Cisco UBE Support for SRTP-RTP Internetworking

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature allows secure enterprise-to-enterprise calls and provides operational enhancements for Session Initiation Protocol (SIP) trunks from Cisco Unified Call Manager and Cisco Unified Call Manager Express. Support for Secure Real-Time Transport Protocol (SRTP)-Real-Time Transport Protocol (RTP) internetworking between one or multiple Cisco Unified Border Elements (Cisco UBEs) is enabled for SIP-SIP audio calls.

In Cisco IOS Release 15.2(1) and Cisco IOS XE Release 3.7S, the SRTP-RTP Interworking feature was extended to support supplementary services on Cisco UBEs.

Prerequisites for CUBE Support for SRTP-RTP Internetworking

- The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature is supported in Cisco Unified CallManager 7.0 and later releases.

Cisco Unified Border Element

- Cisco IOS Release 12.4(22)YB or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.7S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for CUBE Support for SRTP-RTP Internetworking

The following features are not supported by the Cisco Unified Border Element Support for SRTP-RTP Internetworking feature:

- Asymmetric SRTP fallback configurations
- Call admission control (CAC) support
- Rotary SIP-SIP
- SRTCP-RTCP interworking
- SRTP-RTP and SRTP-SRTP video calls
- Transcoding for SRTP-SRTP audio calls

Information About CUBE for SRTP-RTP Internetworking

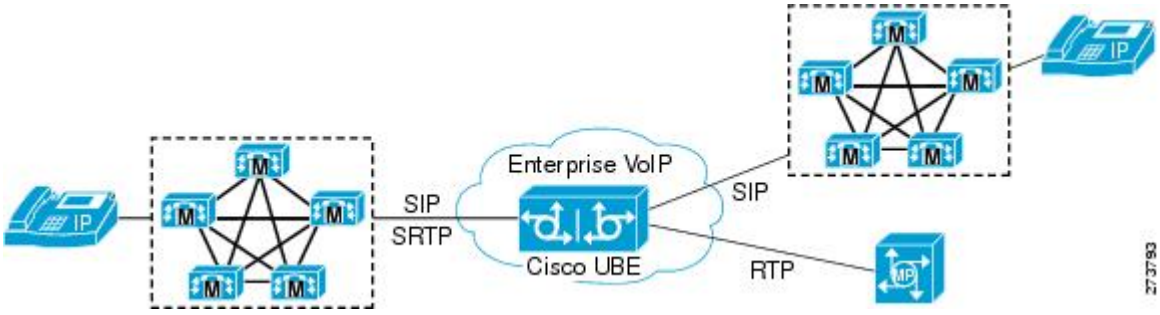
To configure support for SRTP-RTP internetworking, you should understand the following concepts:

CUBE Support for SRTP-RTP Internetworking

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature connects SRTP Cisco Unified CallManager domains with the following:

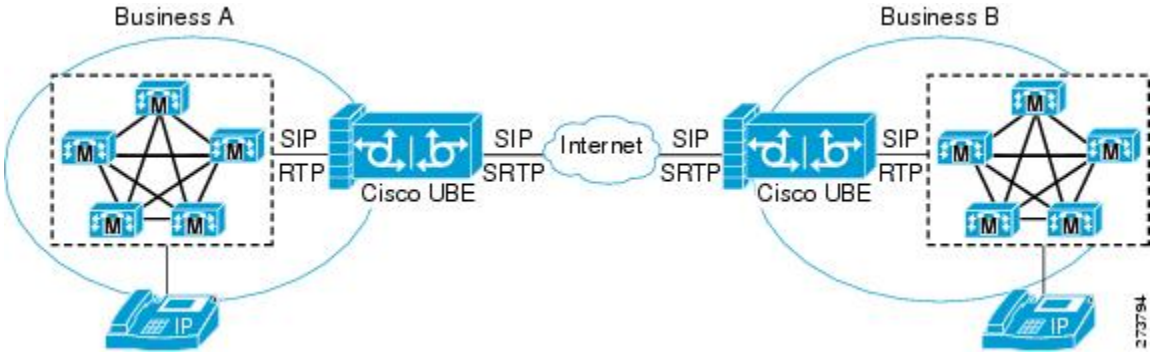
- RTP Cisco Unified CallManager domains. Domains that do not support SRTP or have not been configured for SRTP, as shown in the figure below.
- RTP Cisco applications or servers. For example, Cisco Unified MeetingPlace, Cisco WebEx, or Cisco Unity, which do not support SRTP, or have not been configured for SRTP, or are resident in a secure data center, as shown in the figure below.
- RTP to third-party equipment. For example, IP trunks to PBXs or virtual machines, which do not support SRTP.

Figure 1: SRTP Domain Connections



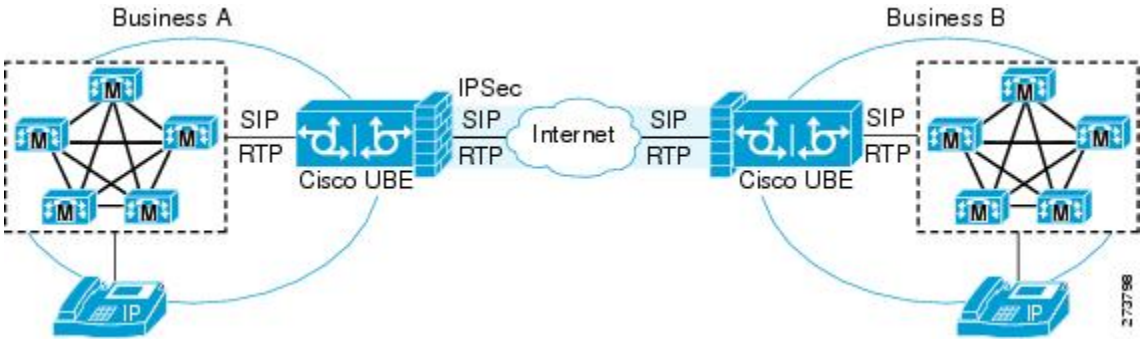
The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature connects SRTP enterprise domains to RTP SIP provider SIP trunks. SRTP-RTP internetworking connects RTP enterprise networks with SRTP over an external network between businesses. This provides flexible secure business-to-business communications without the need for static IPsec tunnels or the need to deploy SRTP within the enterprise, as shown in the figure below.

Figure 2: Secure Business-to-Business Communications



SRTP-RTP internetworking also connects SRTP enterprise networks with static IPsec over external networks, as shown inthe figure below.

Figure 3: SRTP Enterprise Network Connections



SRTP-RTP internetworking on the Cisco UBE in a network topology uses single-pair key generation. Existing audio and dual-tone multifrequency (DTMF) transcoding is used to support voice calls. SRTP-RTP internetworking support is provided in both flow-through and high-density mode. SRTP-SRTP pass-through is not impacted.

SRTP is configured on one dial peer and RTP is configured on the other dial peer using the **srtp** and **srtp fallback** commands. The dial-peer configuration takes precedence over the global configuration on the Cisco UBE.

Fallback handling occurs if one of the call endpoints does not support SRTP. The call can fall back to RTP-RTP, or the call can fail, depending on the configuration. Fallback takes place only if the **srtp fallback** command is configured on the respective dial peer. RTP-RTP fallback occurs when no transcoding resources are available for SRTP-RTP internetworking.

TLS on the Cisco Unified Border Element

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature allows Transport Layer Security (TLS) to be enabled or disabled between the Skinny Call Control Protocol (SCCP) server and the SCCP client. By default, TLS is enabled, which provides added protection at the transport level and ensures that SRTP keys are not easily accessible. Once TLS is disabled, the SRTP keys are not protected.

SRTP-RTP internetworking is available with normal and universal transcoders. The transcoder on the Cisco Unified Border Element is invoked using SCCP messaging between the SCCP server and the SCCP client. SCCP messages carry the SRTP keys to the digital signal processor (DSP) farm at the SCCP client. The transcoder can be within the same router or can be located in a separate router. TLS should be disabled only when the transcoder is located in the same router. To disable TLS, configure the **no** form of the **tls** command in dsp farm profile configuration mode. Disabling TLS improves CPU performance.

Supplementary Services Support on the Cisco UBE for RTP-SRTP Calls

The Supplementary Services Support on Cisco UBE for RTP-SRTP Calls feature supports the following supplementary services on the Cisco UBE:

- Midcall codec change with voice class codec configuration for SRTP-RTP and SRTP pass-through calls.
- Reinvite-based call hold.
- Reinvite-based call resume.
- Music on hold (MoH) invoked from the Cisco Unified Communications Manager (Cisco UCM), where the call leg changes between SRTP and RTP for an MoH source.

  Reinvite-based call forward.
- Reinvite-based call transfer.
- Call transfer based on a REFER message, with local consumption or pass-through of the REFER message on the Cisco UBE.
- Call forward based on a 302 message, with local consumption or pass-through of the 302 message on the Cisco UBE.
- T.38 fax switchover.
- Fax pass-through switchover.
- DO-EO for SRTP-RTP calls.
- DO-EO for SRTP pass-through calls.

When the initial SRTP-RTP or SRTP pass-through call is established on the Cisco UBE, a call can switch between SRTP and RTP for various supplementary services that can be invoked on the end points. Transcoder resources are used to perform SRTP-RTP conversion on Cisco UBE. When the call switches between SRTP and RTP, the transcoder is dynamically inserted, deleted, or modified. Both normal transcoding and high-density (optimized) transcoding are supported.

For call transfers involving REFER and 302 messages (messages that are locally consumed on Cisco UBE), end-to-end media renegotiation is initiated from Cisco UBE only when you configure the supplementary-service media-renegotiate command in voice service voip configuration mode.

When supplementary services are invoked from the end points, the call can switch between SRTP and RTP during the call duration. Hence, Cisco recommends that you configure such SIP trunks for SRTP fallback.

How to Configure Cisco UBE Support for SRTP-RTP Internetworking

Configuring Cisco UBE Support for SRTP-RTP Internetworking

Configuring the Certificate Authority

Perform the steps described in this section to configure the certificate authority.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **database level complete**
6. **grant auto**
7. **no shutdown**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server on your IPv4 or IPv6 system, including the Cisco web browser user interface.

	Command or Action	Purpose
Step 4	**crypto pki server** *cs-label* **Example:** `Device(config)# crypto pki server 3854-cube`	Enables a Cisco IOS certificate server and enters certificate server configuration mode. • In the example, 3854-cube is specified as the name of the certificate server.
Step 5	**database level complete** **Example:** `Device(cs-server)# database level complete`	Controls what type of data is stored in the certificate enrollment database. • In the example, each issued certificate is written to the database.
Step 6	**grant auto** **Example:** `Device(cs-server)# grant auto`	Specifies automatic certificate enrollment.
Step 7	**no shutdown** **Example:** `Device(cs-server)# no shutdown`	Reenables the certificate server. • Create and enter a new password when prompted.
Step 8	**exit** **Example:** `Device(cs-server)# exit`	Exits certificate server configuration mode.

Configuring a Trustpoint for the Secure Universal Transcoder

Perform the task in this section to configure, authenticate, and enroll a trustpoint for the secure universal transcoder.

Before You Begin

Before you configure a trustpoint for the secure universal transcoder, you should configure the certificate authority, as described in the Configuring the Certificate Authority, on page 5.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **serial-number**
6. **revocation-check** *method*
7. **rsakeypair** *key-label*
8. **end**
9. **crypto pki authenticate** *name*
10. **crypto pki enroll** *name*
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpoint** *name* **Example:** `Device(config)# crypto pki trustpoint secdsp`	Declares the trustpoint that the router uses and enters ca-trustpoint configuration mode. • In the example, the trustpoint is named secdsp.
Step 4	**enrollment url** *url* **Example:** `Device(ca-trustpoint)# enrollment url http://10.13.2.52:80`	Specifies the enrollment parameters of a certification authority (CA). • In the example, the URL is defined as http://10.13.2.52:80.
Step 5	**serial-number** **Example:** `Device(ca-trustpoint)# serial-number`	Specifies whether the router serial number should be included in the certificate request.

	Command or Action	Purpose
Step 6	**revocation-check** *method* **Example:** `Device(ca-trustpoint)# revocation-check crl`	Checks the revocation status of a certificate. • In the example, the certificate revocation list checks the revocation status.
Step 7	**rsakeypair** *key-label* **Example:** `Device(ca-trustpoint)# rsakeypair 3845-cube`	Specifies which key pair to associate with the certificate. • In the example, the key pair 3845-cube generated during enrollment is associated with the certificate.
Step 8	**end** **Example:** `Device(ca-trustpoint)# end`	Exits ca-trustpoint configuration mode.
Step 9	**crypto pki authenticate** *name* **Example:** `Device(config)# crypto pki authenticate secdsp`	Authenticates the CA. • Accept the trustpoint CA certificate if prompted.
Step 10	**crypto pki enroll** *name* **Example:** `Device(config)# crypto pki enroll secdsp`	Obtains the certificate for the router from the CA. • Create and enter a new password if prompted. • Request a certificate from the CA if prompted.
Step 11	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuring DSP Farm Services

Perform the task in this section to configure DSP farm services.

Before You Begin

Before you configure DSP farm services, you should configure the trustpoint for the secure universal transcoder, as described in the Configuring a Trustpoint for the Secure Universal Transcoder, on page 6.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot*
4. **dspfarm**
5. **dsp services dspfarm**
6. Repeat Steps 3, 4, and 5 to configure a second voice card.
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice-card** *slot* **Example:** `Device(config)# voice-card 0`	Configures a voice card and enters voice-card configuration mode. • In the example, voice card 0 is configured.
Step 4	**dspfarm** **Example:** `Device(config-voicecard)# dspfarm`	Adds a specified voice card to those participating in a DSP resource pool.
Step 5	**dsp services dspfarm** **Example:** `Device(config-voicecard)# dsp services dspfarm`	Enables DSP farm services for a particular voice network module.
Step 6	Repeat Steps 3, 4, and 5 to configure a second voice card.	--

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-voicecard)# exit`	Exits voice-card configuration mode.

Associating SCCP to the Secure DSP Farm Profile

Perform the task in this section to associate SCCP to the secure DSP farm profile.

Before You Begin

Before you associate SCCP to the secure DSP farm profile, you should configure DSP farm services, as described in the Configuring DSP Farm Services, on page 8.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp local** *interface-type interface-number*
4. **sccp ccm** *ip-address* **identifier** *identifier-number* **version** *version-number*
5. **sccp**
6. **associate ccm** *identifier-number* **priority** *priority-number*
7. **associate profile** *profile-identifier* **register** *device-name*
8. **dspfarm profile** *profile-identifier* **transcode universal security**
9. **trustpoint** *trustpoint-label*
10. **codec** *codec-type*
11. Repeat Step 10 to configure reuired codecs.
12. **maximum sessions** *number*
13. **associate application sccp**
14. **no shutdown**
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sccp local** *interface-type interface-number* **Example:** `Device(config)# sccp local GigabitEthernet 0/0`	Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco CallManager. • In the example, the following parameters are set: • GigabitEthernet is defined as the interface type that the SCCP application uses to register with Cisco CallManager. • The interface number that the SCCP application uses to register with Cisco CallManager is specified as 0/0.
Step 4	**sccp ccm** *ip-address* **identifier** *identifier-number* **version** *version-number* **Example:** `Device(config)# sccp ccm 10.13.2.52 identifier 1 version 5.0.1`	Adds a Cisco Unified Communications Manager server to the list of available servers. • In the example, the following parameters are set: • 10.13.2.52 is configured as the IP address of the Cisco Unified Communications Manager server. • The number 1 identifies the Cisco Unified Communications Manager server. • The Cisco Unified Communications Manager version is identified as 5.0.1.
Step 5	**sccp** **Example:** `Device(config)# sccp`	Enables SCCP and related applications (transcoding and conferencing) and enters SCCP Cisco CallManager configuration mode.
Step 6	**associate ccm** *identifier-number* **priority** *priority-number* **Example:** `Device(config-sccp-ccm)# associate ccm 1 priority 1`	Associates a Cisco Unified CallManager with a Cisco CallManager group and establishes its priority within the group. • In the example, the following parameters are set: • The number 1 identifies the Cisco Unified CallManager. • The Cisco Unified CallManager is configured with the highest priority within the Cisco CallManager group.
Step 7	**associate profile** *profile-identifier* **register** *device-name*	Associates a DSP farm profile with a Cisco CallManager group. • In the example, the following parameters are set:

	Command or Action	Purpose
	Example: `Device(config-sccp-ccm)# associate profile 1 register sxcoder`	• The number 1 identifies the DSP farm profile. • Sxcoder is configured as the user-specified device name in Cisco Unified CallManager.
Step 8	**dspfarm profile** *profile-identifier* **transcode universal security** **Example:** `Device(config-sccp-ccm)# dspfarm profile 1 transcode universal security`	Defines a profile for DSP farm services and enters DSP farm profile configuration mode. • In the example, the following parameters are set: • Profile 1 is enabled for transcoding. • Profile 1 is enabled for secure DSP farm services.
Step 9	**trustpoint** *trustpoint-label* **Example:** `Device(config-dspfarm-profile)# trustpoint secdsp`	Associates a trustpoint with a DSP farm profile. • In the example, the trustpoint to be associated with the DSP farm profile is labeled secdsp.
Step 10	**codec** *codec-type* **Example:** `Device(config-dspfarm-profile)# codec g711ulaw`	Specifies the codecs that are supported by a DSP farm profile. • In the example, the g711ulaw codec is specified.
Step 11	Repeat Step 10 to configure reuired codecs.	--
Step 12	**maximum sessions** *number* **Example:** `Device(config-dspfarm-profile)# maximum sessions 84`	Specifies the maximum number of sessions that are supported by the profile. • In the example, a maximum of 84 sessions are supported by the profile. The maximum number of sessions depends on the number of DSPs available for transcoding.
Step 13	**associate application sccp** **Example:** `Device(config-dspfarm-profile)# associate application sccp`	Associates SCCP to the DSP farm profile.
Step 14	**no shutdown** **Example:** `Device(config-dspfarm-profile)# no shutdown`	Allocates DSP farm resources and associates them with the application.

	Command or Action	Purpose
Step 15	**exit** **Example:** `Device(config-dspfarm-profile)# exit`	Exits DSP farm profile configuration mode.

Registering the Secure Universal Transcoder to the CUBE

Perform the task in this section to register the secure universal transcoder to the Cisco Unified Border Element. The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature supports both secure transcoders and secure universal transcoders.

Before You Begin

Before you register the secure universal transcoder to the Cisco Unified Border Element, you should associated SCCP to the secure DSP farm profile, as described in the Associating SCCP to the Secure DSP Farm Profile, on page 10.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **sdspfarm transcode sessions** *number*
5. **sdspfarm tag** *number device-name*
6. **em logout** *time1 time2 time3*
7. **max-ephones** *max-ephones*
8. **max-dn** *max-directory-numbers*
9. **ip source-address** *ip-address*
10. **secure-signaling trustpoint** *label*
11. **tftp-server-credentials trustpoint** *label*
12. **create cnf-files**
13. **no sccp**
14. **sccp**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device> configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Device(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**sdspfarm transcode sessions** *number* **Example:** `Device(config-telephony)# sdspfarm transcode sessions 84`	Specifies the maximum number of transcoding sessions allowed per Cisco CallManager Express router. • In the example, a maximum of 84 DSP farm sessions are specified.
Step 5	**sdspfarm tag** *number device-name* **Example:** `Device(config-telephony)# sdspfarm tag 1 sxcoder`	Permits a DSP farm to be to registered to Cisco Unified CallManager Express and associates it with an SCCP client interface's MAC address. • In the example, DSP farm 1 is associated with the sxcoder device.
Step 6	**em logout** *time1 time2 time3* **Example:** `Device(config-telephony)# em logout 0:0 0:0 0:0`	Configures three time-of-day-based timers for automatically logging out all Extension Mobility feature users. • In the example, all users are logged out from Extension Mobility after 00:00.
Step 7	**max-ephones** *max-ephones* **Example:** `Device(config-telephony)# max-ephones 4`	Sets the maximum number of Cisco IP phones to be supported by a Cisco CallManager Express router. • In the example, a maximum of four phones are supported by the Cisco CallManager Express router.
Step 8	**max-dn** *max-directory-numbers* **Example:** `Device(config-telephony)# max-dn 4`	Sets the maximum number of extensions (ephone-dns) to be supported by a Cisco Unified CallManager Express router. • In the example, a maximum of four extensions is allowed.

	Command or Action	Purpose
Step 9	**ip source-address** *ip-address* **Example:** `Device(config-telephony)# ip source-address 10.13.2.52`	Identifies the IP address and port through which IP phones communicate with a Cisco Unified CallManager Express router. • In the example, 10.13.2.52 is configured as the router IP address.
Step 10	**secure-signaling trustpoint** *label* **Example:** `Device(config-telephony)# secure-signaling trustpoint secdsp`	Specifies the name of the Public Key Infrastructure (PKI) trustpoint with the certificate to be used for TLS handshakes with IP phones on TCP port 2443. • In the example, PKI trustpoint secdsp is configured.
Step 11	**tftp-server-credentials trustpoint** *label* **Example:** `Device(config-telephony)# tftp-server-credentials trustpoint scme`	Specifies the PKI trustpoint that signs the phone configuration files. • In the example, PKI trustpoint scme is configured.
Step 12	**create cnf-files** **Example:** `Device(config-telephony)# create cnf-files`	Builds the XML configuration files that are required for IP phones in Cisco Unified CallManager Express.
Step 13	**no sccp** **Example:** `Device(config-telephony)# no sccp`	Disables SCCP and its related applications (transcoding and conferencing) and exits telephony-service configuration mode.
Step 14	**sccp** **Example:** `Device(config)# sccp`	Enables SCCP and related applications (transcoding and conferencing).
Step 15	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Configuring SRTP-RTP Internetworking Support

Perform the task in this section to enable SRTP-RTP internetworking support between one or multiple Cisco Unified Border Elements for SIP-SIP audio calls. In this task, RTP is configured on the incoming call leg and SRTP is configured on the outgoing call leg.

Before You Begin

Before you configure the Cisco Unified Border Element Support for SRTP-RTP Internetworking feature, you should register the secure universal transcoder to the Cisco Unified Border Element, as described in the Registering the Secure Universal Transcoder to the CUBE, on page 13.

Note The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature is available only on platforms that support transcoding on the Cisco Unified Border Element. The feature is also available only on secure Cisco IOS images on the Cisco Unified Border Element.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **destination-pattern** *string*
5. **session protocol sipv2**
6. **session target ipv4:** *destination-address*
7. **incoming called-number** *string*
8. **codec** *codec*
9. **end**
10. **dial-peer voice** *tag* **voip**
11. Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.
12. **srtp**
13. **codec** *codec*
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**dial-peer voice** *tag* **voip**
	
	Example:
	
	`Device(config)# dial-peer voice 201 voip`
		Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode.
		• In the example, the following parameters are set:
		  • Dial peer 201 is defined.
		  • VoIP is shown as the method of encapsulation.

Step 4	**destination-pattern** *string* **Example:** `Device(config-dial-peer)# destination-pattern 5550111`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer string. • In the example, 5550111 is specified as the pattern for the telephone number.
Step 5	**session protocol sipv2** **Example:** `Device(config-dial-peer)# session protocol sipv2`	Specifies a session protocol for calls between local and remote routers using the packet network. • In the example, the **sipv2** keyword is configured so that the dial peer uses the IEFTF SIP.
Step 6	**session target ipv4:** *destination-address* **Example:** `Device(config-dial-peer)# session target ipv4:10.13.25.102`	Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer. • In the example, the IP address of the dial peer to receive calls is configured as 10.13.25.102.
Step 7	**incoming called-number** *string* **Example:** `Device(config-dial-peer)# incoming called-number 5550111`	Specifies a digit string that can be matched by an incoming call to associate the call with a dial peer. • In the example, 5550111 is specified as the pattern for the E.164 or private dialing plan telephone number.
Step 8	**codec** *codec* **Example:** `Device(config-dial-peer)# codec g711ulaw`	Specifies the voice coder rate of speech for the dial peer. • In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config-dial-peer)#end`	Exits dial peer voice configuration mode.

Step 10	**dial-peer voice** *tag* **voip**
	
	Example:
	`Device(config)# dial-peer voice 200 voip`
		Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode.
		• In the example, the following parameters are set:
		  • Dial peer 200 is defined.
		  • VoIP is shown as the method of encapsulation.

Step 11	Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.	--
Step 12	**srtp** **Example:** `Device(config-dial-peer)# srtp`	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 13	**codec** *codec* **Example:** `Device(config-dial-peer)# codec g711ulaw`	Specifies the voice coder rate of speech for the dial peer. • In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 14	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial peer voice configuration mode.

Troubleshooting Tips

The following commands can help troubleshoot Cisco Unified Border Element support for SRTP-RTP internetworking:

- **show crypto pki certificates**
- **show sccp**
- **show sdspfarm**

Enabling SRTP on the Cisco UBE

You can configure SRTP with the fallback option so that a call can fall back to RTP if SRTP is not supported by the other call end. Enabling SRTP is required for supporting nonsecure supplementary services such as MoH, call forward, and call transfer.

Enabling SRTP Globally

Perform this task to enable SRTP globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **srtp fallback**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice-service configuration mode and specifies VoIP encapsulation as the voice-encapsulation type.
Step 4	**srtp fallback** **Example:** `RoDeviceuter(conf-voi-serv)# srtp fallback`	Enables call fallback to nonsecure mode. **Note** If the secure SIP trunk is towards the Cisco UCM, you must configure the **srtp negotiate cisco** command in voice-service configuration mode for a non-Cisco fallback to work.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(conf-voi-serv)# exit`	Exits voice service configuration mode.

Example: Enabling SRTP Globally

```
Device(config)# voice service voip
Device(conf-voi-serv)# srtp fallback
Device(conf-voi-serv)# exit
```

Enabling SRTP on a Dial Peer

Perform this task to enable SRTP on a dial peer.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 10 voip`	Defines a particular dial peer to specify VoIP as the method of voice encapsulation and enters dial peer voice configuration mode.

	Command or Action	Purpose
Step 4	**srtp fallback** **Example:** `Device(config-dial-peer)# srtp fallback`	Enables specific dial-peer calls to fall back to nonsecure mode. **Note** If the secure SIP trunk is towards the Cisco UCM, you must configure the **srtp negotiate cisco** command in dial peer voice configuration mode for a non-Cisco fallback to work.
Step 5	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial peer voice configuration mode.

Example: Enabling SRTP on a Dial Peer

```
Device(config)# dial-peer voice 10 voip
Device(config-dial-peer)# srtp fallback
Device(config-dial-peer)# exit
```

Troubleshooting Tips

The following commands can help troubleshoot SRTP-RTP supplementary services support on Cisco UBE:

- **debug ccsip all**
- **debug sccp all**
- **debug voip ccapi inout**

Verifying SRTP-RTP Supplementary Services Support on the Cisco UBE

Perform this task to verify the configuration for SRTP-RTP supplementary services support on the Cisco UBE. The **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. **enable**
2. **show call active voice brief**
3. **show sccp connection**
4. **show dspfarm dsp active**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show call active voice brief**
Displays call information for voice calls in progress.

Example:

```
Device# show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
ulticast call-legs: 0
Total call-legs: 4
0    : 1 12:49:45.256 IST Fri Jun 3 2011.1 +29060 pid:1 Answer 10008001 connected
 dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
 IP 10.45.40.40:7892 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a

0    : 2 12:49:45.256 IST Fri Jun 3 2011.2 +29060 pid:22 Originate 20009001 connected
 dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
 IP 10.45.40.40:7893 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a

0    : 3 12:50:14.326 IST Fri Jun 3 2011.1 +0 pid:0 Originate  connecting
 dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
 IP 10.45.34.252:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a

0    : 5 12:50:14.326 IST Fri Jun 3 2011.2 +0 pid:0 Originate  connecting
 dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
 IP 10.45.34.252:2000 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
```

Step 3 **show sccp connection**
Displays SCCP connection details.

Example:

```
Device# show sccp connection
sess_id    conn_id      stype mode     codec   sport rport ripaddr conn_id_tx

65537      4          s-xcode sendrecv g711u   17124 2000  10.45.34.252
65537      8            xcode sendrecv g711u   30052 2000  10.45.34.252

Total number of active session(s) 1, and connection(s) 2
```

Step 4 **show dspfarm dsp active**
Displays active DSP information about the DSP farm service.

Example:

```
Device# show dspfarm dsp active
SLOT DSP VERSION  STATUS CHNL USE   TYPE    RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED
```

```
0    1   30.0.209 UP     1    USED  xcode   1      4         2876      1706
0    1   30.0.209 UP     1    USED  xcode   1      5         1698      2876

Total number of DSPFARM DSP channel(s) 1
```

Configuration Examples for CUBE Support for SRTP-RTP Internetworking

SRTP-RTP Internetworking Example

The following example shows how to configure Cisco Unified Border Element support for SRTP-RTP internetworking. In this example, the incoming call leg is RTP and the outgoing call leg is SRTP.

```
enable
 configure terminal
 ip http server
 crypto pki server 3845-cube
  database level complete
  grant auto
  no shutdown
%PKI-6-CS_GRANT_AUTO: All enrollment requests will be automatically granted.
% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key or type Return to exit
Password:
Re-enter password:
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% SSH-5-ENABLED: SSH 1.99 has been enabled
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.
%PKI-6-CS_ENABLED: Certificate server now enabled.
!
crypto pki trustpoint secdsp
 enrollment url http://10.13.2.52:80
 serial-number
 revocation-check crl
 rsakeypair 3845-cube
 exit
!
crypto pki authenticate secdsp
Certificate has the following attributes:
 Fingerprint MD5: CCC82E9E 4382CCFE ADA0EB8C 524E2FC1
 Fingerprint SHA1: 34B9C4BF 4841AB31 7B0810AD 80084475 3965F140
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
crypto pki enroll secdsp
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate. For security reasons your password will
 not be saved in the configuration. Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: 3845-CUBE
% The serial number in the certificate will be: FHK1212F4MU
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate secdsp verbose' command will show the fingerprint.
```

```
CRYPTO_PKI:  Certificate Request Fingerprint MD5: 56CE5FC3 B8411CF3 93A343DA 785C2360
CRYPTO_PKI:  Certificate Request Fingerprint SHA1: EE029629 55F5CA10 21E50F08 F56440A2
DDC7469D
%PKI-6-CERTRET: Certificate received from Certificate Authority
!
voice-card 0
 dspfarm
 dsp services dspfarm
 voice-card 1
 dspfarm
 dsp services dspfarm
 exit
!
sccp local GigabitEthernet 0/0
sccp ccm 10.13.2.52 identifier 1 version 5.0.1
sccp
SCCP operational state bring up is successful.sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register sxcoder
 dspfarm profile 1 transcode universal security
  trustpoint secdsp
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec g729r8
  codec ilbc
  codec g729br8
  maximum sessions 84
  associate application sccp
  no shutdown
  exit
!
telephony-service
%LINEPROTO-5-UPDOWN: Line protocol on Interface EDSP0, changed state to upsdspfarm units 1
 sdspfarm transcode sessions 84
 sdspfarm tag 1 sxcoder
 em logout 0:0 0:0 0:0
 max-ephones 4
 max-dn 4
 ip source-address 10.13.2.52
Updating CNF files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
CNF files updating complete
 secure-signaling trustpoint secdsp
 tftp-server-credentials trustpoint scme
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
CNF files update complete (post init)
 create cnf-files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
 no sccp
!
sccp
SCCP operational state bring up is successful.
end
%SDSPFARM-6-REGISTER: mtp-1:sxcoder IP:10.13.2.52 Socket:1 DeviceType:MTP has registered.
%SYS-5-CONFIG_I: Configured from console by console
dial-peer voice 201 voip
 destination-pattern 5550111
 session protocol sipv2
 session target ipv4:10.13.25.102
 incoming called-number 5550112
 codec g711ulaw
!
dial-peer voice 200 voip
 destination-pattern 5550112
 session protocol sipv2
 session target ipv4:10.13.2.51
 incoming called-number 5550111
 srtp
 codec g711ulaw
```

Feature Information for CUBE Support for SRTP-RTP Internetworking

Table 1: Feature Information for Cisco Unified Border Element Support for SRTP-RTP Internetworking

Feature Name	Releases	Feature Information
Cisco Unified Border Element Support for SRTP-RTP Internetworking	12.4(22)YB , 15.0(1)M	This feature allows secure enterprise-to-enterprise calls. Support for SRTP-RTP internetworking between one or multiple Cisco Unified Border Elements is enabled for SIP-SIP audio calls. The following sections provide information about this feature: The following command was introduced: **tls**.
Supplementary Services Support on Cisco UBE for RTP-SRTP Calls	15.2(1)T	The SRTP-RTP Internetworking feature was enhanced to support supplementary services for SRTP-RTP calls on Cisco UBE.
Supplementary Services Support on Cisco UBE for RTP-SRTP Calls	Cisco IOS XE Release 3.7S	The SRTP-RTP Internetworking feature was enhanced to support supplementary services for SRTP-RTP calls on Cisco UBE.