains one of the cryptoToken types defined for the CryptoH323Token field specified in H.225. Currently, the only type of cryptoToken supported is the cryptoEPPwdHash.

The following fields are contained within the cryptoEPPwdHash structure:

Field	Description
alias	The Gateway alias, which is the H.323 ID of the Gateway.
timestamp	The current time stamp.
token	The MD5 encoded PwdCertToken. This field contains the following: <ul style="list-style-type: none"> <li>timestamp—The same as the timestamp of the cryptoEPPwdHash.</li> <li>password—The gateway's password.</li> <li>generalID—The same Gateway alias as the one included in the cryptoEPPwdHash.</li> <li>tokenId—The object ID.</li> </ul>

## ARQ Message

When H.323 security is enabled on the Gateway, additional fields are included in the ARQ message. The contents of the field depend on whether the ARQ message is sent from the source Gateway or the destination Gateway.

### Source Gateway ARQ Message

If the ARQ message is sent from the source Gateway, the following fields are included:

Field	Description
cryptoTokens	This field contains one of the cryptoToken types defined for the CryptoH323Token field specified in H.225. Currently, the only type of cryptoToken supported is the cryptoEPPwdHash.

The following fields are contained within the cryptoEPPwdHash structure:

Field	Description
alias	The user's account number or the Gateway's H.323 ID if endpoint authentication is selected.
timestamp	The current time stamp.
token	The MD5 encoded PwdCertToken. This field contains the following: <ul style="list-style-type: none"> <li>• timestamp—The same as the timestamp of the cryptoEPPwdHash.</li> <li>• password—If “endpoint” is selected, this is the Gateway’s security password. Otherwise, it is the user's password or PIN.</li> <li>• generalID—If “endpoint” is selected, this is the Gateway's H.323 ID. Otherwise, it is the user's ID or account number.</li> <li>• tokenID—The object ID.</li> </ul>

### Destination Gateway ARQ Message

If the ARQ message is sent from the destination Gateway, the following fields are included:

Field	Description
cryptoTokens	This field contains one of the cryptoToken types defined for the CryptoH323Token field specified in H.225. Currently, the only type of cryptoToken supported is the cryptoEPPwdHash.

The following fields are contained within the cryptoEPPwdHash structure:

Field	Description
alias	The alias (H.323 ID or E.164 address) of the destination Gateway.
timestamp	The current time stamp.
token	The MD5 encoded PwdCertToken. This field contains the following: <ul style="list-style-type: none"> <li>• timestamp—The same as the timestamp of the cryptoEPPwdHash.</li> <li>• password—The destination gateway’s password.</li> <li>• generalID—The same Gateway alias as the one included in the cryptoEPPwdHash.</li> <li>• tokenID—The object ID.</li> </ul>

## ACF Message

If H.323 security is enabled on the Gateway, the Gatekeeper should include the billing-related information the nonStandardParameter field of the clearTokens structure. If the call is using a prepaid call service, the clearTokens field should indicate the maximum call duration. In the case of prepaid call service, the Gateway will terminate the call if it exceeds the allowed time.

The following clearToken fields should be included in the ACF message:

Field	Description
nonStandard	The billing information for the call.
tokenOID	The generic billing object ID.

The following fields are contained within the nonStandardParameter structure:

Field	Description
nonStandardIdentifier	The generic billing object ID.
BillingInfo	The billing information. This field can contain the following: <ul style="list-style-type: none"> <li>• bill_to—A string identifying the subscriber that should be billed for this call.</li> <li>• reference_id—A unique ID generated by the billing system.</li> <li>• billing_mode—Whether the call is being made using prepaid call service (debit_mode) or not (credit_mode).</li> <li>• max_duration—The maximum duration allowed for the call. Used only for prepaid call service.</li> <li>• balance—The account balance of the caller. For a billing mode of credit_mode, this should be a negative value that represents the current amount owed by the subscriber. Otherwise, this should be a positive amount that represents the credit remaining on the subscribers debit account.</li> <li>• currency—The currency used in reporting the balance.</li> <li>• timezone—The time zone of the call, represented by a hexadecimal string that indicates the difference in seconds between the caller's location and the Universal Time Clock (UTC).</li> </ul>

## DRQ Message

The Gateway sends a DRQ message when the call ends. If H.323 security is enabled on the Gateway, the call usage information is included in the DRQ message. The call usage information is sent in the nonStandardParameter field of the ClearToken structure.

The following fields are contained within the nonStandardParameter structure:

Field	Description
duration	The duration of the call in seconds.

Field	Description
callLog	<p>The call usage information. This field contains the following information:</p> <ul style="list-style-type: none"><li>• DISCONNECT_REASON—The disconnect reason. Possible values are:<ul style="list-style-type: none"><li>— DISCONNECT_NORMAL—The call ended normally.</li><li>— DISCONNECT_DISCONNECT—The call ended due to a technical failure.</li><li>— DISCONNECT_ABANDONED—The call never took place, for example if the remote phone was not answered.</li><li>— DISCONNECT_PREEMPT—The call was ended by the Gateway. This would be the disconnect reason issued if the call was ended because the max_duration was exceeded.</li></ul></li><li>• DISCONNECT_STRING—A string that further describes the disconnect reason.</li><li>• TIME—The time the call started, indicated by a hexadecimal string that represents the time, in seconds, since 00:00 January 1, 1970 UTC.</li><li>• ORIGIN—Whether the call was inbound or outbound.</li></ul>

## Related Documentation

- Configuring Interactive Voice Response for Cisco Access Platforms  
[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/5300/cfios/0061ivr.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/cfios/0061ivr.htm)
- Service Provider Features for Voice over IP  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/voip1203.htm>
- Voice over IP for the Cisco AS5300  
<http://www.cisco.com/univercd/cc/td/doc/product/access/nubuvoip/voip5300/index.htm>
- Voice over IP for the Cisco AS5800  
<http://www.cisco.com/univercd/cc/td/doc/product/access/nubuvoip/voip5800/index.htm>
- Voice over IP for the Cisco 2600/Cisco 3600 Series  
<http://www.cisco.com/univercd/cc/td/doc/product/access/nubuvoip/voip3600/index.htm>
- Configuring H.323 VoIP Gateway for Cisco Access Platforms  
[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/5300/iosinfo/ios\\_mods/0044gw.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/iosinfo/ios_mods/0044gw.htm)
- Configuring H.323 VoIP Gatekeeper for Cisco Access Platforms  
[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/5300/iosinfo/ios\\_mods/0042gk.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/iosinfo/ios_mods/0042gk.htm)
- Prepaid Distributed Calling Card via Packet Telephony  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/0134bowi.htm>

## Glossary

**AAA**—Authentication, Authorization, and Accounting. AAA is a suite of network security services that provides the primary framework through which you can set up access control on your Cisco router or access server.

**gatekeeper**—A gatekeeper maintains a registry of devices in the multimedia network. The devices register with the gatekeeper at startup and request admission to a call from the gatekeeper.

The gatekeeper is an H.323 entity on the LAN that provides address translation and control access to the LAN for H.323 terminals and gateways. The gatekeeper can provide other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways.

**gateway**—A gateway allows H.323 terminals to communicate with non-H.323 terminals by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

An H.323 gateway is an endpoint on the LAN that provides real-time, two-way communications between H.323 terminals on the LAN and other ITU-T terminals in the WAN or to another H.323 gateway.

**IVR**—Interactive voice response. When someone dials in, IVR responds with a prompt to get a personal identification number (PIN), and so on.

**PIN**—Personal identification number. Password used with account number for authentication.

**POTS**—Plain old telephone service. Basic telephone service supplying standard single line telephones, telephone lines, and access to the PSTN.

**PSTN**—Public Switched Telephone Network. PSTN refers to the local telephone company.

**RADIUS**—Remote Access Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

**TCL**—Tool Command Language. TCL is an interpreted script language developed by Dr. John Ousterhout of the University of California, Berkeley, and is now developed and maintained by Sun Microsystems Laboratories.

**URL**—Universal Resource Locator. Standardized addressing scheme for accessing hypertext documents and other services using a browser.

**VoIP**—Voice over IP. The ability to carry normal telephone-style voice signals over an IP-based network with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to Cisco's open standards-based (for example, H.323) approach to IP voice traffic.

---

**Note** For a list of other internetworking terms, see Internetworking Terms and Acronyms document that is available on the Documentation CD-ROM and Cisco Connection Online (CCO) at the following URL: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>.

---

## Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet

e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact [cco-help@cisco.com](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).

---

**Note** If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or [tac@cisco.com](mailto:tac@cisco.com). To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or [cs-rep@cisco.com](mailto:cs-rep@cisco.com).

---

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, GigaStack, IGX, Internet Quotient, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, Secure Script, ServiceWay, SlideCast, SMARTnet, *The Cell*, TrafficDirector, TransPath, ViewRunner, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9909R)

Copyright © 1999, Cisco Systems, Inc.  
All rights reserved.