

Cisco H.235 Accounting and Security Enhancements for Cisco Gateways

This document describes the Cisco H.235 Accounting and Security Gateway Enhancements for Cisco IOS Release 12.0(7)T. It includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 2
- Prerequisites, page 3
- Configuration Tasks, page 3
- Configuration Examples, page 4
- Command Reference, page 7
- Debug Commands, page 9
- Glossary, page 9

Feature Overview

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 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 “Command Reference” 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).

Benefits

Gateway Security and Accounting

This feature provides sender validation by using an authentication key in the gateway’s RAS messages. This key is used by the gatekeeper to authenticate the source of the messages and ensure secure communication.

Related Documents

Configuring H.323 VoIP Gateway for Cisco Access Platforms

Supported Platforms

- Cisco 2600
- Cisco 3600
- Cisco MC3810
- Cisco AS5200
- Cisco AS5300
- Cisco AS5800
- Cisco 7200

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Enabling security on the Cisco gateway will result in the RAS messages containing a secure key. In order 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.

Configuration Tasks

See the following sections for configuration tasks for the Cisco H.235 Accounting and Security features:

- Downloading IVR Scripts
- Configuring the IVR Inbound Dial Peer
- Enabling Security on the Gateway

Downloading IVR Scripts

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 Tool Command Language (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.

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.

You can download TCL scripts from the CCO Software Center at the following URL:

<http://www.cisco.com/cgi-bin/ibld/all.pl?i=support&c=3>

Note The audio files used in the IVR scripts are typically loaded using URL-like scripts or from Flash memory.

Configuring the IVR Inbound Dial Peer

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

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

Step	Command	Purpose
1	Router # configure terminal	Enter the global configuration mode.
2	Router (dial-peer) # dial-peer voice <i>number</i> pots	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)# call application <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 IVR TCL script is stored.
4	Router (dial-peer)# destination-pattern <i>e164_address</i>	Enter the E164 address associated with this dial peer.
5	Router (dial-peer)# port <i>port_number</i>	Configure the voice port associated with this dial peer.
6	Router (dial-peer)# exit	Exit the dial-peer configuration mode.

Enabling Security on the Gateway

Step	Command	Purpose
1	Router # configure terminal	Enter the global configuration mode.
2	Router (config)# gateway	Enter the gateway configuration mode.
3	Router (gateway)# security password <i>password</i> level { endpoint per-call all }	Enable security and specify the level of validation to be performed.
4	Router (gateway)# exit	Exit the gateway configuration mode.

Verifying Security

The command **show running configuration** displays the security password and level when it is enabled. By default, security is disabled.

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

Configuration Examples

This section provides the following configuration examples:

- Security Enabled

Security Enabled

The following example illustrates the resulting configuration in which an IVR script is called and 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 documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 T command reference publications.

security password level

To control whether H.323 security is enabled on the gateway, use the **security password level** command. To disable, use the **no** form of this command.

security password level { *endpoint* | *per-call* | *all* }

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

Syntax Description

<i>level</i>	This option can be used to control the scope of the authentication/authorization being provided by the gateway.
<i>endpoint</i>	Authentication of the endpoint/gateway will be provided. In the case of H.323, this selection will authenticate the RAS channel and messages.
<i>per-call</i>	In addition to the endpoint, each call is authenticated and authorized by the gatekeeper. The selection of this option will enable the prompting for an account number and pin number when a call is received. The associated POTS dial peer over which calls will be received should be configured for an IVR application that is designed to prompt for an account or pin number and authenticate with a gatekeeper using RAS.
<i>all</i>	Both endpoint and per-call authentication and authorization will be provided. This is the default selection.

Defaults

Both endpoint and per-call authentication is provided.

Command Modes

Global configuration mode

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

This command is designed to add security on inbound IP call legs where the call might originate from a gateway you don't know and trust, but routed by a gatekeeper you do know and trust.

It can also be used in the case when you want to do subscriber authentication on the gatekeeper instead of from the gateway.

Examples

The following example shows that each call is authenticated by the gatekeeper:

```
security password 151E0A0E level per-call
```

Debug Commands

There are no new or modified debug commands for this feature.

Glossary

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

ANI—Answer number indication. The calling number (number of calling party).

ARQ—Admission request.

CAS—Channel associated signaling.

dial peer—An addressable call endpoint. In Voice over IP (VoIP), there are two types of dial peers: POTS and VoIP.

endpoint—An H.323 terminal or gateway. An endpoint can call and be called. It generates or terminates the information stream, or both.

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 may 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 at which a circuit-switched call is encoded and repackaged into IP packets.

A 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.

H.323—An International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the conferencing system, and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

H.323 RAS—Registration, admission, and status. The RAS signaling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.

LRQ—Location request.

node—An H.323 entity that uses RAS to communicate with the gatekeeper. For example, an endpoint such as a terminal, proxy, or gateway.

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.

QoS—Quality of service, which refers to the measure of service quality provided to the user.

RAS—Registration, admission, and status protocol. This is the protocol that is used between endpoints and the gatekeeper to perform management functions.

RBS—Robbed bit signaling

RRQ—Registration request.

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