Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways

First Published: 2006
Last Updated: June 11, 2009

The Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature provides authentication, integrity, and encryption of voice media and call control signaling for H.323 protocol-based voice gateways.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways" section on page 22.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

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

Prerequisites for Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways

Make sure that the following tasks have been completed before configuring the Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature:

- Cisco IOS H.323 protocol is configured.
- Cisco IOS gateways have the prerequisite Cisco IOS images installed. Voice security features are delivered on Advanced IP Services or Advanced Enterprise Services images.
- IP security (IPSec) is configured on the Cisco IOS gateway. For more information on configuring Cisco IOS-based (software) IPSec, refer to the following:
  - *IPSec Considerations and Recommendations*
  - *Cisco IOS Security Configuration Guide,* Release 12.4
  - *Cisco IOS Security Command Reference,* Release 12.4
- Cisco CallManager 5.0 or a later release is running if the Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature is deployed in a Cisco CallManager network. For more information on configuring Cisco CallManager, refer to the document *Cisco CallManager Security Guide, Release 5.0.*

Restrictions for Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways

The following secure encrypted services are not supported in Cisco IOS Release 12.4(6)T1:

- Voice security during conferencing, transcoding, and music-on-hold.
- Secure Cisco IOS SIP (Session Initiation Protocol) gateways and call flows.
- H.323 endpoints other than those listed in Table 1.
- Interworking scenarios on the Cisco IOS IP-to-IP gateway, including:
  - Fast start to slow start signaling
  - Slow start to fast start signaling
- The call failure retry (rotary) feature on the Cisco IOS IP-to-IP gateway.
- Voice security for IVR applications, such as automated attendant, where, even though the endpoint is Secure Real-Time Transport Protocol (SRTP) capable, voice is streamed to the gateway without using a digital signal processor (DSP).

Table 1 lists supported gateways, network modules, and codecs for voice security features.

Table 1 Supported Gateways, Network Modules, and Codecs for Voice Security Features

Supported Gateways	Supported Network Modules	Supported Codecs
• Cisco 2600XM • Cisco 2691 • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3725 • Cisco 3745 • Cisco 3825 • Cisco 3845 • Cisco VG224 • Cisco IAD 2430	• AIM-VOICE • AIM-ATM-VOICE-30 • EVM-HD • NM-HDA • NM-HDV • NM-HDV2 • NM-HDV2-1T1/E1 • NM-HDV2-2T1/E1 • NM-HD-1V • NM-HD-2V • NM-HD-2VE • PVDM2	• G.711 mu-law • G.711 a-law • G.729 • G.729A

Information About Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways

To configure the Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature, you should understand the following concepts:

- Benefits of Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways, page 3
- Feature Design of Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways, page 4

Benefits of Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways

- Provides privacy and confidentiality for voice calls
- Protects against voice security violations
- Facilitates the replacement of traditional time-division multiplexing (TDM) telephony systems with IP systems

Feature Design of Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways

In a typical communications network, there is a risk of security breaches affecting voice communications over the IP network. The *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* feature provided voice security features to address requirements for privacy, integrity, and confidentiality of voice conversations for Cisco IOS Media Gateway Control Protocol (MGCP) gateways. With the new Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature, Cisco extends voice security features to Cisco IOS H.323 protocol-based gateways, and expands the number of network modules that support media authentication and encryption.

The Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature supports the following capabilities between gateways:

- Gateway to gateway call control authentication and encryption using IPSec.
- Media encryption and authentication of voice streams using SRTP.
- Exchange of RTP Control Protocol (RTCP) information using Secure RTCP.
- SRTP to RTP fallback for calls between secure and nonsecure endpoints. You can configure secure call fallback either globally or by dial peer.
- Cisco IOS IP-to-IP gateway interoperation with secure Cisco IOS H.323 gateways.

Security Technologies

The Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature provides secure IP telephony signaling and media to achieve secure voice calls. Cisco implements voice security over the IP telephony network by establishing and maintaining authenticated communications using the following security technologies:

- Signaling authentication validates that no tampering has occurred with signaling packets during transmission.
- Encryption, the process of converting clear-text data into enciphered data, provides data integrity and authentication.
- IPSec, a standards-based set of security protocols and algorithms, ensures that signaling information such as DTMF digits, passwords, personal identification numbers (PINs), and encryption keys that is sent between voice gateways and gatekeepers is encrypted.
- Media encryption using standards-based SRTP ensures that media streams between supported devices are secure.
- Cisco IOS H.323 supports the AES_CM_128_HMAC_SHA1_32 cryptographic suite, which includes the AES-128-countermode encryption algorithm and the Hashed Message Authentication Codes (HMAC) Secure Hash Algorithm1 (SHA1) authentication algorithm.
- Cisco IOS H.323 supports H.235.8 compliant procedures for the signalling, negotiation and transport of the SRTP cryptographic keys, authentication and encryption algorithm identifiers and other session parameters between H.323 endpoints.

Note Although you may enable media authentication and encryption without signaling encryption, Cisco discourages this practice. If the connection between gateways is not secure, media keys will be sent in clear text and your voice call will not be considered secure.

The following behaviors must be present for a voice call to be secure in the Cisco IOS H.323 IP telephony network:

- The network modules, as listed in Table 1, and digital signal processor (DSP) associated with the TDM/analog call leg must be secure capable.
- VoIP call leg security is enabled either globally or on a per-dial peer basis.
- H.323 call setup generates encryption keys are carried to the remote end.
- The terminating gateway (TGW) checks for secure capabilities of the DSP and indicates its capabilities to the originating gateway (OGW).
- Once the OGW receives remote end capabilities indicating the TGW is secure capable, the call is secure.

If the previous behaviors do not occur, the call is not secure, and depending on the fallback policy configured, the call is disconnected.

Both IPSec and SRTP must be enabled for voice call security. Possible interactions of IPSec and SRTP and the resulting outcomes are listed in Table 2.

Table 2 IPSec and SRTP Interactions

IPSec	SRTP	Result
ON	ON	Call signaling and media are both secure.
OFF	ON	Media is secure; however, signaling is not secure. Keys are visible in signaling messages in clear text.
ON	OFF	Signaling is protected; however, media is not secure.
OFF	OFF	Both media and signaling are not secure.

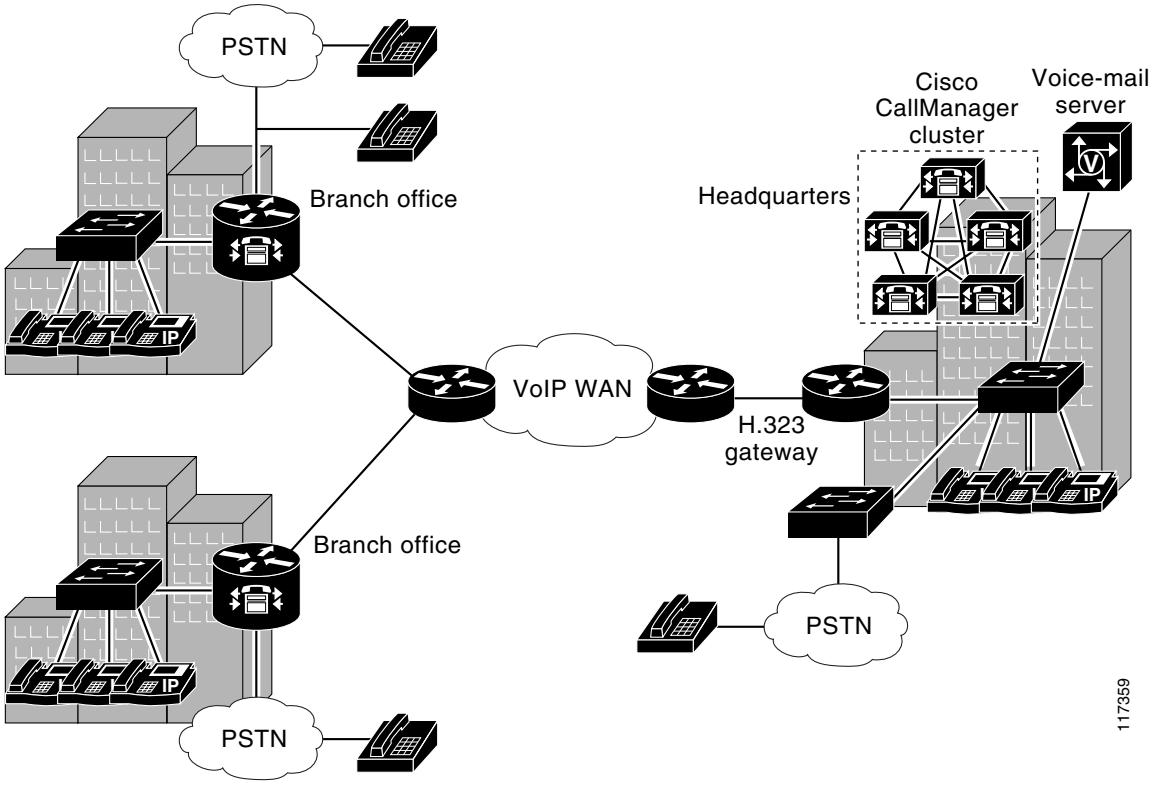
Note We strongly recommend that you first establish an IPSec connection between gateways before you configure security using SRTP. Otherwise, media keys will be sent in clear text and your voice call will not be considered secure.

Cisco IOS H.323 Gateway Behavior

In order to secure voice call control and signaling, IPSec is configured on both gateways and gatekeeper (GK), if any, with a preshared key. Upon bootup, the gateway and GK, if any, authenticate each other by preshared key. After successful authentication, IPSec starts secured traffic in tunnel mode. After IPSec is started, the gateway sends Registration, Admission, and Status (RAS) messages to the GK through secured IPSec tunnel. H.225 call control messages between gateways flow through the secured IPSec channel established between them. IPSec configuration on both gateways, OGW and TGW, is required before voice calls can be placed. Cisco recommends hardware Virtual Private Network (VPN) on the gateway for improved performance. After the IPSec tunnel is established, all call control signaling H.225 and H.245 packets between gateways go through the secured IPSec tunnel. OGW and TGW then determine if an endpoint is SRTP and SRTCP capable and send this information to the other end.

Figure 1 shows a typical topology where voice security features are deployed.

Figure 1 Voice Security Features in the IP Telephony Network



Cisco IOS IP-to-IP Gateway Behavior

The Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature interoperates with the Cisco IOS IP-to-IP gateway to provide voice security features. An IP-to-IP gateway (IPIPGW), also known as a border element or session border controller, facilitates connectivity between independent VoIP networks by enabling H.323 VoIP and video conferencing calls from one IP network to another. The IPIPGW performs many of the same functions as a public switched telephone network (PSTN)-to-IP gateway, but typically joins two IP call legs, rather than a PSTN and an IP call leg. The Cisco Multiservice IP-to-IP Gateway feature is a special Cisco IOS software image that runs on Cisco multiservice gateway platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

When used in a secure H.323 deployment with Cisco IOS H.323 gateways, the IPIPGW supports secure calls in flow through and flow around mode. In flow through mode, SRTP packets are terminated and reorganized, and passed through the IPIPGW. Because only the User Datagram Protocol (UDP) header is changed, and RTP packet contents are not decrypted and encrypted, no DSP resource is required. In flow around mode, RTP packets flow around and do not enter the IPIPGW. Signaling is fully terminated and reorganized in either mode.

The following IPIPGW features are not supported:

- Secure transcoding and conferencing support on the IPIPGW using SRTP to RTP and vice versa
- Fast start to slow start signaling and vice versa

- H.323 to SIP network interconnection

For more information on the Cisco IOS IP-to-IP gateway, refer to the *Cisco Multiservice IP-to-IP Gateway* document.

Figure 2 shows a toll bypass topology diagram for secure voice call setup in an IPIPGW scenario. The following points summarize this configuration:

- Configure IPSec tunnels between GW-GK and GW-GW, a prerequisite to protect the signaling channels. IPSec tunnels are terminated and reorganized hop by hop.
- Configure SRTP at the OGW and TGW to protect the media. SRTP media is end to end.
- When voice calls are made, calls will be secure per the configuration.
- SRTP is supported on secure-capable DSPs and the associated network modules listed in Table 1.

Figure 2 Toll Bypass Topology Diagram

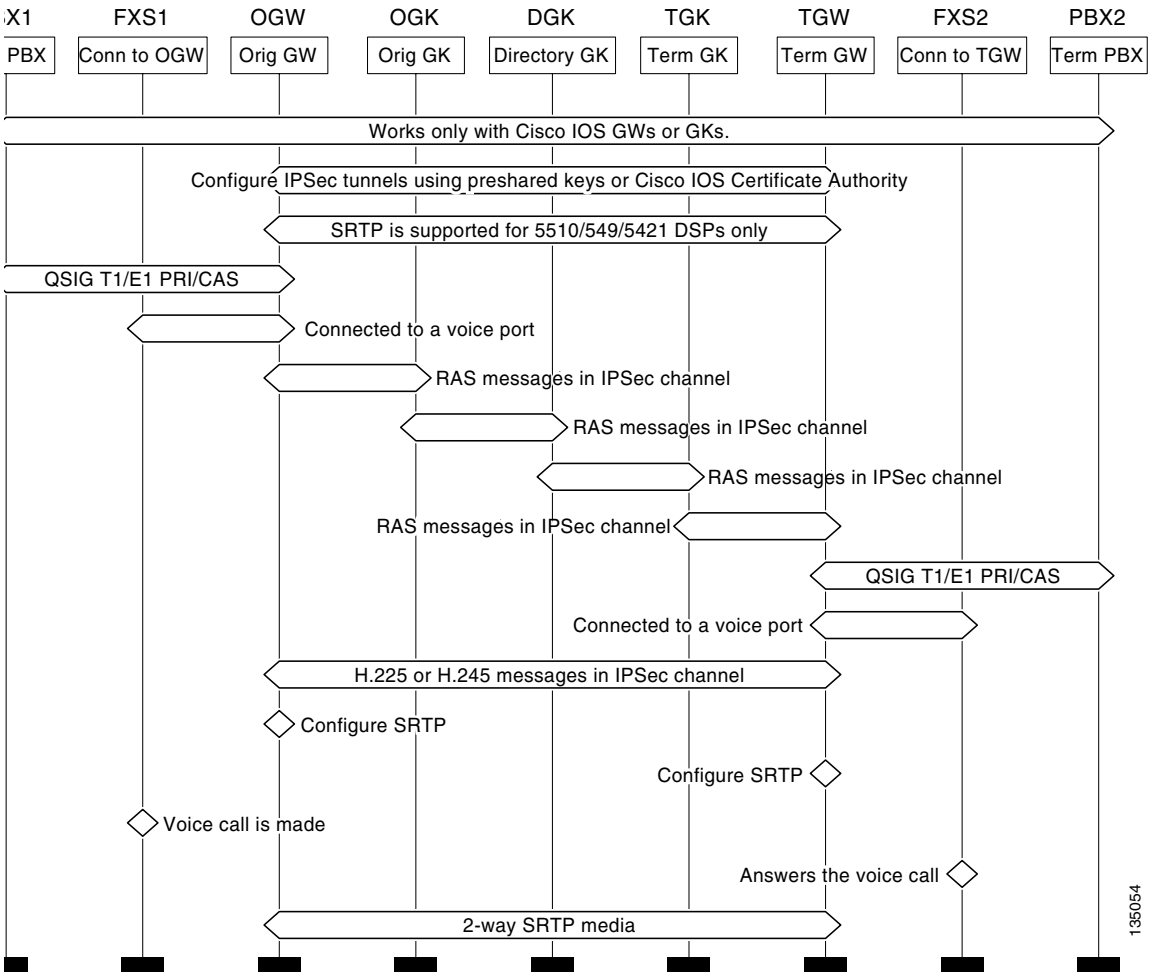
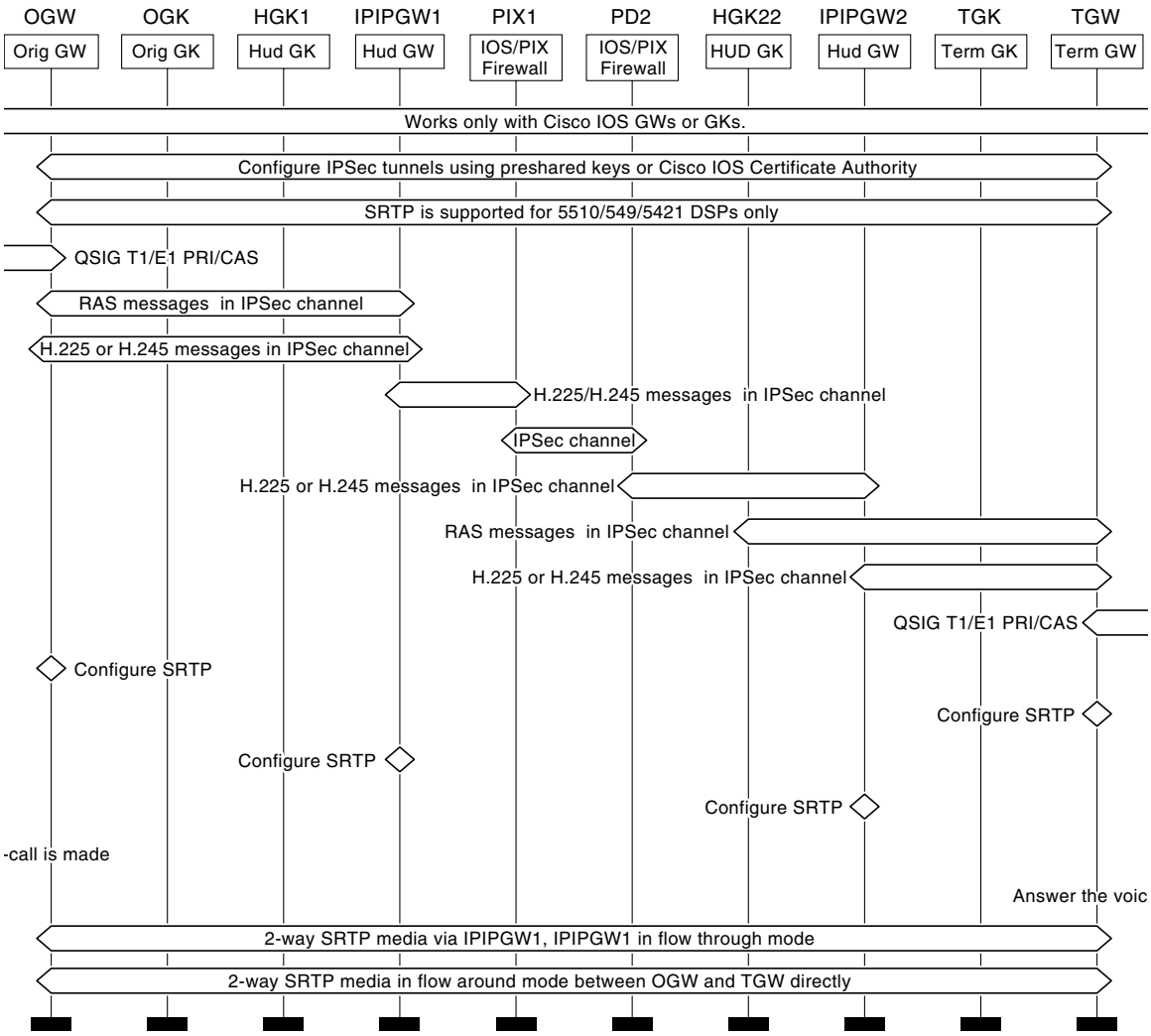


Figure 3 shows a topology diagram for secure voice call setup in an IPIPGW and Network Address Translation (NAT)/firewall scenario. The following points summarize this configuration:

- Configure IPSec tunnels between GW-GK and GW-GW, IPIPGW-PIX, a prerequisite to protect the signaling channels. IPSec tunnels are terminated and reorganized hop by hop.

- Configure SRTP at the OGW and TGW to protect the media. SRTP media is end to end.
- When voice calls are made, calls will be secure per the configuration.
- SRTP is supported on secure-capable DSPs and the associated network modules listed in Table 1.

Figure 3 IPIPGW and PIX Topology Diagram



How to Configure Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways

This section contains the following procedures:

- Configuring Media and Signaling Authentication and Encryption for Secure Voice Calls Globally, page 9, (required)
- Configuring Media and Signaling Authentication and Encryption for Secure Dial-Peer Calls, page 11, (required)

- Verifying and Troubleshooting Media and Signaling Authentication and Encryption Secure Call Configuration, page 12, (optional)

Configuring Media and Signaling Authentication and Encryption for Secure Voice Calls Globally

This task configures secure media authentication and encryption on the H.323 gateway. You can configure SRTP capability either globally or at the dial peer level; configuration in only one mode is necessary.

Prerequisites

We strongly recommend that you first establish an IPSec connection between gateways before you configure security using SRTP. Otherwise, media keys will be sent in clear text and your voice call will not be considered secure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **srtp [fallback]**
5. **allow-connections** *from-type* **to** *to-type*
6. **exitvoice-card** *slot*
7. **codec complexity secure**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode. • The **voip** keyword specifies VoIP encapsulation.

	Command or Action	Purpose
Step 4	**srtp** [**fallback**] **Example:** `Router(conf-voi-serv)# srtp`	Enables security policies. • The **srtp** command enables secure calls using SRTP for media encryption and authentication and disables fallback. • The **fallback** keyword enables call fallback to nonsecure (RTP) mode, allowing the user to make calls that are not secure. **Note** This security policy applies to all calls going through the gateway and is not configurable on a per-call basis.
Step 5	**allow-connections** *from-type* **to** *to-type* **Example:** `Router(conf-voi-serv)# allow-connections h323 to h323`	(Optional) Enables secure calls on a Cisco IOS multiservice IP-to-IP gateway.
Step 6	**exit** **Example:** `Router(conf-voi-serv)# exit`	Exits the current configuration mode.
Step 7	**voice-card** *slot* **Example:** `Router(config)# voice-card 1`	Enters voice-card configuration mode and configures the voice card in the specified network module slot.
Step 8	**codec complexity secure** **Example:** `Router(config-voice-card)# codec complexity secure`	Restricts the number of channels per network module from 4 to 2, enabling SRTP support on the TI-549 and TI-5421DSPs, and on the following network modules: • AIM-VOICE • AIM-ATM-VOICE-30 • NM-HDA • NM-HDV You need not specify secure codec complexity for TI-5510 DSPs, which support SRTP capability in all complexity modes. The TI-5510 DSP defaults to the **codec complexity flex** command, which enables the DSP to handle a flexible number of channels required for SRTP support.
Step 9	**exit** **Example:** `Router(config-voice-card)# exit`	Exits the current configuration mode.

Configuring Media and Signaling Authentication and Encryption for Secure Dial-Peer Calls

This task configures all calls for a given dial peer to go through in either secure or nonsecure mode. You can configure SRTP capability either at the dial peer level or globally; configuration in only one mode is necessary.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **srtp** [**fallback** | **system**]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 101 voip`	Enters dial-peer voice configuration mode and defines a particular dial peer. • The **voip** keyword specifies a VoIP peer.

	Command or Action	Purpose
Step 4	**srtp** [**fallback** | **system**] **Example:** `Router(config-dial-peer)# srtp fallback`	Enables secure calls that use SRTP for media encryption and authentication and specifies fallback capability. Using the **no srtp** command disables security and causes the dial peer to fall back to RTP mode. • The **srtp** command enables secure calls. • The **fallback** keyword enables fallback to nonsecure mode (RTP) on an individual dial peer. The **no** form of this command disables fallback and disables SRTP. • The **system** keyword enables SRTP capability on a global level, rather than on the individual dial peer. This command defaults SRTP behavior to the global level. **Note** This dial-peer configuration command takes precedence over the globally configured **srtp** command enabled in voice service voip configuration mode.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current configuration mode.

Verifying and Troubleshooting Media and Signaling Authentication and Encryption Secure Call Configuration

This task verifies and troubleshoots secure call configuration.

SUMMARY STEPS

1. **show running-config**
2. **debug h245 srtp**
3. **show voice call status**
4. **show dial-peer voice** *number*

Step 1 To verify the configuration, use the **show running-config** command. Sample output is located in the "Global and Dial Peer SRTP Calls: Example" section on page 13.

Step 2 Use the **debug h245 srtp** command to display SRTP information exchanged during H.225 and H.245 signaling.

Step 3 Use the **show voice call status** command to verify the status of encrypted and decrypted packets:

a. Use the **show voice call status** command to display all voice ports and obtain the CallID of a specific call.

b. Use the **show voice call status** *call-id* command to display encrypted and decrypted packets for the specified call.

Step 4 Use the **show dial-peer voice** *number* command to display SRTP and fallback configuration status for a specific VoIP dial peer.

Configuration Examples for Secure Global and Dial Peer Calls

This section provides the following configuration example:

- Global and Dial Peer SRTP Calls: Example, page 13

Global and Dial Peer SRTP Calls: Example

The following ia a sample configuration of the Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature showing secure calls enabled globally on the originating gateway, without the capability to fall back to nonsecure mode:

```
Router# show running-config
```

Note The following sample configuration does not allow a call to fall back to nonsecure mode, that is, a user cannot make nonsecure calls.

```
Building configuration...

Current configuration : 2826 bytes
!
! Last configuration change at 15:23:32 UTC Sat Apr 20 2002
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service sequence-numbers
!
hostname router_1
!
boot-start-marker
boot-end-marker
!
logging buffered 6000000 debugging
enable password cisco
!
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate aim 0
no network-clock-participate aim 1
voice-card 1
 codec complexity secure
 dspfarm
!
voice-card 2
 no dspfarm
!
no aaa new-model
ip subnet-zero
```

```
ip cef
!
no ip domain lookup
ip host dirt 10.1.1.129
ip ips po max-events 100
no ftp-server write-enable
isdn switch-type primary-5ess
```

The following lines show SRTP enabled and fallback to nonsecure mode is disabled at the global level:

```
voice service voip
 srtp
 fax protocol pass-through g711ulaw
 h323
  call start slow
!
!
voice class codec 1
 codec preference 1 g711ulaw
!
voice class codec 2
 codec preference 1 g711ulaw
controller T1 1/0
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1/1
 framing esf
 linecode b8zs
!
no crypto isakmp enable
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.4.127.2 255.255.0.0
 duplex auto
 speed auto
!
interface Serial1/0:23
 no ip address
 isdn switch-type primary-5ess
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.4.0.1
!
ip http server
no ip http secure-server
control-plane
!
!
!
voice-port 1/0:23
```

```
!
voice-port 2/1/0
 connection plar 5550102
!
voice-port 2/1/1
!
voice-port 2/1/2
!
voice-port 2/1/3
!
!
!
!
dial-peer cor custom
!
dial-peer voice 100 pots
 destination-pattern 5550101
 incoming called-number 5550191
 direct-inward-dial
 port 1/0:23
 forward-digits all
!
dial-peer voice 101 voip
 destination-pattern 5550191
 modem passthrough nse codec g711ulaw
 voice-class codec 1
 session target ipv4:10.4.127.4
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 102 voip
 destination-pattern 5550102
 voice-class codec 1
 session target ipv4:10.4.127.4
 dtmf-relay rtp-nte
 no vad
dial-peer voice 200 pots
 destination-pattern 5550110
 incoming called-number 5550100
 port 2/1/1
!
dial-peer voice 201 voip
 destination-pattern 5550010
 voice-class codec 1
 session target ipv4:10.4.127.4
 no vad
!
dial-peer voice 300 pots
 destination-pattern 5550120
 incoming called-number 5550150
 port 2/1/2
!
dial-peer voice 301 voip
 destination-pattern 5550150
 voice-class codec 1
 session target ipv4:10.4.127.4
 no vad
!
gateway
 timer receive-rtp 1200
!
!
!
!
```

```
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 login
!
ntp master
end
```

The following ia a sample configuration of the Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature showing SRTP enabled on an individual dial peer on the terminating gateway with no fallback to nonsecure calls:

Note The following sample configuration does not allow a call to fall back to nonsecure mode; that is, a user cannot make nonsecure calls.

```
Router# show running-config

Building configuration...
config_dialpeer_srtp:52:voipPeerCfgSrtp: 0 srtp

Current configuration : 1932 bytes
!
! Last configuration change at 04:20:50 UTC Mon Mar 25 2002
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service sequence-numbers
!
hostname router_2
!
boot-start-marker
boot-end-marker
!
logging buffered 6000000 debugging
enable password cisco
!
no network-clock-participate slot 1
no network-clock-participate aim 0
no network-clock-participate aim 1
voice-card 1
 codec complexity secure
 dspfarm
!
no aaa new-model
no ip subnet-zero
ip cef
!
no ip domain lookup
ip ips po max-events 100
no ftp-server write-enable
isdn switch-type primary-5ess
!
voice service voip
 h323
!
```

```
!
voice class codec 1
 codec preference 1 g711alaw
!
voice class codec 2
 codec preference 1 g711alaw
!
controller T1 1/0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-20,24
!
controller T1 1/1
 framing esf
 clock source internal
 linecode b8zs
!
no crypto isakmp enable
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.4.127.3 255.255.0.0
 duplex auto
 speed auto
!
interface Serial1/0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-5ess
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.4.0.1
!
ip http server
no ip http secure-server
!
!
!
control-plane
!
voice-port 1/0:23
!
dial-peer cor custom
!
dial-peer voice 100 pots
 destination-pattern 5550101
 incoming called-number 5550191
 port 1/0:23
 prefix 5550101
```

The following lines show SRTP is enabled with no fallback to nonsecure mode on dial peer 101:

```
dial-peer voice 101 voip
 destination-pattern 5550101
 voice-class codec 1
```

```
 session target ipv4:10.4.127.4
 srtp
 no vad
!
gateway
 timer receive-rtp 1200
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 login
!
ntp clock-period 17179218
ntp server 10.4.127.2
end
```

The following is a sample configuration of the Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature showing secure calls disabled on a Cisco IOS IP-to-IP gateway:

Note The following sample configuration does not allow secure calls on dial peer 101; that is, a user cannot make secure calls.

```
Router# show running-config

Building configuration...
Current configuration : 2130 bytes
!
! Last configuration change at 04:20:47 UTC Mon Mar 25 2002
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service sequence-numbers
!
hostname router_2
!
boot-start-marker
boot system flash:c3745-ipvoice-mz
boot-end-marker
!
logging buffered 6000000 debugging
enable password cisco
!
no network-clock-participate slot 2
network-clock-participate slot 3
no network-clock-participate aim 0
network-clock-participate aim 1
no aaa new-model
ip subnet-zero
no ip cef
!
ip ips po max-events 100
no ftp-server write-enable
voice-card 2
 no dspfarm
!
```

The following lines show H.323 connections are enabled on a Cisco IOS IP-to-IP gateway:

```
voice service voip
 allow-connections h323 to h323
 h323
!
voice class codec 1
 codec preference 1 g711alaw
!
voice class codec 2
 codec preference 1 g711alaw
!
controller E1 3/0
!
controller E1 3/1
!
no crypto isakmp enable
!
interface FastEthernet0/0
 ip address 10.4.127.4 255.255.0.0
 no ip mroute-cache
 load-interval 30
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip default-gateway 10.4.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.4.0.1
!
no ip http server
no ip http secure-server
!
control-plane
!
dial-peer cor custom
!
dial-peer voice 1 voip
 description OGW->TGW [H.323->H.323]
 voice-class codec 2
 incoming called-number 408....
 no vad
!
dial-peer voice 10 voip
 description OGW->TGW [H.323->H.323]
 destination-pattern 408....
 voice-class codec 2
 session target ipv4:10.4.127.3
 no vad
!
dial-peer voice 2 voip
 description TGW->OGW [H.323->H.323]
 voice-class codec 1
 incoming called-number 919....
 no vad
```

```
!
dial-peer voice 20 voip
 description TGW->OGW [H.323->H.323]
 destination-pattern 919....
 voice-class codec 1
 session target ipv4:10.4.127.2
 no vad
```

The following lines show that secure calls are not enabled on the individual dial peer, and there is no fallback to nonsecure mode:

```
dial-peer voice 101 voip
 no srtp
!
gateway
 timer receive-rtcp 30
 timer receive-rtp 1200
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 30 0
 password cisco
 login
!
ntp clock-period 17173803
ntp server 10.4.127.2
end
```

Additional References

The following sections provide references related to the Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways feature.

Related Documents

Related Topic	Document Title
Cisco CallManager security configuration	*Cisco CallManager Security Guide,* Release 5.0
Cisco IOS H.323 configuration	*Cisco IOS H.323 Configuration Guide*
Cisco IOS voice configuration	*Cisco IOS Voice Configuration Library*
Cisco IOS voice command reference	*Cisco IOS Voice Command Reference,* Release 12.4T
Advanced Encryption Standard (AES) feature	*Advanced Encryption Standard*
IPSec configuration	*Cisco IOS Security Configuration Guide,* Release 12.4
IPSec commands	*Cisco IOS Security Command Reference,* Release 12.4T

Standards

Standards	Title
IETF draft draft-ietf-mmusic-sdescriptions-02.txt	*Security Descriptions for Media Streams*
IETF draft draft-ietf-avt-srtp-09.txt	*Secure Real-time Transport Protocol*

MIBs

MIBs	MIBs Link
No new or modified MIBS are supported by this feature, and support for existing MIB has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Voice Command Reference* at http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html and the *Cisco IOS Debug Command Reference* at

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **debug h245 srtp**
- **show dial-peer voice**
- **srtp (dial-peer)**
- **srtp (voice)**

Feature Information for Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways

Feature Name	Releases	Feature Information
Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways	12.4(6)T1	This feature was introduced.

Glossary

CLI—command-line interface.

HMAC—Hashed Message Authentication Codes.

IETF—Internet Engineering Task Force. Standards body for Internet Standards.

IPSec—IP security.

PIN—personal identification number.

RTCP—Real-Time Transport Protocol Control Protocol.

RTP—Real-Time Transport Protocol

SHA1—Secure Hash Algorithm1.

SRTP—Secure RTP.

SRTCP—Secure RTCP.

VoIP—Voice over IP.