Configuring Voice Functionality

This chapter provides information about configuring voice functionality on the Cisco 4000 Series Integrated Services Routers (ISRs).

This chapter includes these sections:

Call Waiting

With the Call Waiting feature, you can receive a second call while you are on the phone attending to another call. When you receive a second call, you hear a call-waiting tone (a tone with a 300 ms duration). Caller ID appears on phones that support caller ID. You can use hookflash to answer a waiting call and place the previously active call on hold. By using hookflash, you can toggle between the active and a call that is on hold. If the Call Waiting feature is disabled, and you hang up the current call, the second call will hear a busy tone. For more information on Call Waiting, see http://www.cisco.com/c/en/us/td/docs/ios/voice/sip/configuration/guide/15_0/sip_15_0_book/sip_cg-hookflash.html#wp999028

Call Transfers

Call transfers are when active calls are put on hold while a second call is established between two users. After you establish the second call and terminate the active call, the call on hold will hear a ringback. The Call Transfer feature supports all three types of call transfers—blind, semi-attended, and attended. For more information on Call Transfers, see the http://www.cisco.com/c/en/us/td/docs/ios/voice/sip/configuration/guide/15_0/sip_15_0_book/sip_cg-hookflash.html#wp999084

E1 R2 Signaling Configuration

To configure the E1 R2, perform these steps:

Before you begin

Before you attempt this configuration, ensure that you meet these prerequisites:

- R2 signaling applies only to E1 controllers.
- In order to run R2 signaling on Cisco 4000 Series ISRs, this hardware is required:
- NIM-MFT-1T1/E1 or NIM-2MFT-T1/E1 or NIM-4MFT-T1/E1or NIM-8MFT-T1/E1 or NIM-1CE1T1-PRI or NIM-2CE1T1-PRI or NIM-8CE1T1-PRI
- Define the command ds0-group on the E1 controllers of Cisco 4000 Series ISRs.
- Cisco IOS XE software release 15.5 (2)

SUMMARY STEPS

1. Set up the controller E1 that connects to the private automatic branch exchange (PBX) or switch.
2. For E1 framing, choose either **CRC** or **non-CRC**
3. For E1 linecoding, choose either **HDB3** or **AMI**.
4. For the E1 clock source, choose either internal or line. Note that different PBXs have different requirements on the clock source.
5. Configure line signaling.
6. Configure interregister signaling.
7. Customize the configuration with the cas-custom command.

DETAILED STEPS

Step 1 Set up the controller E1 that connects to the private automatic branch exchange (PBX) or switch.

Ensure that the framing and linecoding of the E1 are properly set.

Step 2 For E1 framing, choose either **CRC** or **non-CRC**

Step 3 For E1 linecoding, choose either **HDB3** or **AMI**.

Step 4 For the E1 clock source, choose either internal or line. Note that different PBXs have different requirements on the clock source.

Step 5 Configure line signaling.

```
(config)# controller E1 0/2/0


 (config-controller)#ds0-group 1 timeslots 1 type ?
...
r2-analog        R2 ITU Q411
r2-digital       R2 ITU Q421
r2-pulse         R2 ITU Supplement 7
...
```

Step 6 Configure interregister signaling.

```
(config)# controller E1 0/2/0

 eefje(config)# controller E1 0/2/0
 eefje(config-controller)#ds0-group 1 timeslots 1 type r2-digital ?
dtmf              DTMF tone signaling
r2-compelled      R2 Compelled Register Signaling
```

```
r2-non-compelled   R2 Non Compelled Register Signaling
r2-semi-compelled  R2 Semi Compelled Register Signaling

...
```

The Cisco implementation of R2 signaling has Dialed Number Identification Service (DNIS) support enabled by default. If you enable the Automatic Number Identification (ANI) option, the collection of DNIS information is still performed. Specification of the ANI option does not disable DNIS collection. DNIS is the number that is called and ANI is the number of the caller. For example, if you configure a router called A to call a router called B, then the DNIS number is assigned to router B and the ANI number is assigned to router A. ANI is similar to caller ID.

Step 7 Customize the configuration with the cas-custom command.

```
(config)# controller E1 0/2/0


(config-controller)#ds0-group 1 timeslots 1 type r2-digital r2-compelled ani
cas-custom 1
  country brazil
  metering
  answer-signal group-b 1

voice-port 0/2/0:1
!
dial-peer voice 200 pots
destination-pattern 43200
direct-inward-dial
port 0/2/0:1

dial-peer voice 3925 voip
destination-pattern 39...
session target ipv4:10.5.25.41
...
```

R2 Configurations

The configurations have been modified in order to show only the information that this document discusses.

Configured for R2 Digital Non-Compelled

```
hostname eefje
!
controller E1 0
 clock source line primary
 dso-group 1 timeslots 1-15 type r2-digital r2-non-compelled
 cas-custom 1

!--- For more information on these commands
!--- refer to
ds0-group
 and
cas-custom.

!
voice-port 0:1
 cptone BE

!--- The cptone command is country specific. For more
!--- information on this command,  refer to
```

```
cptone
.

!
dial-peer voice 123 pots
 destination-pattern 123
 direct-inward-dial
 port 0:1
 prefix 123
!
dial-peer voice 567 voip
 destination-pattern 567
 session target ipv4:10.0.0.2
```

Configured for R2 Digital Semi-Compelled

```
hostname eefje
!
controller E1 0
 clock source line primary
 ds0-group 1 timeslots 1-15 type r2-digital r2-semi-compelled
 cas-custom 1

!--- For more information on these commands
!---  refer to
ds0-group
 and
cas-custom
.

!
voice-port 0:1
 cptone BE

!--- The cptone command is country specific. For more
!--- information on this command,  refer to
cptone
.

dial-peer voice 123 pots
 destination-pattern 123
 direct-inward-dial
 port 0:1
 prefix 123
!
dial-peer voice 567 voip
 destination-pattern 567
 session target ipv4:10.0.0.2
```

Configured for R2 Digital Compelled ANI

```
hostname eefje
! controller E1 0 clock source line primary ds0-group
1 timeslots 1-15 type r2-digital r2-compelled ani cas-custom 1

!--- For more information on these commands
!---  refer to
ds0-group
 and
cas-custom
.

voice-port 0:1 cptone BE

!--- The cptone command is country specific. For more
!--- information on this command,  refer to
```

```
cptone
.

dial-peer voice 123 pots destination-pattern 123 direct-inward-dial port
0:1 prefix 123
!
dial-peer voice 567 voip destination-pattern 567 session
target ipv4:10.0.0.2
```

Sample Debug Command Output

This example shows the output for the **debug vpm sig** command.

```
(config-controller)#debug vpm sig
Syslog logging: enabled
(0 messages dropped, 9 messages rate-limited, 1 flushes, 0 overruns,
 xml disabled, filtering disabled)No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging:  level debugging, 163274 messages logged, xml disabled,filtering disabled

Exception Logging: size (4096 bytes)    Count and timestamp logging messages: disabled
Persistent logging: disabledNo active filter modules.
Trap logging: level informational, 172 message lines logged
Logging Source-Interface:
VRF Name:Log Buffer (4096 bytes):0): DSX (E1 0/2/0:0): STATE: R2_IN_COLLECT_DNIS R2 Got
Event 1
*Jan 29 21:32:22.258:r2_reg_generate_digits(0/2/0:1(1)): Tx digit '1'
*Jan 29 21:32:22.369: htsp_digit_ready(0/2/0:1(1)): Rx digit='#'
*Jan 29 21:32:22.369: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0):STATE: R2_IN_COLLECT_DNIS
R2 Got Event R2_TONE_OFF
*Jan 29 21:32:22.369: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '#'
*Jan 29 21:32:22.569: htsp_dialing_done(0/2/0:1(1))
*Jan 29 21:32:25.258: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0):STATE: R2_IN_COLLECT_DNIS
R2 Got Event R2_TONE_TIMER
*Jan 29 21:32:25.258: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '3#'
*Jan 29 21:32:25.520: htsp_digit_ready_up(0/2/0:1(1)): Rx digit='1'
*Jan 29 21:32:25.520: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_CATEGORY R2
Got Event 1
*Jan 29 21:32:25.520: Enter r2_comp_category
*Jan 29 21:32:25.520: R2 Event : 1
*Jan 29 21:32:25.520:  ####### collect_call_enable = 0
*Jan 29 21:32:25.520: ######## Not Sending B7 ###################
*Jan 29 21:32:25.520: r2_reg_event_proc(0/2/0:1(1)) ADDR_INFO_COLLECTED (DNIS=39001,
ANI=39700)
*Jan 29 21:32:25.520: r2_reg_process_event: [0/2/0:1(1), R2_REG_COLLECTING,
E_R2_REG_ADDR_COLLECTED(89)]
*Jan 29 21:32:25.520: r2_reg_ic_addr_collected(0/2/0:1(1))htsp_switch_ind
*Jan 29 21:32:25.521: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_SETUP_ACK]
*Jan 29 21:32:25.521: r2_q421_ic_setup_ack(0/2/0:1(1)) E_HTSP_SETUP_ACK
*Jan 29 21:32:25.521: r2_reg_switch(0/2/0:1(1))
*Jan 29 21:32:25.521: r2_reg_process_event: [0/2/0:1(1), R2_REG_WAIT_FOR_SWITCH,
E_R2_REG_SWITCH(96)]
*Jan 29 21:32:25.521: r2_reg_ic_switched(0/2/0:1(1))
*Jan 29 21:32:25.522: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_PROCEEDING]
*Jan 29 21:32:25.530:htsp_call_bridged invoked
*Jan 29 21:32:25.530: r2_reg_event_proc(0/2/0:1(1)) ALERTING RECEIVED
*Jan 29 21:32:25.530: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_WAIT_REMOTE_ALERT
 R2 Got Event R2_ALERTING
*Jan 29 21:32:25.530:rx R2_ALERTING in r2_comp_wait_remote_alert
*Jan 29 21:32:25.530: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '1'htsp_alert_notify
```

```
*Jan 29 21:32:25.531:r2_reg_event_proc(0/2/0:1(1)) ALERTING RECEIVED
*Jan 29 21:32:25.531: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_COMPLETE R2
Got Event R2_ALERTING
*Jan 29 21:32:25.540: htsp_dsp_message: RESP_SIG_STATUS: state=0x0 timestamp=0
systime=80352360
*Jan 29 21:32:25.540:htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER, E_DSP_SIG_0000]
*Jan 29 21:32:25.651: htsp_dialing_done(0/2/0:1(1))
*Jan 29 21:32:25.751: htsp_digit_ready(0/2/0:1(1)): Rx digit='#'
*Jan 29 21:32:25.751: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_COMPLETE R2
Got Event R2_TONE_OFF
*Jan 29 21:32:25.751: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '#'
*Jan 29 21:32:25.961: htsp_dialing_done(0/2/0:1(1))
*Jan 29 21:32:26.752: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_WAIT_GUARD R2
 Got Event R2_TONE_TIMER
*Jan 29 21:32:26.752: R2_IN_CONNECT: call end dial
*Jan 29 21:32:26.752: r2_reg_end_dial(0/2/0:1(1))htsp_call_service_msghtsp_call_service_msg
 not EFXS (11)htsp_call_service_msghtsp_call_service_msg not EFXS (11)
*Jan 29 21:32:26.754: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_VOICE_CUT_THROUGH]
*Jan 29 21:32:26.754: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_VOICE_CUT_THROUGH]
*Jan 29 21:32:26.754: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_VOICE_CUT_THROUGH]
*Jan 29 21:32:51.909: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER, E_HTSP_CONNECT]
*Jan 29 21:32:51.909: r2_q421_ic_answer(0/2/0:1(1)) E_HTSP_CONNECT
*Jan 29 21:32:51.909: r2_q421_ic_answer(0/2/0:1(1)) Tx ANSWER seizure: delay 0 ms,elapsed
32419 msvnm_dsp_set_sig_state:[R2 Q.421 0/2/0:1(1)] set signal state = 0x4
*Jan 29 21:32:51.910: r2_reg_channel_connected(0/2/0:1(1))
*Jan 29 21:32:51.910: r2_reg_process_event: [0/2/0:1(1), R2_REG_WAIT_FOR_CONNECT,
E_R2_REG_CONNECT(90)]
*Jan 29 21:32:51.910: r2_reg_connect(0/2/0:1(1))htsp_call_service_msghtsp_call_service_msg
 not EFXS (11)
```

This example shows the output for the **debug vtsp all** command.

```
(config-controller)#debug vtsp all
Log Buffer (4096 bytes)::S_R2_DIALING_COMP, event:E_VTSP_DIGIT_END]
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/dc_digit:
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_R2_DIALING_COMP, event:E_TSP_R2_DIAL]
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/dc_dial:
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dial_nopush:
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/ds_do_dial:     Digits To
Dial=#
*Jan 29 21:56:33.901: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_dial_done_cb:
*Jan 29 21:56:33.901: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_R2_DIALING_COMP, event:E_VTSP_DSM_DIALING_COMPLETE]
*Jan 29 21:56:33.901: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/dc_dialing_done:
*Jan 29 21:56:34.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_R2_DIALING_COMP, event:E_TSP_R2_END_DIAL]
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/ds_end_dial:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_digit_pop:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_digit_pop:     Digit
Reporting=FALSE
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_alert_dial_complete:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_service_msg_down:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_timer_stop:     Timer
Stop Time=80497275
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_peer_event_cb:
Event=E_DSM_CC_CAPS_ACK
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_service_msg_down:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_timer_stop:     Timer
Stop Time=80497275
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_peer_event_cb:
```

```
Event=E_DSM_CC_CAPS_ACK
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_peer_event_cb:
Event=E_DSM_CC_CAPS_ACK
*Jan 29 21:56:34.692: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_feature_notify_cb:
    Feature ID=0, Feature Status=1
*Jan 29 21:56:34.692: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:

*Jan 29 21:56:34.692:
//213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:exit@1299
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_feature_notify_cb:
    Feature ID=0, Feature Status=1
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:

*Jan 29 21:56:34.693:
//213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:exit@1299
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_feature_notify_cb:
    Feature ID=0, Feature Status=1
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:

*Jan 29 21:56:34.693:
//213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:exit@1299
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_call_connect: Connected
 Name
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_call_connect: Connected
 Number 39701
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_call_connect: Connected
 oct3a  30
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_ALERTING, event:E_CC_CONNECT]
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_alert_connect:    Progress
 Indication=2
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_ring_noan_timer_stop:
   Timer Stop Time=80499620
*Jan 29 21:56:58.142: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_CONNECT, event:E_CC_SERVICE_MSG]
*Jan 29 21:56:58.142: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_service_msg_down:
*Jan 29 21:56:58.142: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_timer_stop:     Timer
Stop Time=80499620
*Jan 29 21:56:58.144: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_fpi_event_cb:
Event=E_DSMP_FPI_ENABLE_TDM_RTCP
```

Feature Group D Configuration

To configure the Feature Group D signaling, perform these steps:

Before you begin

The Feature Group D signaling is supported on Cisco 4000 Series Integrated Services Routers from IOS XE release 15.5 (2). Feature Group D service is a trunk side connection that enables telephone customers to choose their long distance network and use the same number of digits irrespective of carrier they use. Routers interface with interexchange carriers using Feature Group D to support voice traffic in the carrier environment.

Before you attempt this configuration, ensure that you meet these prerequisites:

- The platform must be using Digital T1/E1 Packet Voice Trunk Network Modules.

- The Digital T1/E1 Packet Voice Trunk Network Module can have one or two slots for voice/WAN Interface Network Modules (NIMs); NIM supports one to eight ports. Only the dual-mode (voice/WAN) multiple trunk cards are supported in the digital E1 packet voice trunk network module, not older VICs.
- Drop-and-Insert capability is supported only between two ports on the same multiple card.

SUMMARY STEPS

1. **configure terminal** {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. **voice-card slot/subslot**
3. **controller T1/E1 slot/subslot/port**
4. **framing** {*sf* | *esf* }
5. **linecode** {*b8zs* | *ami*}
6. **ds0-group** *ds0-group-no***timeslots** `timeslot-list type`{*e&m-fgd* | *fgd-eana*}
7. **no shutdown**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** {*ip-address* | *interface-type interface-number* [*ip-address*]} **Example:** `Router(config)# configure terminal`	Enters global configuration mode.
Step 2	**voice-card slot/subslot** **Example:** `Router(config)# voice-card slot/subslot`	Enters voice card interface configuration mode and specify the slot location by using a value from 0 to 5, depending upon your router.
Step 3	**controller T1/E1 slot/subslot/port** **Example:** `Router(config)# controller T1 slot/subslot/port`	Enters controller configuration mode for the T1 controller at the specified slot/port location. Valid values for slot and port are 0 and 1.
Step 4	**framing** {*sf* | *esf* } **Example:** `Router(config)# framing {sf | esf}`	Sets the framing according to your service provider's instructions. Choose Extended Superframe (ESF) format or Superframe (SF) format.
Step 5	**linecode** {*b8zs* | *ami*}	Sets the line encoding according to your service provider's instructions. Bipolar-8 zero substitution (B8ZS) encodes a sequence of eight zeros in a unique binary sequence to detect line coding violations. Alternate mark inversion (AMI) represents zeros using a 01 during each bit cell, and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density.

	Command or Action	Purpose
		Ones density is not maintained independent of the data stream.
Step 6	**ds0-group** *ds0-group-no* **timeslots** *timeslot-list* *type*{*e&m-fgd* | *fgd-eana*}	Defines the T1 channels for use by compressed voice calls as well as the signaling method the router uses to connect to the PBX or CO. ds0-group-no is a value from 0 to 23 that identifies the DS0 group. Note The ds0-group command automatically creates a logical voice port that is numbered as follows: slot/port:ds0-group-no. Although only one voice port is created, applicable calls are routed to any channel in the group. timeslot-list is a single number, numbers separated by commas, or a pair of numbers separated by a hyphen to indicate a range of timeslots. For T1, allowable values are from 1 to 24. To map individual DS0 timeslots, define additional groups. The system maps additional voice ports for each defined group. The signaling method selection for type depends on the connection that you are making. The e&m-fgd setting allows E&M interface connections for PBX trunk lines (tie lines) and telephone equipment to use feature group D switched-access service. The fgd-eana setting supports the exchange access North American (EANA) signaling.
Step 7	**no shutdown**	Activates the controller.
Step 8	**exit**	Exits controller configuration mode. Skip the next step if you are not setting up Drop and Insert .

Media and Signaling Authentication and Encryption

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature implements voice security features that include signaling authentication along with media and signaling encryption on MGCP gateways. For more information on Media and Signaling Authentication and Encryption Feature, see the http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/mgcp/configuration/15-mt/vm-15-mt-book/vm-gw-med-sig.html

Multicast Music-on-Hold

The Music-on-Hold (MOH) feature enables you to subscribe to a music streaming service when you are using a Cisco IOS MGCP voice gateway. Music streams from an MOH server to the voice interfaces of on-net and off-net callers that have been placed on hold. Cisco Communications Manager supports the capability to place callers on hold with music supplied from a streaming multicast MOH server.

By means of a preconfigured multicast address on the Cisco Unified Communications Manager or gateway, the gateway can "listen" for Real-Time Transport Protocol (RTP) packets that are broadcast from a default router in the network and can relay the packets to designated voice interfaces in the network. You can initiate the call on hold. However, you cannot initiate music on hold on a MGCP controlled analog phone. Whenever

a called party places a calling party on hold, Cisco Communications Manager requests the MOH server to stream RTP packets to the "on-hold" interface through the preconfigured multicast address. In this way, RTP packets are relayed to appropriately configured voice interfaces that have been placed on hold. When you configure a multicast address on a gateway, the gateway sends an Internet Gateway Management Protocol (IGMP) "join" message to the default router, indicating to the default router that the gateway is ready to receive RTP multicast packets.

Multiple MOH servers can be present in the same network, but each server must have a different Class D IP address, and the address must be configured in Cisco Communications Manager and the MGCP voice gateways. For more information on configuring MOH, see the http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cminterop/configuration/15-0m/vc-15-0m-book/vc-ucm-mgcp-gw.html#GUID-A3461142-2F05-4420-AEE6-032FCA3B7952

TLS 1.2 support on SCCP Gateways

The TLS 1.2 support on SCCP Gateways feature details the configuration of TLS 1.2 on SCCP protocol for digital signal processor (DSP) farm including Unicast conference bridge

(CFB), Media Termination Point (MTP), and SCCP telephony control (STC) application (STCAPP).

DSP on gateways can be used as media resources for transrating or transcoding. Each media resource uses Secure Skinny Client Control Protocol (SCCP) to communicate with Cisco Unified Communications Manager. Currently SSL 3.1, which is equivalent to TLS1.0, is used for sending secure signals. This feature enhances the support to TLS 1.2. From Cisco IOS XE Cupertino 17.7.1a, TLS 1.2 is enhanced to support the Next-Generation Encryption (NGE) cipher suites.

Note Cisco Unified Communications Manager (CUCM) Version 14SU2 has been enhanced to support Secured SCCP gateways with the Subject Name field (CN Name) with or without colons, for example, AA:22:BB:44:55 or AA22BB4455.

CUCM checks the CN field of the incoming certificate from the SCCP Gateway and verifies it against the DeviceName configured in CUCM for this gateway. DeviceName contains MAC address of the gateway. CUCM converts the MAC address in the DeviceName to MAC address with colons (for example: AA:22:BB:44:55) and validates with the CN name in the Gateway's certificate. Therefore, CUCM mandates Gateway to use MAC address with colons for the CN field in the certificate, that is, subject name.

Due to new guidelines from Defense Information Systems Agency (DISA), it is a requirement not to use colons for the subject name field CN. For example, AA22BB4455.

SCCP TLS connection

CiscoSSL is based on OpenSSL. SCCP uses CiscoSSL to secure the communication signals.

If a resource is configured in the secure mode, the SCCP application initiates a process to complete Transport Layer Security (TLS) handshaking. During the handshake, the server sends information to CiscoSSL about the TLS version and cipher suites supported. Previously, only SSL3.1 was supported for SCCP secure signalling. SSL3.1 is equivalent to TLS 1.0. The TLS 1.2 Support feature introduces TLS1.2 support to SCCP secure signalling.

After TLS handshaking is complete, SCCP is notified and SCCP kills the process.

If the handshaking is completed successfully, a REGISTER message is sent to Cisco Unified Communications Manager through the secure tunnel. If handshaking fails and a retry is needed, a new process is initiated.

Note For SCCP-based signalling, only TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is supported.

Cipher Suites

For SCCP-based signaling, TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is supported.

From Cisco IOS XE Cupertino 17.7.1a, the following NGE cipher suites are also supported:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

These cipher suites enable secure voice signaling for both the STCAPP analog phone and the SCCP DSPFarm conferencing service. The cipher suite selection is negotiated between gateway and CUCM.

The following prerequisites are applicable for using NGE cipher suites:

- Configure TLS 1.2. For more information, see Configuring TLS version for STC application, on page 12.
- Use CUCM Release 14.1 SU1 or later, and Voice Gateways or platforms that support TLS 1.2.
- From the CUCM Web UI, navigate to **Cipher Management** and set the **CIPHER switch** as **NGE**. For more information, see Cipher Management.

For more information about verifying cipher suites, see Verifying TLS Version and Cipher Suites, on page 12.

For the SRTP-encrypted media, you can use higher-grade cipher suites - AEAD-AES-128-GCM or AEAD-AES-256-GCM. The selection of these cipher suites is automatically negotiated between GW and CUCM for both secure analog voice and hardware conference bridge voice media. Authenticated Encryption with Associated Data (AEAD) ciphers simultaneously provide confidentiality, integrity, and authenticity, without built-in SHA algorithms to validate message integrity.

Supported Platforms

The TLS 1.2 support on the SCCP Gateways feature is supported on the following platforms:

- Cisco 4321 Integrated Services Router
- Cisco 4331 Integrated Services Router
- Cisco 4351 Integrated Services Router
- Cisco 4431 Integrated Services Router
- Cisco 4451-X Integrated Services Router
- Cisco 4461 Integrated Services Router
- Cisco Catalyst 8200 and 8300 Series Edge Platforms
- Cisco VG400, VG420, and VG450 Analog Voice Gateways

Configuring TLS version for STC application

Perform the following task to configure a TLS version for the STC application:

```
enable
configure terminal
stcapp security tls-version v1.2
exit
```

Note The stcapp security tls command sets the TLS version to v.1.0, v1.1, or v1.2 only. If not configured explicitly, TLS v1.0 is selected by default.

Configuring TLS version in Secure Mode for DSP Farm Profile

Perform the following task to configure the TLS version in secure mode for DSP farm profile:

```
enable
configure terminal
dspfarm profile 7 conference security
  tls-version v1.2
  exit
```

Note Note: The **tls** command can be configured only in security mode.

Verifying TLS Version and Cipher Suites

Perform the following task to verify the TLS version and cipher suite:

```
# show dspfarm profile 100
Dspfarm Profile Configuration

 Profile ID = 100, Service = CONFERENCING, Resource ID = 2
 Profile Service Mode : secure
 Trustpoint : Overlord_DSPFarm_GW
 TLS Version  : v1.2
 TLS Cipher   : ECDHE-RSA-AES256-GCM-SHA384
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Total Number of Resources Configured : 10
 Total Number of Resources Available : 10
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Maximum conference participants : 8
 Codec Configuration: num_of_codecs:6
 Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g711alaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g729ar8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729abr8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729r8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729br8, Maximum Packetization Period : 60 , Transcoder: Not Required
```

Verifying STCAPP Application TLS Version

Perform the following tasks to verify the TLS version of the STCAPP application:

```
Device# show call application voice stcapp
App Status: Active
CCM Status: UP
CCM Group: 120
Registration Mode: CCM
Total Devices: 0
Total Calls in Progress: 0
Total Call Legs in Use: 0
ROH Timeout: 45
TLS Version: v1.2

# show stcapp dev voice 0/1/0
Port Identifier:  0/1/0
Device Type:      ALG
Device Id:        585
Device Name:      ANB3176C85F0080
Device Security Mode : Encrypted
  TLS version        : TLS version 1.2
  TLS cipher         : ECDHE-RSA-AES256-GCM-SHA384
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 80010
Dial Peer(s):     100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Line Mode:        CALL_CONF
Hook State:       OFFHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
HG Status:        Unknown
PLAR:             DISABLE
Callback State:   DISABLED
CWT Repetition Interval: 0 second(s) (no repetition)
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6

Call State for Connection 2 (ACTIVE): TsConnected
Connected Call Info:
   Call Reference: 33535871
   Call ID (DSP):  187
   Local IP Addr:  172.19.155.8
   Local IP Port:  8234
   Remote IP Addr: 172.19.155.61
   Remote IP Port: 8154
   Calling Number: 80010
   Called Number:
   Codec:          g711ulaw
   SRTP:           on
   RX Cipher:      AEAD_AES_256_GCM
   TX Cipher:      AEAD_AES_256_GCM
```

Perform the following task to verify the sRTP cipher suite for the DSPfarm connection:

```
# show sccp connection detail

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)
```

```
sess_id    conn_id    call-id    codec   pkt-period dtmf_method    type
bridge-info(bid, cid)   mmbridge-info(bid, cid) srtp_cryptosuite          dscp
                      call_ref   spid       conn_id_tx

16778224   -          125        N/A     N/A        rfc2833_pthru     confmsp   All RTPSPI
 Callegs      All MM-MSP Callegs      N/A                       N/A
                      -          -          -

16778224   16777232   126        g711u   20         rfc2833_pthru  s- rtpspi    (101,125)
               N/A                      AEAD_AES_256_GCM          184
                      30751576   16777219   -

16778224   16777231   124        g711u   20         rfc2833_pthru  s- rtpspi    (100,125)
               N/A                      AEAD_AES_256_GCM          184
                      30751576   16777219   -


Total number of active session(s) 1, connection(s) 2, and callegs 3
```

Verifying Call Information

To display call information for TDM and IVR calls stored in the Forwarding Plane Interface (FPI), use the **showvoipfpi calls** command. You can select a call ID and verify the cipher suite using the **show voip fpi calls confID** *call_id_number* command. In this example, cipher suite 6 is AES_256_GCM.

```
#show voip fpi calls
Number of Calls : 2
---------- ---------- ---------- ---------- --------------- ---------------
    confID correlator    AcallID     BcallID           state           event
---------- ---------- ---------- ---------- --------------- ---------------
         1          1         87         88       ALLOCATED DETAIL_STAT_RSP
        21         21         89         90       ALLOCATED DETAIL_STAT_RSP

#show voip fpi calls confID 1
--------------------------------------------------------------------------------
VoIP-FPI call entry details:
--------------------------------------------------------------------------------
Call Type        :           TDM_IP     confID          :                1
correlator       :                1     call_state      :        ALLOCATED
last_event       :  DETAIL_STAT_RSP     alloc_start_time :       1796860810
modify_start_time:                0     delete_start_time:                0
Media Type(SideA):             SRTP     cipher suite    :                6
--------------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted             :         1
.....
```

Additional References

Related Topic	Document Title
Cisco IOS Voice Gateways Configuration Guide	Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide

Feature Information for TLS 1.2 support on SCCP Gateways

Table 1: Feature Information for TLS 1.2 support on SCCP Gateways

Feature Name	Releases	Feature Information
TLS 1.2 support on SCCP Gateways	Cisco IOS XE Fuji 16.7.1	The TLS 1.2 support on SCCP Gateways feature details the configuration of TLS 1.2 on SCCP protocol for DSP farm including CFB, MTP, and STCAPP. The following commands were introduced: **stcapp security tls-version**, **tls-version**.
Support for NGE Cipher Suites	Cisco IOS XE Cupertino 17.7.1a	This feature supports NGE cipher suites for secure voice signaling and secure media. These cipher suites are applicable for both the STCAPP analog phone and the SCCP DSPFarm conferencing service.